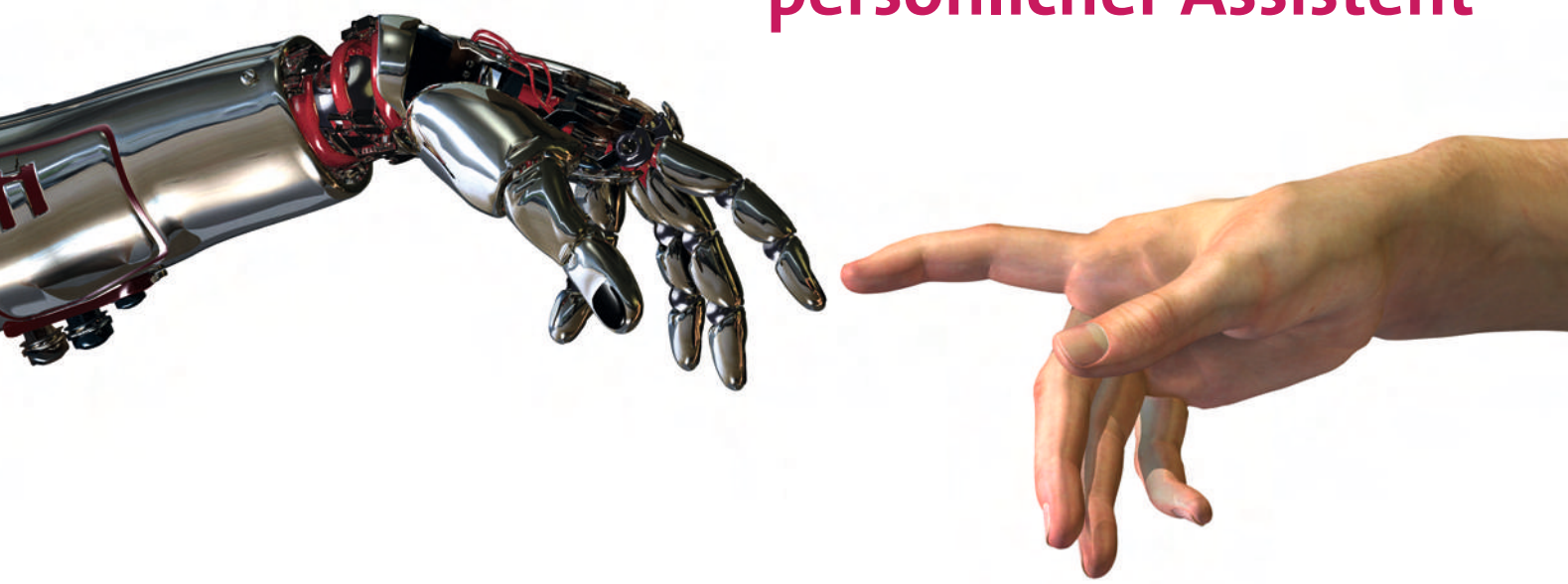
Wie sicher und vertrauenswürdig sind Roboter?

Intelligente Helfer als persönlicher Assistent



Hilfsbereite Assistenten wie Roboter werden jeden Tag intelligenter und leistungsfähiger. Ein Roboter kann schon jetzt auch ein Freund, ein Kumpel und ein Ansprechpartner sein. Immer mehr Roboter kommen zu uns nach Hause und können uns bei vielen Alltagsaufgaben helfen, manchmal auch diese übernehmen. Ein Aspekt, der mit der rasanten Entwicklung „der Roboter" einhergeht, ist die Gewährleistung der Unversehrtheit der Menschen, die in der Nähe der Roboter sind oder sich auf persönliche Assistenten verlassen müssen. Hier stellt sich die Frage, wie sicher können Roboter und andere intelligente Assistenten sein?

Roboter werden immer mehr zu echten Hilfen, weil sie in verschiedenen Bereichen aktiv Arbeiten übernehmen. Der Fantasie sind keine Grenzen gesetzt, und das Potenzial ist enorm. Bei autonomen Autos beispielsweise wird der Fahrer zum Passagier, der während der Reisezeit entspannt lesen, Musik hören, mit dem Smartphone im Internet surfen, E-Mails schreiben, spielen, sich Filme anschauen und vieles mehr tun kann. Klar ist, Roboter werden längst nicht mehr nur in Science-Fiction-Filmen gezeigt und beschrieben, sondern bereits heute auch real genutzt. Grob lassen sich drei Kategorien von Robotern unterscheiden:

Hausroboter:
Diese intelligenten Helfer können beispielsweise unsere Teppiche saugen, den Rasen mähen, die Fenster putzen, vorlesen, überwachen, dass wir nicht hilflos auf dem Boden liegen oder den Herd nicht ausgeschalten haben, und vieles mehr. Ziel ist hier, möglichst viele hilfreiche Alltagsaufgaben zu erledigen, sodass unser Leben leichter wird. Der Besitzer spart Zeit und Energie, die er für andere Aufgaben verwenden kann.

Industrieroboter:
Industrieroboter, die traditionell für bestimmte, immer wiederkehrende Handlangerarbeiten oder Arbeitsschritte innerhalb eines Produktionsprozesses eingesetzt werden, arbeiten sehr präzise und schnell – und abgesehen von Wartungsunterbrechungen ohne Pausen. Mittlerweile übernehmen sie auch komplexere Aufgaben wie zum Beispiel Autos schweißen und montieren. Außerhalb klar definierter Arbeitsschritte an einem bestimmten Ort beziehungsweise innerhalb eines fest umrissenen Bereichs bewegen sich Roboter aus Sicherheitsgründen meist sehr geschwindigkeitsreduziert.

Killerroboter oder Waffensysteme:
Killerroboter werden bei Kriegshandlungen genutzt. Sie sind leistungsstark und mehr oder weniger unverletzbar. Sie werden zum Beispiel genutzt, um Bomben zu entschärfen und andere für Menschen sehr gefährliche Aufgabe zu übernehmen. Als Drohnen kommen Roboter heute immer mehr auch für die Eliminierung von Kriminellen, Terroristen und Soldaten zum Einsatz.

Prinzipiell gibt es kaum eine Aufgabe, die nicht auch von Robotern ausgeführt werden kann. In Japan hat gar ein Hotel ohne menschliches Personal eröffnet, es wird durchweg von Robotern betrieben. Das Hotel heißt „Henn-na", auf Deutsch etwa „Das seltsame Hotel", und befindet sich in dem Vergnügungs- und Freizeitpark Huis Ten Bosch in Sasebo, Nagasaki. Das Hauptziel des neuen Hotelkonzepts ist es, Komfort zum kleinen Preis mit der Hilfe von billigen Robotern anzubieten.[1]

Ein weiteres und sehr aktuelles Thema sind autonome Fahrzeuge. Hier kommen die Vorreiter aus dem Silicon Valley und heißen Tesla und Google. Ein Smart-Auto braucht idealerweise auch eine Smart-Infrastruktur. So können Messstationen Informationen über den aktuellen Zustand der Straße sammeln, beispielsweise, ob es einen Stau gibt oder

wie nass oder wie glatt die Straße ist. Diese Informationen können sie an die sich nähernden Autos senden. Auch können sich die Autos gegenseitig informieren und damit die Infrastruktur Straße optimal nutzen.

In Deutschland ist auf der Autobahn A9 in Bayern eine Teststrecke für selbstfahrende Autos geplant. Eine Teilstrecke der A9 soll digitalisiert werden. Verkehrsminister Alexander Dobrindt will im Rahmen eines Pilotprojekts ein Stück der Autobahn so ausrüsten, dass eine Kommunikation von Fahrzeug zu Straße sowie von Fahrzeug zu Fahrzeug möglich wird. Das Projekt soll noch 2016 starten. Eines Tages könnten dort laut Dobrindt „Fahrzeuge mit Assistenzsystemen und später auch voll automatisierte Fahrzeuge fahren". Die Ziele des hochautomatisierten Fahrens: „mehr Verkehrssicherheit, besserer Verkehrsfluss, weniger Schadstoffe und eine Entlastung des Fahrers.[2] Die Nachricht von einem Unfalltoten aus den USA, der mit einem selbstfahrenden Auto von Tesla unterwegs war, zeigt aber, dass der Weg dorthin nicht einfach sein wird. Die Technik sollte eine erhöhte Verkehrssicherheit erzielen und nicht Unfälle verursachen.

Der Sicherheitslevel ist noch nicht hoch genug und das Vertrauen in Technik, wenn es um das eigene Leben geht, ist noch nicht vorhanden. Die Toleranz gegenüber Missbrauch, Fehlfunktionen, Verfügbarkeit, usw. ist im Internet erstaunlich hoch – wenn es aber um Leib und Leben geht, werden berechtigt deutlich höhere Maßstäbe gesetzt!

Das größte Problem ist, dass der Einsatz von Robotern in der Industrie, in der Medizin, auf der Straße oder zuhause ein noch nicht genau einzuschätzendes Risiko darstellt. Wie können Roboter die Sicherheit und Unversehrtheit von Menschen sichern? Oder ist unser Leben in der Nähe von Robotern gar in Gefahr? Wie können die Gefahren vermieden werden? Wir können Fehlentscheidungen ausgeschlossen werden? Welche Sicherheitsmaßnahmen sind angemessenen, um das Leben der Menschen zu schützen?

Risiko Vernetzung

Robotik-Forscher gehen davon aus, dass Roboter in Zukunft voneinander aus Fehlern lernen müssen, miteinander sprechen sowie via Internet gesteuert werden können. Das Gleiche gilt auch für autonomes Fahren und die vernetzten Fahrzeuge. Das Auto muss mit der Straße und mit den anderen Autos in Echtzeit kommunizieren, um die gewünschten Ziele zu erreichen (Car-to-Car- und Car-to-Infrastructure-Kommunikation oder Car-to-X-Kommunikation).

Mit der Vernetzung besteht das Risiko, dass Daten missbraucht und die Roboter oder selbstfahrende Autos gehackt werden können. Ein Beispiel dafür ist das Forschungsprojekt „RoboEarth", das Roboter online vernetzen will: In einer weltweit zugänglichen Cloud sollen sie Wissen austauschen [3]. Die Forscher warnen davor, dass Angreifer diese Vernetzung missbrauchen könnten, um sich etwa in einen Roboter zu hacken und damit Schäden anzurichten. Der Science-Fiction-Film „Terminator" könnte Realität werden: Roboter und Drohnen sind kurz davor, autonom in den Krieg zu ziehen. In bestimmten Kriegssituationen könnten Roboter womöglich besser als Menschen in der Lage sein, ethisch zu handeln. Sie könnten viel mehr Informationen viel schneller verarbeiten und so weniger tödliche Fehler begehen. Eine Maschine handelt ohne Hass, ohne Frust, ohne Rachsucht, ohne Nervosität oder Angst um das eigene Leben.

Risiko Software

Ein großes Risiko bei Rechnern aller Art – ganz besonders aber bei solchen, die wie eben Roboter in der Lage sind, Handlungen auszuführen – ist die mangelnde Softwarequalität. Trotz kontinuierlicher Verbesserungen beinhaltet Software generell Fehler, die für Fehlfunktionen verantwortlich sind und Hackern Angriffsflächen bieten. Das Problem sollte ernst genommen werden, ansonsten könnten im Falle von Robotern lebensbedrohliche Folgen auftreten. Wenn beispielsweise ein Roboter und ein Mensch zusammen im selben Raum sind, könnte ein Softwarefehler möglicherweise zu Zusammenstößen führen, die für die Person eine Lebensgefahr darstellen.

Im schlimmsten Fall kann eine Kollision zwischen Mensch und Roboter sogar tödlich sein. Ein Beispiel dafür ist das Zerschneiden eines Kinderfußes durch einen Mähroboter.[4] Ein anderes Beispiel ist ein Unfall mit einem Montageroboter in einem Werk des Automobilkonzerns Volkswagen. Bei diesem Unfall ist ein Techniker tödlich verletzt worden [5]. In Zukunft sollen Roboter aber noch enger mit ihren menschlichen Kollegen zusammenarbeiten oder Menschen zuhause unterstützen. Deswegen müssen hohe Sicherheitsanforderungen bei der Realisierung von Robotern erfüllt werden, damit deren Einsatz überhaupt möglich wird.

Auch autonome Fahrzeuge haben deutlich mehr Software, die prinzipiell gehackt werden und Fehlentscheidungen treffen kann. Je mehr IT im Auto verbaut und verwendet wird, desto vielfältiger sind die Möglichkeiten, die Software und damit das Auto zu hacken. Angriffspunkte bilden etwa die Wartungsschnittstellen und mehr und mehr auch das Internet, an das über Mobilfunknetze schon sehr viele Autos angeschlossen sind. Hacker könnten so Zugriff auf ein Auto erlangen. Die Risiken, dass Schaftsoftware installiert und/oder das Auto ferngesteuert wird, sind sehr groß – siehe auch.[6] Auch hier werden nicht nur hohe finanzielle Schäden auftreten, es werden auch Menschen sterben, weil die Software gehackt und missbraucht wurde.

Regelwerke für den Schutz von Menschen vor ihren Robotern

Welche prinzipiellen Möglichkeiten werden uns helfen, mehr Vertrauen in die Sicherheit von Robotern zu erlangen? Eine Lösung kann eine Risikoanalyse gemäß den sicherheitstechnischen Anforderungen der Roboter sein (ISO-Norm 10218). Dieser Teil der ISO legt Anforderungen und Anleitungen für die sichere Konstruktion, für Schutzmaßnahmen und die Benutzerinformation für Industrieroboter fest.

Grundlegende Gefährdungen in Verbindung mit Robotern werden beschrieben sowie Anforderungen, um die mit diesen Gefährdungen verbundenen Risiken zu beseitigen oder hinreichend zu verringern.[7] Die ISO-Norm ISO/TS 15066 beschreibt des Weiteren, wie Roboter zukünftig noch enger mit ihren menschlichen Kollegen zusammenarbeiten können, ohne dass bei einem Fehler im System eine Gefährdung des Menschen auftritt.[8] Diese Norm für kollaborierende Roboter unterstützt Unternehmen bei der Risikoanalyse, wenn sie Robotersysteme einführen wollen.

Als oberste Leitlinie gibt es nach wie vor die von Isaac Asimov formulierten „Robotergesetze": Diese beschreiben, wie das Verhalten der Roboter gegenüber Menschen sein sollte.[9] Diese ursprünglichen Grundregeln der Robotik lauten:

1. Ein Roboter darf einem menschlichen Wesen keinen Schaden zufügen oder durch Untätigkeit zulassen, dass einem menschlichen Wesen Schaden zugefügt wird.

2. Ein Roboter muss den Befehlen gehorchen, die ihm von Menschen erteilt werden, es sei denn, dies würde gegen das erste Gebot verstoßen.

3. Ein Roboter muss seine eigene Existenz schützen, solange solch ein Schutz nicht gegen das erste oder zweite Gebot verstößt.

Ein weiteres, eher wieder praktisches Regelwerk ist die Richtlinie 2006/42/EG für Maschinen und Roboter. In ihr sind zahlreiche weitere Sicherheitsanforderungen definiert[10]. Diese Maschinenrichtlinie regelt ein einheitliches Schutzniveau zur Unfallverhütung für Maschinen. Auch die amerikanische Norm ANSI RIA R15.06 beschäftigt sich mit der Sicherheit bei Robotern. Sie besteht aus Sicherheitsanforderungen für Roboter, Menschen und Hersteller[11].

Prinzipielle Sicherheitsmechanismen

Im Zusammenhang mit Robotern stehen IT-Sicherheit und Safety ganz oben auf der Prioritätenliste. Safety beschreibt die Betriebssicherheit und Security die Angriffssicherheit eines Roboters oder eines selbstfahrenden Autos. Im Folgenden werden einige prinzipielle Sicherheitsmechanismen dargestellt:

Um Fehler zu vermeiden, sollte Roboter-Software erst in einer virtuellen Umgebung ausführliche Simulationsläufe absolvieren: Mit virtuellen Roboter-Controllern und Software zur 3D-Robotersimulation können bei Offline-Programmierung alle Schritte der Robotersteuerung simuliert und durchgespielt werden, bevor die Hardware-Geräte zum Einsatz kommen.

Ein weiterer Sicherheitsmechanismus, der hilft, Menschen zu schützen, ist die Ausrüstung des Roboters mit intelligenten Sensoren. Ein Beispiel dafür ist die Anwendung einer sensiblen Roboterhaut: Die Roboterhaut besteht aus Sensoren, die Berührungen erkennt. Sobald diese Roboterhaut einen Kontakt meldet, soll sich der Roboter langsamer bewegen, stoppen oder sogar zurückweichen oder ausweichen. Wenn der Abstand zum Menschen zu gering wird, stoppt der Roboter. Ein großer Nachteil ist, dass es sehr teuer ist, einen Roboter mit künstlicher Haut auszustatten, weil dafür viele Sensoren benötigt werden.

Ein anderer Sicherheitsmechanismus ist die Verwendung eines Sicherheitslaserscanners zum Scannen der Umgebung beziehungsweise zur Überwachung von Schutzfeldern. Sobald eine Person das Schutzfeld betritt, wird der komplette Roboter angehalten. Darüber hinaus gibt es noch Überwachungssysteme, die durch den Einsatz von Projektoren und 3D-Kameras den Raum des Roboters überwachen. Die zu überwachenden Schutzzonen werden direkt auf den Fußboden oder auch an die Wand projiziert. Dabei zeichnen die Projektionsstrahlen sichtbare Linien in den Arbeitsraum. Menschen erkennen das Schutzfeld sofort und wissen, wie weit sie sich dem Roboter nähern dürfen. Wenn die Sicherheitsbereiche von Personen verletzt werden, erkennt die Kamera umgehend, dass die projizierten Linien unterbrochen werden. Der Roboter reagiert entsprechend.

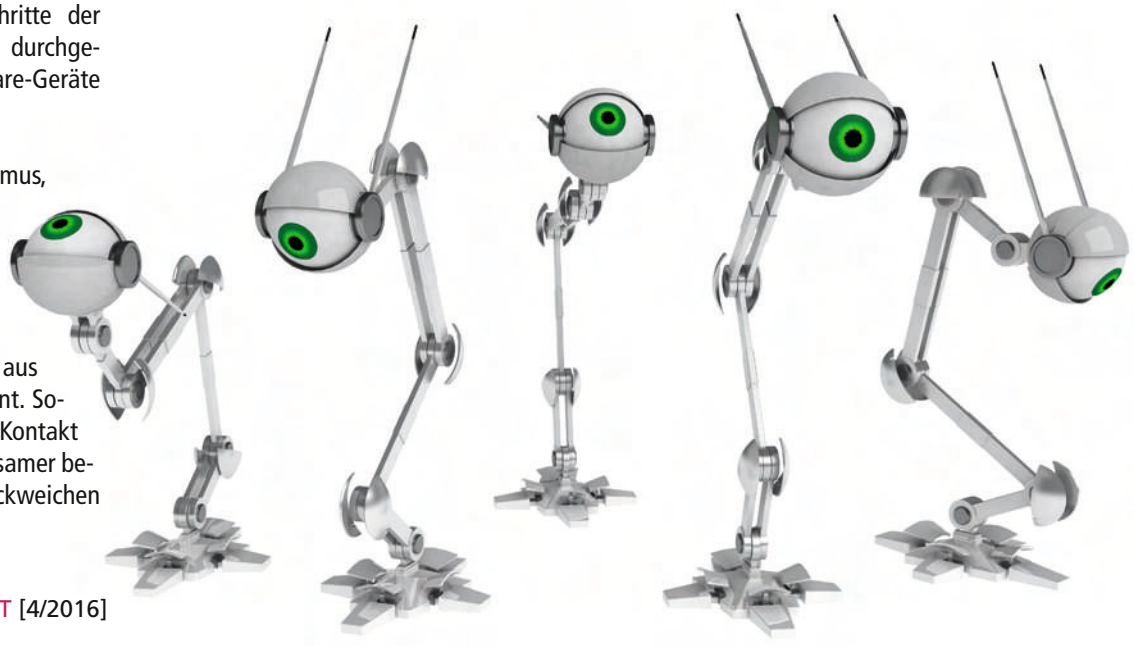
Auch lassen sich optische und akustische Warnsignale erzeugen[12]. Wie beim Raumüberwachungssystem können Sensoren, Laserscanner und 3D-Kameras beim autonomen Fahrzeug eingesetzt werden, um Informationen über den Straßenverkehr zu sammeln. Zum Beispiel: der Einsatz von Kamerasystemen im Rückspiegel, die im sichtbaren Licht arbeiten, um Verkehrsschilder und Fußgänger zu erkennen.

Außerdem gibt es Not-Halt-Tasten: Sie ermöglichen Personen, die sich nicht im Detail mit der Technik des Roboters auskennen, den Roboter schnell und intuitiv zu stoppen.

Außerdem sollte bei Robotern, wie bei PCs üblich, ein Software-Update-Konzept umgesetzt werden, um bekannt gewordenen Softwarefehlern direkt entgegenwirken zu können.

Es gibt im Alltag immer noch sehr viele Aufgaben, die Roboter nicht so gut wie Menschen erfüllen können. Roboter sind nicht kreativ und können nur die vorgegebenen Aufgaben erledigen. Im Gegensatz dazu entwickeln die Menschen jeden Tag etwas Neues, das Roboter gegebenenfalls umsetzen. Der heutige Roboter tut das, was die Programmierer für ihn vorgesehenen haben. Er ist nicht in der Lage, seine eigene Tätigkeit selbständig zu bestimmen.

Prognosen sagen voraus, dass fast die Hälfte aller derzeitigen Jobs zukünftig von Maschinen erledigt werden könnte und viele Personen ihre heutigen Arbeitsplätze verlieren werden. Laut einer Studie der Unternehmensberatung A.T. Kearney beispielsweise sind 45 Prozent der Arbeitsplätze durch die Einführung von Robotern bedroht[14]. Gefährdete Berufe sind zum Beispiel Büro- und Sekretariatskräfte, Berufe im Verkauf, Berufe in der kaufmännischen und technischen Betriebswirtschaft und viele mehr. Nicht gefährdet sind laut der Studie zum Beispiel Berufe in der Kinderbetreuung und -erziehung, Berufe in der Gesundheits- und Krankenpflege sowie Aufsichts- und Führungskräfte.



Aktuelle Herausforderungen

Zurzeit sind die Preise für Roboter noch sehr hoch, so dass die Investition nicht immer lohnenswert ist. Ein weiterer Punkt ist, dass beispielsweise ein Smart-Auto idealerweise auch eine Smart-Infrastruktur braucht: digitale Straßen und digitale Karten, um kommunizieren zu können – und das könnte sehr aufwändig sein.

Eine weitere Herausforderung, die noch geklärt werden muss, ist wer haftet, wenn der Roboter Schäden verursacht? Der Roboter selber? Die Firma, die den Roboter hergestellt oder verkauft hat? Der oder die Programmierer des Roboters? Der Nutzer des Roboters? Niemand?

Die gleiche Herausforderung besteht beim autonomen Fahren, wenn ein Unfall passiert ist. Wer ist schuldig, wer haftet für Schäden, wenn niemand fährt? Der Fahrer, der Autohersteller oder die Versicherung? Der Straßenverkehr in China, in den USA oder in Deutschland unterscheidet sich voneinander. Was müssen wir tun, um ein autonomes Auto aus Deutschland in die USA zu bringen. Kann das autonome Auto dort fahren?

Auf all diese Fragen gibt es zurzeit keine zufriedenstellenden Antworten. Die Gesetze müssen geändert und diese Fragen beantwortet werden.

Resümee

Roboter sind heute schon im Einsatz! Sie kommen zum Beispiel zu uns nach Hause und können uns bei vielen Alltagsaufgaben helfen. Auf der anderer Seite muss darauf geachtet werden, dass diese neue Entwicklung „Roboter" für uns Menschen gefährlich sein kann, weil Roboter zurzeit nicht in der Lage sind, die Unversehrtheit von Menschen zu garantieren. Deswegen müssen intelligente und sichere Roboter entwickelt werden.

Bei der Auswahl des Roboters und anderer Assistenzsysteme ist darauf zu achten, dass die erforderlichen Sicherheitsfunktionen angemessen bereitgestellt werden. Die Sicherheit spielt bei Roboterapplikationen eine zentrale Rolle. In der Praxis erfordert jede Applikation eine eigene sicherheitstechnische Betrachtung.

Beim autonomen Fahren können wir bequemer von einem Ort zum anderen kommen und gleichzeitig eine andere Aktivität erledigen. Autonome und vernetzte Autos sorgen künftig für mehr Sicherheit auf den Straßen, aber gleichzeitig tun sich neue Risiken auf, die vom Level der IT-Sicherheit abhängen. Auch wenn die Summe der Verkehrstoten mit der Hilfe von selbstfahrenden Autos weiter reduziert werden wird, stellt sich die Frage, ob Menschen Softwarefehler oder Hackerangriffe als Ursache von Verkehrstoten akzeptieren werden? Wie auch bei Flugzeugen, wo IT-Security und Safety eng zusammen gehören, sind die IT-Sicherheitsarchitekturen und -mechanismen deutlich aufwändiger als in der normalen IT. Wenn wir Roboter und andere intelligente Assistenzsysteme in der Zukunft mehr nutzen wollen, brauchen wir einen Quantensprung bei der Sicherheit. Dazu müssten sich die Hersteller von Robotern, selbstfahrenden Autos und Vertreter der IT-Sicherheitsindustrie strategisch zusammentun. Das aber ist leider zurzeit noch nicht zu erkennen. ■

Quellen:

1 *http://www.h-n-h.jp/en/*
2 *http://www.sueddeutsche.de/auto/autonomes-fahren-haende-weg-vom-lenkrad-1.2321538*
2 *http://roboearth.org/*
4 *http://www.nwzonline.de/blaulicht/maehroboter-zerschneidet-kinderfuss-maehroboter-zerschneidet-kinderfuss_a_30,1,979365985.html*
5 *http://www.golem.de/news/vw-toedlicher-arbeitsunfall-mit-einem-roboter-1507-114997.html*
6 *http://www.deutschlandfunk.de/autonomes-fahren-hacken-ins-auto-der-zukunft.676.de.html?dram:article_id=324879*
7 *http://www.deutschlandfunk.de/autonomes-fahren-hacken-ins-auto-der-zukunft.676.de.html?dram:article_id=324879*
8 *http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref2057*
9 *http://www.planet-wissen.de/technik/computer_und_roboter/roboter_mechanische_helfer/pwieisaacasimov100.html*
10 *http://www.maschinenrichtlinie.de/news/*
11 *http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2FRIA+R15.06+%2F+ANSI%2FRIA%2FISO+10218+%2F+RIA+TR+R15.206+-+Industrial+Robots+Safety+Package&sourcekeyword=_inurl%3Awebstore.ansi.org%23inurl%3Asku%3Dansi&source=google&adgroup=ANSI-Standards&gclid=CJmt4_aQvM0CFbYW0wodsv8KBg*
12 *https://www.pilz.com/de-INT/solutions/sectors/robotics*
13 *https://www.atkearney.de/pressemitteilung/-/asset_publisher/00OIL7Jc67KL/content/45-prozent-jobs-durch-roboter-bedroht*

HAYTHEM BEN DHIA,
studiert im Master Internet-Sicherheit am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit der Sicherheit und Vertrauenswürdigkeit von Robotern und selbstfahrenden Autos.

NORBERT POHLMANN,
Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT