„Kfz-Forensik“: Spezialisten des Bundeskriminalamts bei der Auswertung von Fahrzeugdaten.

„Connected Cars“: Innenminister Wolfgang Sobotka, Viktoria Weber und Walter Seeböck von der Donau-Uni Krems.

Daten, Ethik, Sicherheit

Ethische Herausforderungen bei selbstfahrenden Autos, Verkehrssicherheit, Datenschutz und -sicherheit vernetzter Autos waren Schwerpunkte bei der 14. Sicherheitskonferenz an der Donau-Universität Krems.

Nach einer Analyse der Unternehmensberatung *McKinsey* soll autonomes Fahren die Verkehrssicherheit erhöhen, die Zahl der Verkehrsunfälle um bis zu 90 Prozent reduzieren, wenn mehrheitlich selbstfahrende Autos auf Straßen unterwegs sein würden. Der Betrieb von selbstfahrenden Fahrzeugen werfe im Sinne von „Safety“ und „Security“ ethische Fragen auf. Zu diesen und anderen Themen diskutierten Expertinnen und Experten bei der 14. Sicherheitskonferenz am 20. Oktober 2016 an der Donau-Universität Krems.

„Das Thema sicheres Fahren im digitalen Zeitalter betrifft uns alle, denn die Digitalisierung bringt neben Chancen neue Herausforderungen für die polizeiliche Arbeit mit sich“, sagte Innenminister Mag. Wolfgang Sobotka in seiner Eröffnungsrede. „Wir entwickeln uns daher im Austausch mit Experten ständig weiter und die 14. Sicherheitskonferenz ist ein zukunftsweisendes Beispiel dafür“, betonte der Innenminister. „Wir können die Möglichkeiten der Digitalisierung beispielsweise im verkehrspolizeilichen Bereich bei Kontrollen, Unfallrekonstruktionen oder Auswertungen nutzen und verbessern auch die Aufklärung von Straftaten im kriminalpolizeilichen Bereich laufend.“

Roboter auf vier Rädern. Philipp Schaumann, Spezialist für IT- und Informationssicherheit, referierte über grundlegende ethische Prinzipien und ihre Anwendung auf autonome Geräte. Beim autonomen Fahren gilt es, menschliches Fehlverhalten der anderen Verkehrsteilnehmer oder technische Gebrechen das Fahrzeugs vorherzusehen und in das Sicherheitskonzept zu integrieren, denn der Algorithmus im Auto muss im Zweifelsfall entscheiden, auf welche Weise ein Unfall vermieden werden soll. Dabei stellt sich die Frage, nach welchen moralischen Grundsätzen autonome Fahrzeuge programmiert werden sollen. Es bietet sich der Utilitarismus an, der auf dem Nützlichkeitsprinzip basiert, das besagt, eine Handlung sei im ethischen Sinne korrekt, sofern sie das Wohlergehen aller von der Handlung Betroffenen optimiere. Eine der Fragen, die sich bei selbstfahrenden Autos stellt, ist: Steht mein Wohl als Fahrzeuginsasse, meine Sicherheit, über dem Wohl der anderen?

Schaumann verdeutlichte das an Beispielen:

Szenario 1: Das selbstfahrende Auto erkennt, dass ein sechsjähriges Kind knapp vor dem Auto über die Straße rennt, dabei stolpert, das Auto kann nicht mehr bremsen, könnte aber dem Kind ausweichen und gegen einen Pfeiler fahren. Wie soll der Algorithmus entscheiden?

Szenario 2: Das selbstfahrende Auto erkennt, dass ein vollbesetzter Schulbus auf das Auto zukommt, links ist eine hohe Wand, rechts ein Abgrund.

Szenario 3: Ein Lastwagen donnert von hinten heran, kann nicht bremsen, das selbstfahrende Auto könnte auf den Gehsteig ausweichen, auf dem Menschen gehen.

Wie entscheiden? Die derzeitige gesetzliche Regelung lautet: Der Fahrer ist immer verantwortlich. Das heißt, er muss ständig konzentriert sein und auf den Verkehr um ihn herum achten. Er darf nicht telefonieren, Textnachrichten verschicken, surfen, spielen oder sich zu den anderen Passagieren umdrehen. Die praktische Lösung wäre: Der Programmierer programmiert eine utilitaristische Lösung, optimiert auf das „allgemeine Wohlergehen“ – und der Autobesitzer muss mit der Entscheidung des Algorithmus leben. Das würde einen Verlust der persönlichen Autonomie bedeuten. Oder sollte es ein Menü geben, so dass der Fahrer beim Start einstellen kann, wie das Auto sich verhalten soll. Zum Beispiel, wenn seine Kinder im Wagen sind, soll das Fahrzeug auf jeden Fall versuchen, die Insassen zu retten, auch auf die Gefahr hin, dass eine größere Zahl anderer Personen zu Schaden kommt.

Studie. Diese Fragen wurden von Forschern in der Studie *The social dilemma of autonomous vehicles* untersucht. Sie wurde im Juni 2016 im Wissenschaftsmagazin *Science* veröffentlicht. Die Mehrheit der Testteilnehmer

Fotos: Bettina Vock/Donauuni Krems, Bundeskriminalamt

Selbstfahrende Autos: Die derzeitige gesetzliche Regelung lautet: Der Fahrer ist immer verantwortlich.

war dafür, dass autonome Fahrzeuge im Sinne des Utilitarismus entscheiden sollten. Das heißt, die geringere Zahl an Toten zu wählen, auch wenn der Fahrer zu Tode kommt. Wenn sie jedoch selbst ein utilitaristisch entscheidendes Auto nutzen würden, war die Mehrheit dafür, dass das Fahrzeug als erste Priorität den Fahrer und die Insassen schützen sollte.

Die Lösung könnte sein, dass Regierungen die utilitaristische Programmierung vorschreiben könnten, aber dafür gab es keine Mehrheit. Würden Regierungen das vorschreiben, würde laut der Studie das Interesse an autonomen Fahrzeugen deutlich sinken.

In Deutschland will Bundesverkehrsminister Alexander Dobrindt durch eine Ethikkommission klären lassen, wer für Unfälle von autonomen Fahrzeugen haftet – Fahrer oder Hersteller. Die Ethikkommission solle einen rechtlichen Rahmen entwickeln, der festlegt, wie computergesteuerte Fahrzeuge in Gefahrensituationen Prioritäten setzen. An diesen Rahmen sollen sich Programmierer orientieren können.

Selbstfahrende Autos werden deutlich sicherer sein, wenn ein Großteil davon unterwegs sein wird. Bis dahin werde laut Schaumann die Zahl der Unfalltoten bei Kollisionen mit anderen Fahrzeugen zwar sinken, aber es werde mehr andere Unfallopfer geben als früher, zum Beispiel mehr Schulkinder oder mehr Radfahrer. Schaumann verwies auf die Einführung der gesetzlichen Pflicht für Autofahrer, das Licht am Tag zu benutzen. Das habe die Zahl der toten Autofahrer auf Kosten der toten Fußgänger reduziert. Für Schaumann stellt sich die Frage, ob die Reduktion von zum Beispiel 20.000 Unfalltoten auf 10.000 Tote gerechtfertigt sei, wenn mehr Schulkinder oder mehr Radfahrer tödlich verunglückten.

Kfz-Forensik. Kontrollinspektor Horst Reisner, MSc, vom *Cybercrime-Competence-Center (C⁴)* des Bundeskriminalamts stellte das Projekt „Kfz-Forensik“ vor – die forensische Untersuchung von IT-Systemen und Datenspeichern in Kraftfahrzeugen zur Klärung von Straftaten. Das Projekt wird kofinanziert aus Mitteln des EU-Fonds für innere Sicherheit. „Durch die fortschreitende Entwicklung von Kommunikationsschnittstellen, Datenspeicher und IT-Systemen in modernen Kraftfahrzeugen wird die Polizei vor neue Herausforderungen und Aufgaben gestellt“, sagte Reisner. Neue Autos haben immer mehr Assistenzsysteme und Sensoren, die Informationen erzeugen, darunter Positionsdaten, Fahrverläufe, Fahrverhalten, Betriebszustände, Fehlerquellen, Bedienungsschritte usw.

Vortragende bei der 14. Sicherheitskonferenz an der Donau-Universität Krems: Philipp Schaumann, Horst Reisner, Christian Zinner, Rolf von Rössing.

Außer zur Klärung von Straftaten geben Fahrzeugdaten Aufschluss über Unfallursachen. Es können Manipulationen am Tachometer oder „Chiptuning“ an einem Fahrzeug festgestellt werden. Reisner erklärte, wie die Kfz-Forensiker des Bundeskriminalamts an diese Daten kommen, um sie auswerten zu können. Selbstfahrende Autos werden mit noch mehr Assistenzsystemen und Kommunikationsschnittstellen ausgestattet sein. „Das wird den Zeitaufwand für Auswertungen erhöhen“, betonte Reisner.

Während Assistenzsysteme die Sicherheit beim Fahren erhöhen sollen, verbauen Fahrzeughersteller oft unzureichend gesicherte IT-Technik in neuen Autos. Diese kann oftmals leicht von Kriminellen manipuliert werden. Hacker können in elektronische Systeme eines Fahrzeugs eindringen und die Steuerung des Fahrzeugs übernehmen. Elektronische Wegfahrsperren stellen kein Problem für Profidiebe dar. „Kaum

Fotos: Bettina Vock/Donauuni Krems (3), Siegbert Lattacher, RioPatuca Images/Fotolia

Selbstfahrender *Steyr*-Traktor: Dient dem *AIT* als Forschungsplattform für autonome Fahrzeuge.

haben Autos neue Sicherheitssysteme, werden sie von Kriminellen überlistet. Mit einem Funkstreckenverlängerer können Kriminelle Fahrzeuge mit Keyless-Go/Keyless-Entry-Systemen innerhalb kurzer Zeit stehlen“, erklärt Reisner. Beim Keyless-Go-System muss beim Starten nur ein Knopf gedrückt werden. „Das Funksignal zwischen Auto und Schlüssel reicht nur wenige Meter. Wenn der Autobesitzer sich vom Auto entfernt, fangen Kriminelle mit „Funkstreckenverlängerern“ die Funksignale zwischen Auto und Schlüssel ab und verstärken diese. Dadurch können sie das Auto ohne Spuren geräuschlos öffnen und damit wegfahren“, erläuterte Reisner. Elektronische Manipulationen an Fahrzeugen hinterlassen Spuren in Steuergeräten, die von Kfz-Forensikern ausgewertet werden.

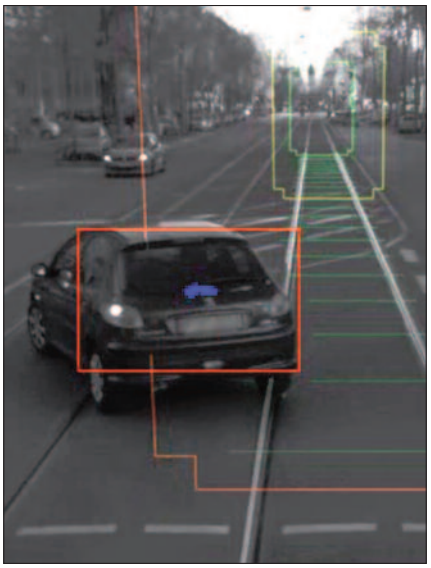
Kameras für autonomes Fahren. Das *AIT Austrian Institute of Technology* hat sich mit seinem Forschungsbereich *Intelligent Vision Systems* auf die 3D-Erfassung von Objekten und selbstlernende IT-Systeme spezialisiert. DI Christian Zinner vom *AIT* stellte den Stand der Forschung im Bereich autonomer Fahrzeuge und Arbeitsmaschinen dar und zeigte in einer Live-Demo einen selbstfahrenden *Steyr*-Traktor, der dem *AIT* als Forschungsplattform für autonome Fahrzeuge dient. Zwei Anschlüsse verbinden die Autopilot-Komponenten von *AIT* mit der Bordelektronik des Traktors. Der Traktor ist mit Kameras ausgestattet, die die Umgebung dreidimensional erfassen; drei Kameras hinter der Frontscheibe und drei am Heck. Bordcomputer wandeln die Aufnahmen in ein 3D-Modell um. Dabei wird die Geländebeschaffenheit analysiert, um Fahrspuren zu ermitteln. Dieses Prinzip kommt auch bei einem Fahrassistenzsystem für Straßenbahnen zum Einsatz, wo es automatisches

FOTO: SIEGBERT LATTACHER

Bremsen vor Hindernissen ermöglicht. Der Traktor wird auch zur Erforschung unterschiedlicher Methoden der Kontrolle eines fahrerlosen Fahrzeugs durch einen menschlichen Operator genutzt. Die Möglichkeiten reichen dabei vom Fernbedienen sämtlicher Fahrfunktionen über einen Folgemodus bis zu dem Punkt, bei dem der Mensch nur noch für das Überwachen einer vollautonom vom Fahrzeug durchgeführten Mission zuständig ist.

Das *AIT* hat als Partner zur Erprobung des selbstfahrenden Traktors das österreichische Bundesheer. Der Traktor wird auf Schießplätzen zum Mähen und zum Mulchen eingesetzt. Diese Arbeit ist gefährlich, weil scharfe Munition herumliegen und Menschen gefährden kann. Neben dem autonomen Traktor testet das *AIT* mit dem Bundesheer einen selbstfahrenden *MAN*-Lastwagen für den Lastentransport in eine gefährliche Umgebung. Die heutigen Kamerasysteme und Sensoren für selbstfahrende Fahrzeuge funktionieren noch nicht voll zuverlässig – beispielsweise bei starkem Regen oder Schneefall. „Die Entwicklungen an den Testfahrzeugen mit AIT-Technik zielen daher speziell auf gute Funktionsfähigkeit im Gelände oder bei widrigen Witterungsbedingungen ab“, sagte Zinner. Kameratechnik von *AIT* ist in einer Straßenbahn in Frankfurt im Einsatz. Sie warnt den Fahrer beim Auftauchen von Hindernissen. Die Straßenbahn soll mit einer zusätzlichen autonomen Bremsfunktion ausgestattet werden und in weiterer Folge mit der Fähigkeit zur selbstständigen Notbremsung. Gemeinsam mit dem Baumaschinenhersteller *Liebherr* erforscht *AIT* Kamerasysteme, die Personen in den Gefahrenbereichen rund um große Radlader auf Baustellen erkennen können. Im Projekt „autoBAHN“ geht es um die Automatisierung einer Regionalbahn – der Einsatz von kleinen, fahrerlosen Fahrzeugen („Trainlets“). Dabei geht es um die Frage, wie kann ein sicherer autonomer Betrieb auf offener Strecke gewährleistet werden?

Für das *AIT,* das sich unter anderem auf die Entwicklung von neuartigen Sicherheitstechnologien auf Basis künstlicher Intelligenz zum Schutz vernetzter Computersysteme kritischer Infrastruktur spezialisiert hat, sind selbstlernende Systeme eine wichtige Grundlage, um die immer komplexer werdenden IT-Systeme sicher zu gestalten und zu beherrschen.



Fahrassistenzsystem für Straßenbahnen: Kamerabasierte Hinderniserkennung von *AIT*.

Safety und Security. Rolf von Rössing, Unternehmensberater für Sicherheit, Risikomanagement und Compliance, sprach über „Sicherheitsmanagement aus Sicht der Fahrzeughersteller“. „Hersteller kämpfen mit wachsenden Fähigkeiten und Möglichkeiten der Fahrzeuge und der Dinge, die sich im Fahrzeug abspielen“, sagte Rössing.

Die Entwicklung der Digitalisierung der Fahrzeuge schreitet rasant voran. 2008 waren es noch einfache Navigationsgeräte im Fahrzeug, einige Jahr später waren Autos schon vernetzt. Dann kamen Assistenzsysteme dazu, autonome Systeme wie Einparkhilfen. Der nächste Schritt wird teilautonomes Fahren sein, dann vollautonomes Fahren. Das rufe laut Rössing eine Diskrepanz hervor zwischen den Sicherheitsrisiken der Safety, der funktionalen Sicherheit, und der Informationssicherheit, der Security.

„Das Infotainement im Auto zielt immer mehr auf den Anschluss der vom Nutzer mitgebrachten Geräte wie Smartphones ab“, erklärte der Sicherheitsexperte. Das sei ein Unsicherheitsfaktor, denn Hightech treffe dort auf veraltete Technik. Das erhebt die Frage, ob die Hersteller in der Lage seien, dem Kunden eine dem Smartphone vergleichbare Funktionalität im Auto zu bieten und dazu die Sicherheit zu gewährleisten. Die Hersteller fühlten sich verpflichtet, für die funktionale Sicherheit eines Fahrzeugs zu sorgen, was darüber hinausgehe sei Sache des Fahrzeugbesitzers. Es gehe jedoch um die Beherrschung der Risiken in der Sicherheit – sowohl Safety als auch Security. Rössing verwies auf das Beispiel des Sicherheitsgurts, der vorher optional zu haben war und erst durch Regelung des Gesetzgebers in jedem Fahrzeug eingebaut sein musste. Solange der Gesetzgeber bestimmte Sicherheitsfunktionen eines Fahrzeugs nicht vorschreibe, müsse der Autobesitzer selber für Security sorgen – etwa durch Zusatzfunktionen, die extra kosten.

Je technisch und elektronisch komplexer ein Fahrzeug sei, desto höher müsse der Sicherheitsanspruch sein. Das beginne etwa bei der Sicherheit und den Kapazitäten am CAN-Bus eines Fahrzeugs. Das Controller Area Network (CAN) vernetzt Steuergeräte in Autos. Deren Kapazität steigt mit zunehmendem Funktionsumfang der Kfz-Elektronik.

„Der Can-Bus ist einer der Schwachpunkte in Fahrzeugen. Das Can-Protokoll hat nur acht Bit, die minimale Verschlüsselungs-Technologie erfordert jedoch 128 Bit“, erläuterte Rössing. Daten, die über den CAN-Bus laufen, können zum Beispiel auf ein Smartphone übertragen werden, das über Bluetooth oder USB-Schnittstelle mit dem Infotainment des Fahrzeugs verbunden wird. Hacker könnten diese Funksignale abfangen, die CAN-Bus-Informationen lesen und Kontrolle über ein Fahrzeug erlangen.

Ein weiteres Sicherheitsrisiko sei menschliches Fehlverhalten, zum Beispiel in der Bedienung der komplexen IT-Anwendungen, die einen Fahrer überlasten könnten. Die wesentliche Zielrichtung der Hersteller im voll autonomen Fahren sei laut Rössing zunächst nicht der individuelle Personenverkehr, sondern das voll autonome Fahren im Frachtverkehr. „Der Hersteller kann nur das Fahrzeug bereitstellen mit einer Funktionalität, er kann sich nicht anmaßen, das Verkehrsgeschehen zu beherrschen“, sagte der Sicherheitsexperte.

Die 14. Sicherheitskonferenz an der Donau-Universität Krems wurde vom Zentrum für Infrastrukturelle Sicherheit unter der Leitung von Dr. Walter Seeböck, MSc, MBA, ausgerichtet. Die Veranstaltung wird vom *Kuratorium Sicheres Österreich, AIT Austrian Institute of Technology, Siemens, KEMAS Technologies,* der *Vereinigung Kriminaldienst Österreich* und *Securitas* unterstützt. *Siegbert Lattacher*

FOTO: AUSTRIAN INSTITUTE OF TECHNOLOGY