Roboter nimmt Rücksicht auf Menschen in nächster Nähe

Mensch und Roboter sollen künftig eng zusammenarbeiten. Neue Sensorsysteme sorgen für intuitive und sichere Abfolgen für die menschlichen Arbeiter.

Alois Pumhösel

Die industrielle Fertigung bewegt sich auf eine stärkere Verzahnung der menschlichen und maschinellen Arbeitskräfte zu. Jenen Bereichen, in denen Roboterarme in Käfigen oder hinter Plexiglasscheiben Produkte montieren, folgen geteilte Abteilungen. Roboter helfen hier den menschlichen Arbeitskräften beispielsweise, indem sie im richtigen Moment das passende Werkzeug oder Bauteil reichen oder indem sie etwa schwere Getriebeteile für die Montage millimetergenau positionieren.

Damit das klappen kann, müssen dem Roboter verlässliche Informationen über seine unmittelbare Umgebung zur Verfügung stehen. Die richtige Sensorik ist Voraussetzung für intelligente Algorithmen, die das System in Abstimmung mit dem Umfeld steuern können. In diesem Bereich ist das Projekt CapSize angesiedelt. Gefördert vom Europäischen Fonds für regionale Entwicklung (Efre) und vom Kärntner Wirtschaftsförderungsfonds (KWF) arbeiten Wissenschafter des Forschungsinstituts Joanneum Research, der Universität Klagenfurt und der FH Kärnten gemeinsam an einer modularen Interaktionszelle für Mensch und Maschine. In der sogenannten Contactless and Safe Interaction Cell (CSIC) als abgeschlossene Einheit weichen die Käfige vordefinierten Räumen, die von umfassender Sensorik durchdrungen sind.

Sensor-Fusion

„Ein wichtiger Aspekt der kollaborativen Arbeitsplätze ist, dass die verschiedenen Sensorsysteme nahtlos miteinander kombiniert werden“, sagt Projektmitarbeiter Johannes Sturm, der mit Projektleiter Dongning Zhao an der FH Kärnten an CapSize arbeitet, über die Bedeutung sogenannter Sensor-Fusion-Technologien für diesen Bereich. Verschiedene Sensortypen werden dabei zu einem Gesamtmodell „zusammengerechnet“ – etwa Kamera- oder Radarsensoren, die einen Überblick geben, und Berührungssensoren, die Informationen von der direkten Roboterumgebung liefern.

In dem Projekt konzentriert man sich auf sogenannte kapazitive Sensoren – ein verbreitetes Prinzip, das etwa hinter vielen Touchscreens steht: Ein elektromagnetisches Feld wird dabei von einer Annäherung oder Berührung verändert, die veränderten Eigenschaften werden gemessen.

Foto: Getty/iStock/Ndoeljindoel

Umfassende Sensorik und Algorithmen sind bei kollaborativen Arbeitsplätzen, wo Mensch und Roboter zusammenarbeiten, essenziell.

Sensoren dieser Art sollen hier aber mitsamt eigenen integrierten Schaltungen, die eine lokale Verarbeitung der Sensorinformationen übernehmen, großflächig in Form von Folien arrangiert werden, mit denen dann Arbeitsoberflächen und Roboterarme überzogen werden. Die so entstandenen Sensor-Arrays sollen Bewegungen in einem Umfeld von bis zu 20 Zentimetern von Roboter und Arbeitsbereich – im Rahmen des Projekts soll neben dem Roboterarm die Oberfläche eines Werktisches mit der Sensorik ausgestattet werden – erkennen. Darunter können auch Gesten fallen, mit denen die Menschen intuitiv ihre Roboterkollegen steuern können, verdeutlicht Sturm.

Die autonom arbeitenden Sensorbereiche sollen über eigene Rechenkapazität, Stromversorgung und Übertragungstechnologie verfügen. Lokale Auswertungsergebnisse werden an eine übergeordnete Systemeinheit übermittelt, wo auch Daten anderer Sensorsysteme und -typen einlangen und zu einem Gesamtbild vereint werden. Eine relevante Frage dabei lautet, wie eine sinnvolle Aufteilung der Berechnungen zwischen lokaler und zentraler Instanz aussehen könnte. Für Sturm hängt die Gestaltung der Datenprozessierung letztlich von der konkreten Anwendung des Systems ab.

Höhere Arbeitsgeschwindigkeit

Die voll integrierte Sensorik im Arbeitsplatz soll etwa davor bewahren, dass tote Winkel entstehen – Situationen, die von keinem der Sensorsysteme schnell genug registriert werden können. Eine nahtlos alle Bereiche abdeckende Sensorik, die sicher arbeitet, würde auch eine höhere Arbeitsgeschwindigkeit der Roboterarme erlauben. „Das System soll sehr adaptiv sein und beispielsweise trotz einer Ausweichbewegung aufgrund der Nähe eines Menschen dennoch einen Handgriff oder eine Tätigkeit gezielt zu Ende führen können“, erläutert Sturm.

Während sich die FH Kärnten im Projekt um das Design der eingebetteten Elektronik kümmert, fokussiert die Uni Klagenfurt auf die Entwicklung des Sensorprinzips und Joanneum Research auf die Roboterintegration. Am Ende des Projekts soll ein Prototyp stehen, der die Funktionsweise der neuartigen Sensorik an einem Roboterarbeitsplatz demonstriert – und auf dem zukünftige Forschungen aufbauen können.

www.cap-size.at

Damit das Zuhause nicht nur smart, sondern auch sicher wird

Ein niederösterreichisches Forschungsprojekt sucht nach verbesserten Ansätzen für erhöhte Sicherheit und Resilienz bei Smarthome-Systemen

Wenn man Kühlschränke, Überwachungskameras und Garagenöffner ins Internet hängt, können von dort aus auch unerwünschte Zugriffe erfolgen. Schutzvorrichtungen sind nötig. Mit der Etablierung von Smarthome-Systemen wurde aber schnell klar, dass die Systeme punkto Sicherheit oft zu wünschen übrig lassen. Standards und Zertifizierungen fehlen, Sicherheitsupdates bleiben aus. Auch die Nutzer sind nachlässig: Standard-Passwörter werden nicht oder nur mit sehr unsicheren Zeichenfolgen ersetzt.

Im Projekt Ares (Resilienz von IoT-basierten Sensoren in der Heimautomation gegen Cyberattacken) der Donau-Universität Krems und der FH St. Pölten, unterstützt von der NÖ Forschungs- und Bildungsgesellschaft (NFB) vom Land Niederösterreich, sollen potenzielle Sicherheitslücken adressiert werden. Um resilientere Systeme zu schaffen, werden neue technische Lösungsansätze angedacht und Problembewusstsein bei den Nutzern geschaffen. „Meist geht es nicht um klassische Delikte wie Diebstahl“, so Projektleiter Thilo Sauter vom Zentrum für Mikro- und Nanosensorik der Donau-Uni. „Bei Cyberstalking gibt es aber zum Beispiel Potenzial – etwa wenn nach einer Scheidung die Zugänge zum Smarthome-System benutzt werden, um den Ex-Partner zu tyrannisieren.“

Ein technischer Fokus im Projekt betrifft die Angreifbarkeit von Sensoren, die im Smarthome omnipräsent sind. Sie helfen, Heizung und Jalousien zu steuern oder Türbereiche zu überwachen. „Die Idee ist, die Sensordaten mit einem Wasserzeichen zu versehen, sodass man ihre Authentizität sicherstellen kann“, sagt Sauter. „Werden die Daten von außen verfälscht, würde das Wasserzeichen zerstört und die Manipulation offensichtlich.“

Das Besondere dabei ist die Datenquelle, die zur Erstellung der Signatur herangezogen werden soll. Die Forscher wollen sich der „Meta-Informationen“ des Systems bedienen: „Man könnte das Rauschen – also zufällige Variationen – in einem Funkkanal oder in der Stromversorgung verwenden, um die Signatur zu basteln“, erklärt Sauter. Der Ansatz wäre resilienter gegen Angriffe als Signaturen, die auf vordefinierten algorithmischen Funktionen basieren und die etwa mithilfe von statistischen Methoden angreifbar sind.

Kameras im Eigenheim können ein Sicherheitsrisiko sein.

Foto: AP / Ryan Nakashima

Ein Problem dabei: Die Datenpakete, die von den Sensoren verschickt werden, sind oft überschaubar klein. „Verschickt ein Temperatursensor einmal pro Minute ein wenige Bit großes Signal, müsste auch das Wasserzeichen entsprechend klein sein“, sagt der Forscher. Ein Lösungsansatz dafür wäre, die Signatur auf mehrere Übertragungen aufzuteilen, um sie beim Empfänger wieder zusammenzufügen.

Die Überprüfung, ob eine Signatur gültig ist, würde wie bei etablierten Kryptoverfahren – etwa per geteilten oder öffentlichen Schlüssel – erfolgen. Letzten Endes soll das Projekt klären, welche Ansätze in diesem Bereich machbar und sinnvoll sind.

Die soziologischen Untersuchungen in dem Projekt beinhalten eine – gerade in Auswertung befindliche – Umfrage, in der nach Erfahrungen mit Angriffen auf Smarthome-Systeme und dem diesbezüglichen, subjektiven Sicherheitsgefühl gefragt wird. So viel vorweg: Sauter gibt sich angesichts der Daten erstaunt, wie verbreitet internetfähige Haushaltsgeräte bereits sind. (pum)