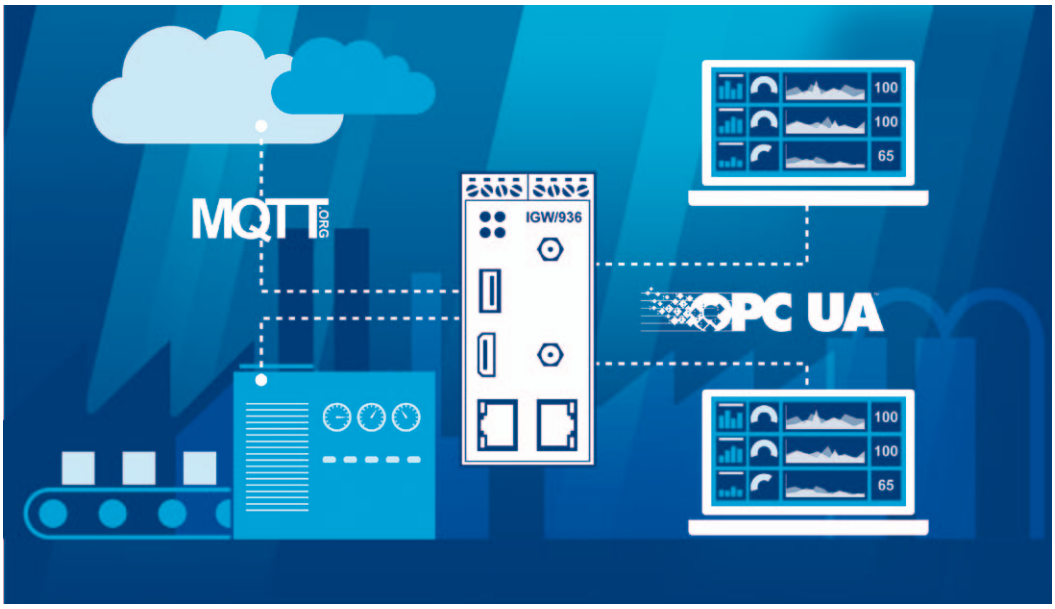
Schwerpunktverlagerung erforderlich



Der Stand der Technik hinsichtlich Kommunikationsprotokollen, Schnittstellen und Standards im M2M- und IoT-Umfeld hat ein sehr hohes Niveau erreicht. Der Handlungsbedarf für echte Innovationen verlagert sich in andere Bereiche. Zu tun gibt es genug. Besonders bei der Sensorik und Security.

Die Problematik

In der Vergangenheit haben sich Heerscharen von Entwicklern sehr intensiv mit allen, was man unter dem Sammelbegriff „Connectivity" zusammenfassen könnte, beschäftigt. Herausgekommen ist dabei, dass man für das Internet der Dinge sowohl in der Consumer- als auch der Industrie-4.0-Welt in erster Linie IEEE 802.3-, Wi-Fi-, Bluetooth-, 6LoWPAN-, MQTT-, OPC UA- und REST-basierte Kommunikationslösungen benötigt. Gravierende Innovationen sind in diesem Bereich nicht mehr zu erwarten, bestenfalls inkrementelle Weiterentwicklungen, wie zum Beispiel Publish/Subscribe (Pub/Sub) und TSN für OPC UA.

Völlig anders sieht es in der Sensorik und IT-Security aus. Hier besteht nach wie vor ein großer Innovationsbedarf, um zum einen dafür zu sorgen, dass IoT-Lösungen auch einen quantifizierbaren Nutzen für den Anwender bieten und zum anderen nicht nahezu im Wochentakt neue Meldungen über besorgniserregende IT-Security-Probleme auftauchen. Dazu im folgenden zwei Beispiele.

Beispiel: Innovative Sensorik

Die Schlüsselkomponenten für praktisch alle IoT-Anwendungen sind Sensoren. Ein erfolgreiches IoT-Produkt mit hohem Anwendernutzen kann durchaus ohne Cloud, aber nur sehr selten ohne einen einzigen Sensor funktionieren. Daher werden dringend sehr gute Sensorikideen benötigt, um dem Internet der Dinge durch besonders intelligente Sensorlösungen bei der Marktdurchdringung zu helfen und wettbewerbsfähige Produkte mit richtungsweisender Technik zu schaffen.

Die Halbleiterindustrie hat über immer preiswertere und leistungsfähigere MEMS-Sensoren bereits die Voraussetzungen geschaffen. Insofern sind im IoT-Umfeld in den nächsten Jahren viele innovative Sensorkonzepte zu erwarten. Besonders Kombinationen aus MEMS-Sensorelementen und KI-Algorithmen des maschinellen Lernens (Machine Learning) versprechen ein sehr hohes Innovationspotenzial. Ein Beispiel ist der Synthetic Sensor für Smart-Home-Anwendungen der Future Interface Group der Carnegie Mellon University (CMU) in Pittsburgh, USA (siehe https://bit.ly/2FwYyxN). Dort wurden im Rahmen eines Forschungsprojektes neun unterschiedliche physische Sensorelemente auf eine Leiterplatte mit einer Grundfläche von ca. 45 x 49 mm montiert (Bild 1), um z. B. eine Küchenlandschaft in eine intelligente Umgebung zu verwandeln. Die einzelnen Sensorelemente dieses Synthetic-Sensor-Beispiels sind:

AMG8833 Grid-EYE

Infrarot-Array-Sensor, der sich z. B. als thermischer Näherungsschalter eignet. Das Sensorelement besteht aus einem 8x8-Array und liefert insgesamt 64 thermische Messpunkte mit individuellen Temperaturwerten. Der Messbereich jedes Arrayelements reicht von 0 bis 80 °C. Es werden Wärmequellen in einem Abstand bis zu sieben Metern gemessen.

TCS34275 RGB-Farbsensor

Optisches Sensorelement mit hoher Empfindlichkeit und integriertem Clear Light Sensing sowie einem IR-Blocking-Filter. Der TCS34275 erkennt die RGB-Farben eines Objektes.

MAG3110F 3D-Magnetometer

Dieses digitale 3-Achsen-Magnetometer eignet sich zur Messung magnetischer Flussdichten, die sich in der Praxis aus der Summe des Erdmagnetfeldes und der lokalen Magnetfelder elektrischer Bauelemente in unmittelbarer Umgebung zusammensetzen.

BME280 Kombo-Sensor

Dieser Umweltsensor misst gleichzeitig die relative Luftfeuchte, Temperatur und den Luftdruck. Dabei wird eine hohe Linearität über den gesamten Messbereich erreicht.

MPU6500 MEMS Motion Tracking Device

Multifunktionaler MEMS-Sensor für verschiedene Bewegungsfunktionen. Der MPU6500 enthält einen 3-Achsen-Beschleunigungssensor, ein 3-Achsen-Gyroskop (Kreiselstabilisator) sowie einen Digital Motion Processor.

AMN211 PIR Motion Sensor

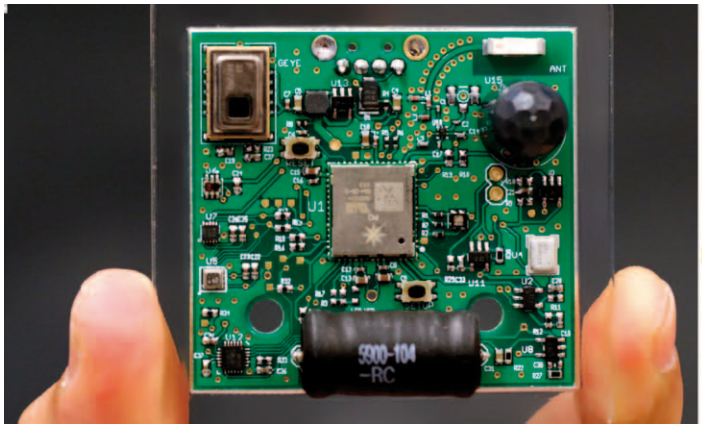
Passiver IR-Sensor, der als einfacher Bewegungsmelder funktioniert. Die Bewegung einer menschlichen oder tierischen Wärmequelle im „Sichtfeld" des Sensors wird über einen digitalen Ausgang gemeldet.

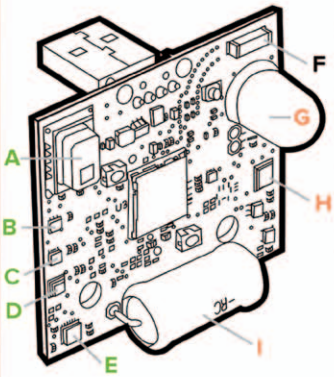
ADMP401 Mikrophone

Dieses einfache MEMS-Sensorelement dient als Mikrofon mit analogem Spannungsausgang, um die

Kurz gefasst

In der Vergangenheit beschäftigte sich die Industrie hauptsächlich mit dem Thema Connectivity. Das Thema Security hatte längst nicht den Stellenwert, den es haben müsste. Die Problematik verschärft sich noch, da immer mehr Intelligente Sensoren hinzukommen.





ID	Name and Sensor	Chan.	Freq.
A	GridEye AMG8833	16	10Hz
B	Color/Illum. TCS34725	4	10Hz
C	Magnetometer MAG3110F	3	10Hz
D	Temp/Baro/Hum. BME280	3	10Hz
E	Accelerometer MPU6500	3	4kHz
F	2.4GHz WiFi (RSSI)	1	10Hz
G	PIR Motion AMN2111	1	10Hz
H	Microphone ADMP401	1	17kHz
I	100mH Inductor (EMI)	1	.5MHz

● Digital Components
● Analog Components

Bild 1: Der Synthetic Sensor der Carnegie Mellon University (CMU) besteht aus insgesamt neun unterschiedlichen Sensorelementen, die zusammen 12 verschiedene Messwerte erfassen können. Bild: Gierad Laput, USA

Daten einer Schallquelle zu erfassen und akustische Analysen durchzuführen.

Des Weiteren befinden sich noch eine 1000-mH-Induktivität und ein Funk-Transceiver auf der Synthetic-Sensor-Baugruppe. Beides kann ebenfalls als Quelle für weitere Sensorrohdaten dienen, z. B. für EMI- und RSSI-Messwerte.

Die neun Sensoren des CMU-Synthetic-Sensors liefern insgesamt 12 unterschiedliche Messwerte. Die Rohdaten der Sensorelemente zu einem bestimmten Zeitpunkt bzw. innerhalb einer bestimmten Zeitspanne dienen als Eingabe für Machine-Learning-Algorithmen. Die jeweiligen Ausprägungen der einzelnen Sensormesswerte sind charakteristisch für bestimmte Aktivitäten im Umfeld des Synthetic Sensors. Damit kann man zum Beispiel einen laufenden bzw. tropfenden Wasserhahn vom eingeschalteten Herd, einer aktiven Kaffeemaschine oder Mikrowelle u. a. Aktivitäten in einer Küchenlandschaft unterscheiden. Hinsichtlich derartiger Differenzierungen findet man im sogenannten Supervised Machine Learning verschiedene Methoden, wie beispielsweise die Cluster Analyse. Dabei werden Datenpunkte (in diesem Fall die Merkmalsausprägungen der einzelnen Sensorrohdaten) gemäß ihren quantifizierten Ausprägungen in Gruppen eingeteilt. Bei dieser Messwerteinteilung werden Abstands- und Ähnlichkeitsmaße miteinander verglichen.

Algorithmen-Training

Durch das Algorithmen-Training per Supervised Machine Learning entsteht ein Datenmodell mit den jeweiligen Aktivitäten bzw. Szenarien im Messbereich des Synthetic Sensors. Das Modell kann danach in einer „Produktivphase" eines Synthetic Sensors mit Echtzeit-Produktivdaten zum automatischen Erkennen von Umgebungsszenarien bis hin zu Verbrauchsdatenmessungen (Durchflussmenge eines Wasserhahn, Energie für Beleuchtung) oder Anomalitätserkennungen (Herd eingeschaltet, seit x Minuten keine Person im Raum usw.) genutzt werden.

Beispiel: Ungeschützte IoT Devices Im Internet

Eine der einfachsten IT-Sicherheits-Grundregeln für vernetzungsfähige Baugruppen ist, dafür zu sorgen, dass ein potenzieller Angreifer aus dem Internet keine offenen Serviceschnittstellen findet, die sich für Cyberattacken jeglicher Art missbrauchen lassen. Diese Anforderung gilt auch für den Fall, dass der IoT-Device-Betreiber seinen Internetzugang unzureichend geschützt hat und bereits ein einfacher Portscan per Internet klare Hinweise auf das mögliche Angriffsziel liefert.

Sicherheitslücken und deren Auswirkungen

Hier in Deutschland wurden die möglichen Auswirkungen vor mehr als fünf Jahren in den Medien bereits ausgiebig diskutiert. Damals waren gravierende Fernzugriffsschwachstellen in den BHKW-Heizanlagen eines namhaften Herstellers entsprechend aufgefallen. Heise.de, Spiegel Online u.v.a. berichteten mit Titeln wie „Sicherheitslücke bedroht Hightech-Heizungen" sehr ausführlich über das Thema. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schaltete sich ein. Die jeweiligen Anlagen wurden durch Unterbrechen einer Kabelverbindung vom Internet getrennt. Der betroffene Heizungshersteller bot den Kunden nach einigen Monaten eine VPN-basierte Problemlösung an und nutzt seither eine sehr sichere Internet-basierte Fernwartung. In anderen Ländern mit hoher Internetverbreitung gab es ähnliche Vorfälle, die zu einer vergleichbaren Medienaufmerksamkeit führten. Eigentlich sollte man nach derartigen Ereignissen davon ausgehen, dass Anbieter kommunikationsfähiger Produkte zwischenzeitlich eine Lernkurve durchlaufen haben und nur noch entsprechend geschützte Produkte auf dem Markt kommen. Leider ist offensichtlich das Gegenteil der Fall: Es werden immer mehr Produkte mit ungeschützten Fernzugriffsschnittstellen angeboten und installiert, so dass die Anzahl der per Internet direkt angreifbaren Devices vermutlich schon im Milliarden-Bereich liegen dürfte.

„Exposed Cyber Assets"

Forscher des international tätigen Unternehmens Trend Micro haben in bestimmten Regionen mit Hilfe der Computer- und Device-Suchmaschine Shodan gezielt nach per Internet erreichbaren Devices gesucht und die Ergebnisse in verschiedenen Reports im November 2017 auf einer Webseite mit dem vielsagenden Titel „Cities Exposed in Shodan: Western European, UK, French, German, and US Cities exposed. Are your connected devices searchable on the internet? Find out what you are risking." veröffentlicht (siehe https://bit.ly/2KqjIS8). Dabei fanden die Trend-Micro-Forscher allein in den 10 größten US-Städten mehr als 178 Millionen sogenannter

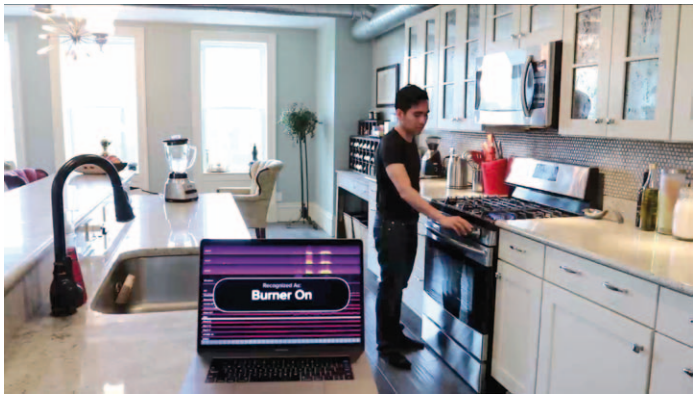


Bild 2: Die CMU-Forscher haben ihren Synthetic Sensor in einer Küchenlandschaft erprobt, um eine intelligente Umgebung zu schaffen und die Vorteile aufzuzeigen. Im Gegensatz zu den sehr teuren intelligenten Haushaltsgeräten, wird in einer Küche nur ein einziger Synthetic Sensor benötigt, um nahezu alle Aktivitäten quantifizierbar zu erkennen. Bild: Carnegie Mellon University, Pittsburgh, USA

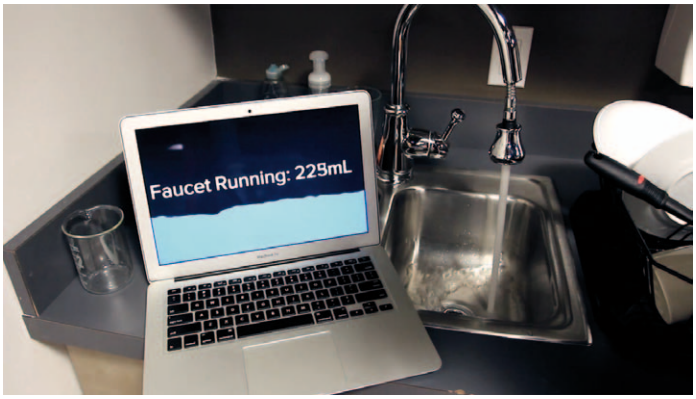


Bild 3: Ein laufender Wasserhahn, ein eingeschalteter Herd, eine aktive Kaffeemaschine oder Mikrowelle erzeugen jeweils unterschiedliche Messwertausprägungen bei den neun Sensoren des Synthetic Sensors. Damit lässt ich ein Machine-Learning-Algorithmus trainieren, um ein Datenmodell zum sicheren Identifizieren der unterschiedlichen Aktivitäten im Synthetic-Sensor-Umfeld zu erzeugen. Bild: Carnegie Mellon University, Pittsburgh, USA .

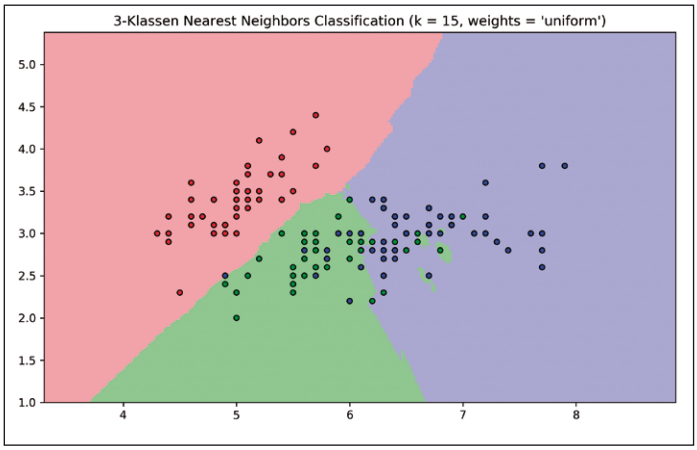


Bild 4: Beim maschinellen Lernen identifiziert ein Algorithmus anhand von Beispieldaten Muster und Regelmäßigkeiten, die dazu genutzt werden können, neue Daten zu klassifizieren, also an Hand ihrer Merkmalsausprägungen in bestimmte Klassen einzuteilen. Dabei kommen Methoden, wie beispielsweise die Nächste-Nachbarn-Klassifikation zum Einsatz, die Abstands- und Ähnlichkeitsmaße der einzelnen Merkmalsausprägungen miteinander vergleicht. Bild: SSV Software Systems

„Exposed Cyber Assets". Damit sind für Shodan und andere Angriffsziel-Suchmaschinen per Internet erreichbare Devices gemeint. Von Shodan gefunden zu werden bedeutet zwar nicht automatisch, dass es über einen möglichen DoS-Angriff hinaus auch weitere ausnutzbare Schwachstellen für potenzielle Cyberangreifer gibt. Ein möglicher Angreifer kann allerdings eine gefundene Device mit den entsprechenden Spezialwerkzeugen sehr genau untersuchen und an Hand der Reaktionen beispielsweise den Geräte- und Betriebssystemtyp bestimmen, um daraus Rückschlüsse auf bekannte Schwachstellen zu ziehen. Das reichte vor zwei Jahren bereits aus, um hunderttausende Telekom-Routern in das Mirai-Botnet zu integrieren und per Internet fernzusteuern.

Bei den Trend-Micro-Untersuchungen per Shodan sind den Security-Forschern offensichtlich auch ungeschützte Internet-Lautsprecher der namhaften Hersteller Sonos (Sonos Play:1, Sonus One) und Bose (SoundTouch) aufgefallen, die Cyberangreifern vielfältige Möglichkeiten bieten. In einem YouTube-Video von Trend Micro (siehe „The Sound of a Targeted Attack" unter https://bit.ly/2HCI0X1) und einer sehr ausführlichen Beschreibung (https://bit.ly/2vZILZ4) werden die Vorgehensweise, die ungeschützten Serviceschnittstellen sowie Hardware-Aspekte recht anschaulich dargestellt. Zahlreiche weitere Berichte im Internet, die die Trend-Micro-Erkenntnisse zu diesen Lautsprechern aufgreifen, beschreiben mögliche Angriffsszenarien bis hin zur missbräuchlichen Kommandoausgabe per Lautsprecher, um Alexa und Co. Befehle zu erteilen.

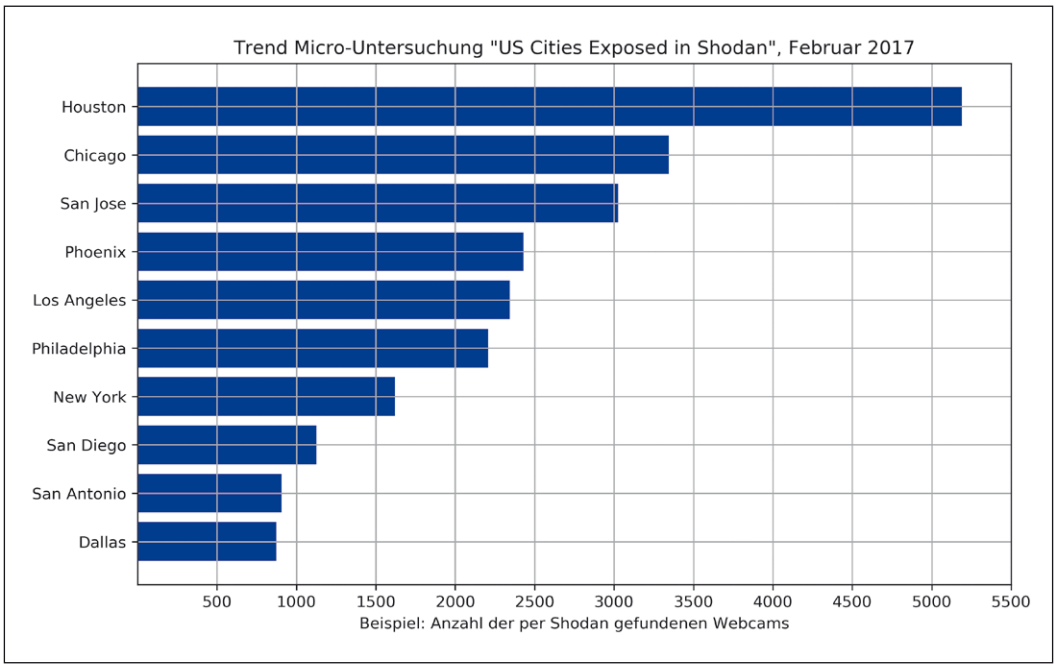


Bild 5: Durch das Internet der Dinge nimmt die Anzahl möglicher Angriffsziele rasant zu. Forscher des Unternehmens Trend Micro haben in bestimmten Regionen mit Hilfe der Computer- und Device-Suchmaschine Shodan gezielt nach per Internet erreichbaren Devices gesucht, die für potenzielle Cyberangreifer von Interesse sein könnten. Allein in den 10 größten US-Städten gibt es aus Trend-Micro-Sicht mehr als 178 Millionen sogenannter „Exposed Cyber Assets".

Wissenslücken

Die beiden Beispiele verdeutlichen auch, dass sich die Anforderungen an das Entwicklerfachwissen verlagern. Um einen Sensor mit Machine-Learning-Algorithmen zu kombinieren, wird fundiertes Data-Science-Wissen benötigt. Das fehlt beispielsweise in den meisten Entwicklungsabteilungen industrieller Kommunikationslösungen gegenwärtig nahezu vollständig bzw. befindet sich gerade in einer frühen Aufbauphase. Hinsichtlich der IT-Security ist der Wissensstand schon deutlich besser. Allerdings hapert es offensichtlich bei der Umsetzung des Fachwissens in entsprechende Produkteigenschaften.

Autor:
Klaus-Dieter Walter, CEO der SSV Software Systems GmbH
www.ssv-embedded.de