

Fehlende Standards bremsen das Internet der Dinge noch

Die Umsetzung des IoT steht erst am Anfang. Zwar überschlagen sich die Marktprognosen für die kommenden Jahre. Aber vor dem breiten Durchbruch sind einige Herausforderungen zu meistern.

DR. MIKE HEIDRICH *

Es ist mehr als ein Hype oder ein Buzzword: Das Internet der Dinge (Internet of Things, IoT) bezeichnet einen technischen Ansatz, der die Art, wie wir künftig leben und produzieren, grundlegend verändert. Die EU definiert das IoT als „die technische Vision, Objekte beliebiger Art in ein universales digitales Netz zu integrieren. Dabei haben die Objekte eine eindeutige Identität und befinden/bewegen sich in einem 'intelligenten' Umfeld.“ Im wissenschaftlichen Kontext findet die Definition von Rob van Kranenburg große Beachtung: Danach ist das IoT eine dynamische, weltweite Netzwerkinfrastruktur mit der Fähigkeit zur Selbst-Konfiguration, auf Basis von standardisierten und interoperablen Kommunikationsprotokollen. In dieser Infrastruktur haben physikalische und virtuelle Dinge – man muss inzwischen ergänzen: auch Services – Identitäten, physikalische Merkmale und virtuelle Persönlichkeiten. Diese Dinge verwenden intelligente Schnittstellen und sind nahtlos integriert in Informationssysteme.

Soweit die nüchterne Definition. Dagegen zeigt ein Blick auf die Einschätzungen großer Marktforschungsunternehmen die Dimension der Veränderung durch das IoT in nächster Zukunft: So prognostiziert Gartner, dass im Jahr 2020 25 Milliarden vernetzter Dinge in Gebrauch sein werden. Zum Vergleich: In diesem Jahr sollen es knapp fünf Milliarden sein. Das Marktvolumen des IoT, überwiegend bezogen auf Geräte, Konnektivität und IT-Services, schätzt IDC auf 1,7 Billionen US-Dollar im Jahr 2020. 2014 waren es noch 656 Milliarden. Das entspricht einer durchschnittlichen Wachstumsrate von 16,9 Prozent im Jahr.



* Dr. Mike Heidrich
... ist Leiter des Geschäftsfelds Industrial Communication am Fraunhofer-Institut für Eingebettete Systeme und Kommunikationstechnik ESK.



Bilder: Fraunhofer ESK

Digitalisierung in der Fertigung – ein Anwendungsfeld des Internets der Dinge: Das Fraunhofer ESK forscht mit Partnern im Bereich industrielle Vernetzung. Ein Beispiel ist das Projekt CICS, bei dem die Produktionssteuerung in der Cloud im Mittelpunkt steht.

Die rasante Entwicklung hat ihren Anfang eigentlich schon in den achtziger Jahren genommen, als die RFID-Technik (radio frequency identification) aufkam. RFID-Etiketten boten erstmals die Möglichkeit, physischen Dingen auf elektronischem Weg digitale Identitäten zu geben. RFID ist jedoch eine passive Technik ohne Eigenintelligenz.

Vom Funketikett zur Vier-Ebenen-Architektur

In den frühen 2000er Jahren kamen zu RFID die Sensornetze (WSN Wireless Sensor Networks) zur Vernetzung intelligenter Sensoren. Diese erfassen Parameter in der Umgebung, etwa Luftdruck, Temperatur bis hin zu Bild-/Kamerainformationen und können

erste Daten-Vorverarbeitungen übernehmen. Die Sensoren kommunizieren drahtlos und sind in der Lage, eigene Netzinfrastrukturen zu bilden. Beflügelt wurde diese Entwicklung durch die Entstehung und Ausbreitung drahtloser Kommunikationsstandards, insbesondere IEEE 802.15.4 (Low Data Rate Wireless PAN, darauf aufbauend z.B. ZigBee), IEEE 802.15.1 (High Data Rate Wireless PAN, darauf aufbauend Bluetooth) sowie IEEE 802.11 (Wireless LAN). Die Integration von Sensorik und RFID-Tags in IT-Systeme, die schnell in der Warenwirtschaft und der Logistik aufgegriffen wurde, stellt praktisch die Keimzelle des IoT dar.

Was sich aus diesen Anfängen entwickelt hat, veranschaulicht ein Blick auf die heuti-

ge Architektur des IoT. Li Da Xu schlägt in seinem Aufsatz „Internet of Things in Industries: A Survey“ ein Vier-Ebenen-Modell (Bild unten) vor: Der Sensing Layer mit der Anbindung von Sensoren und Tags bildet die Schnittstelle zur physikalischen Welt. Hier findet die Datenerfassung statt. Hier ist aber auch die Aktorik, also der Einfluss auf die physische Welt, angesiedelt. Auf dem Networking Layer erfolgt die Vernetzung von Sensor- und Aktorsystemen.

Dies geschieht in der Regel drahtlos, allerdings werden Backbone-Netze oft über Leitungen eingebunden. Der Service Layer ist der Ort virtueller Services, die auf Dienstplattformen erzeugt und verwaltet werden wie etwa Suchmaschinen für physische Dinge. Diese Services dienen zur Erfüllung spezifischer Aufgaben, etwa Wartungsunterstützung über den gesamten Lebenszyklus. Zuletzt erlaubt der Interface Layer als Schnittstelle die Interaktion von Mensch und IoT.

Am deutlichsten wird die letztgenannte Ebene der Betrachtung im Gesundheitswesen. Hier kann das IoT die Patientenversorgung verbessern und für alle Beteiligten vereinfachen. Ein Beispiel dafür ist die Überwachung wichtiger Körperfunktionen über Sensoren und die Übertragung der Daten an Ärzte und Krankenhäuser, die wiederum angemessen reagieren können.

PRAXIS WERT

Zukunftschance für Deutschland

Das IoT ist insgesamt noch auf dem Weg zur etablierten Technologie. Es entwickelt sich gerade, und die ersten optimistischen bis euphorischen Erwartungen sind einer praxisnahen Sichtweise gewichen. Das heißt: Technologische Herausforderungen müssen bewältigt und mit der konzeptionellen Weiterentwicklung des IoT in Einklang gebracht werden.

IoT als Herausforderung

Unternehmen, die hier vorne mit dabei sind, unterstreichen ihren Anspruch auf einen internationalen Spitzenplatz in den kommenden Jahrzehnten. Deshalb sollte gerade Deutschland mit seinen weltweit führenden Branchen Automobil- und Maschinenbau alles daran setzen, zu den Trendsettern und wissenschaftlichen Vorreitern des IoT zu gehören.

EMTRON

A FORTEC GROUP MEMBER



LED Netzteile



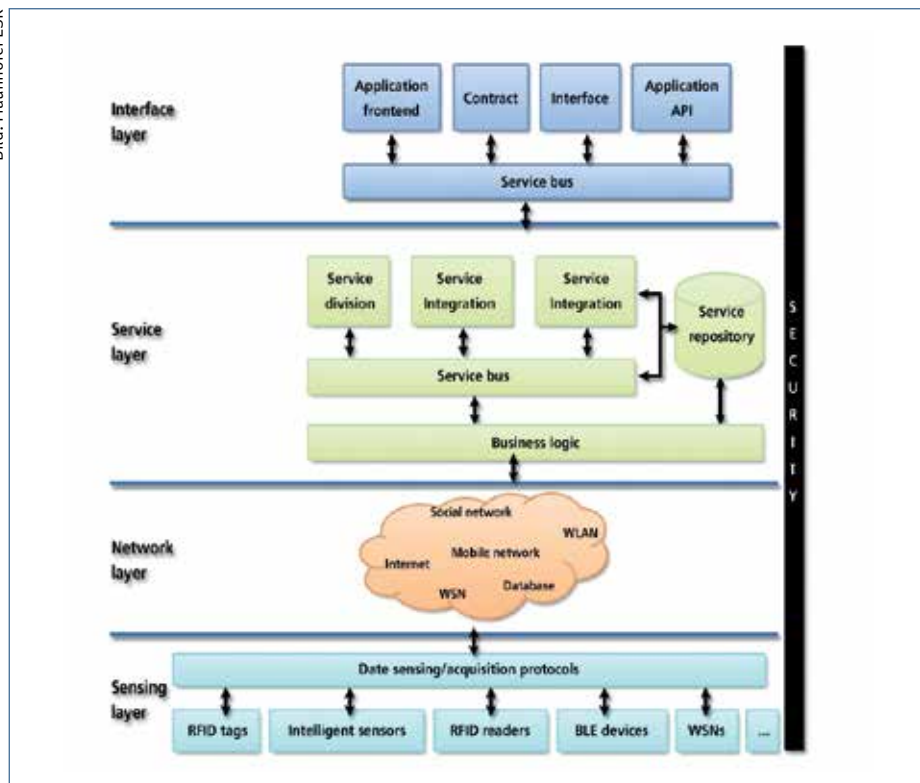
DIN Hutschienennetzteile



PFC Schaltnetzteile

www.emtron.de

Bild: Fraunhofer ESK



Vier-Schichten-Architektur: Möglicher Aufbau einer industrienahen IoT-Architektur nach Xu, *Internet of Things in Industries: A Survey*, 2014

Tages-Newsletter

die Nachrichten der letzten 24 Stunden

Jetzt

anmelden

ELEKTRONIK
PRAXIS

www.elektronikpraxis.de/newsletter



LIQUID CRYSTALS
als Folien und
Thermometer

www.celsi.com
Kostenlose Muster
auf Anfrage an
celsi@spirig.com

SPIRIG

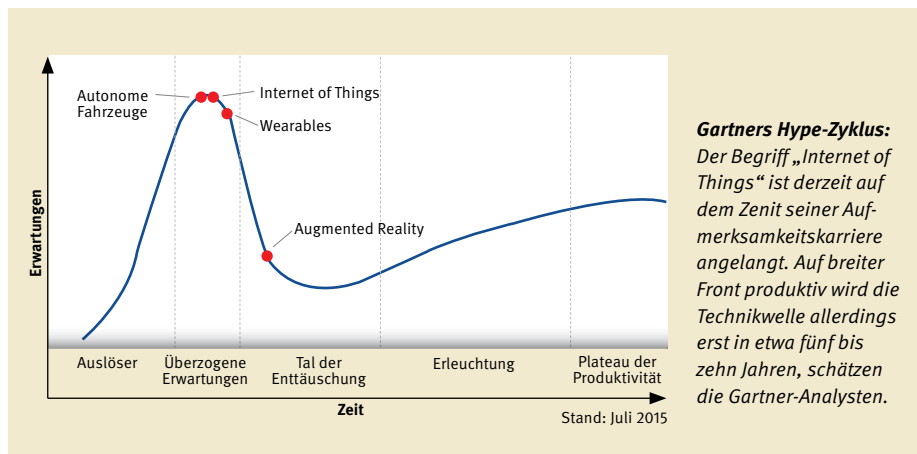


Bild: Gartner

lange gespeichert werden, wie es zur Erfüllung dieser Zwecke unbedingt nötig erscheint. Hier ist dringender technischer und juristischer Forschungsbedarf gegeben, zumal das Bundesverfassungsgericht 1983 in seinem „Volkszählungsurteil“ das Recht auf informationelle Selbstbestimmung als Grundrecht in Deutschland anerkannt hat.

Ein ähnliches Bild ergibt sich aus dem Blickwinkel der Datensicherheit: Die Komponenten sind lange Zeit unbewacht, die Kommunikation erfolgt über Funk und die Sensoren und Funketiketten haben nicht die Kapazität, komplexere Sicherheitssysteme zu unterstützen. So genügt etwa die Passwortlänge, die von den meisten Funketiketten unterstützt wird, nicht den Sicherheitsanforderungen, wie Atzori schon in seinem 2010 erschienen Aufsatz „The Internet of Things: A survey“ erläutert.

Künstliche Intelligenz wird IoT langfristig prägen

Während Forschung und Industrie danach streben, diese Herausforderungen in den Griff zu bekommen, entwickeln sich Konzepte und Ansätze des IoT weiter, die dann wieder in neue Anforderungen münden. Ein solcher Trend ist die Integration sozialer Netzwerke in IoT-Lösungen. Der Leitgedanke dabei ist, die Kommunikation zwischen den Dingen im IoT zu verbessern. Demnach können Social Media dafür sorgen, dass IoT-Objekte zu Akteuren und Peers im Internet werden. Auch das Thema Energiesparen wird bei der Entwicklung von IoT-Endgeräten wie Sensoren in den Vordergrund treten.

Ebenso wenig kann sich das IoT dem Vormarsch der künstlichen Intelligenz entziehen. Forderungen, das IoT zum Internet der intelligenten Dinge weiter zu entwickeln, werden in der Wissenschaft bereits erhoben. Intelligenz in Dingen und Kommunikationsnetzen bedeutet Selbst-Konfiguration, Selbst-Optimierung, Selbstschutz und Selbstheilung. Intelligenz heißt auch: Umgebungsentelligenz oder Kontextbewusstsein. Gerade im IoT mit Milliarden von Sensoren ist es unabdingbar, dass Systeme, vor allem Middleware-Systeme, die anfallenden Daten besser verstehen und die Entscheidung unterstützen, welche Daten weiterverarbeitet werden müssen. Und auch im IoT wird die Cloud zu neuen Ansätzen führen. Dass sich Dinge und Systeme darüber vernetzen, ist nicht neu. Wohl aber der Ansatz, über die Cloud IoT-Dienste anzubieten, so etwa „Sensing as a Service“, wie es Xu nennt. // FG

Fraunhofer ESK
+49(0)89 5470880

Auch im Bereich der Lebensmittelversorgung schafft das IoT mehr Qualität beim Endverbraucher. Hier erlauben vernetzte Sensoren die Kontrolle der Lebensmittel – von der Produktion über Transport und Lagerung bis zur Auslieferung an den Kunden.

Sein Optimierungspotenzial entfaltet das IoT ganz besonders in der Fertigungsbranche, wo es in Deutschland im Zusammenhang mit Industrie 4.0 diskutiert wird. Das zeigen beispielhaft die Daten des Telekommunikationsanbieters Verizon: Um jährlich 204 Prozent steigt demnach die Anzahl der IoT-Verbindungen im produzierenden Sektor. Dabei spielt die Möglichkeit, Produktion und Produktionsbedingungen wie Vibrationen, Temperatur oder Druck für eine verbesserte Wartung und Instandhaltung über vernetzte Sensoren und Aktuatoren zu überwachen, eine große Rolle. Das senkt die Kosten, weil weniger Vorort-Einsätze von Servicetechnikern anfallen und so Personal anderweitig eingesetzt werden kann. Die Produktion wird aber auch flexibler, weil sich etwa Neuerungen im Design sehr viel schneller in den Herstellungsprozess integrieren lassen. Das gleiche gilt für kundenindividuelle Anpassungen. Die Produktionsverantwortlichen haben auch die Möglichkeit, sich dank der IoT-Technik auf ihrem Tablet einen aktuellen Überblick über Rohstoffvorrat und Lagerhaltung zu verschaffen. Die Unternehmensberatung McKinsey beziffert den wirtschaftlichen Mehrwert durch das IoT in der Fertigung auf 3,7 Billionen Dollar bis 2025.

Damit das IoT sein Potenzial in den diversen Lebensbereichen und Branchen voll entfalten kann, müssen eine Reihe von technischen Herausforderungen bewältigt werden. Das gilt zuallererst für das große Thema Standardisierung. Xu weist in seinem Aufsatz zu Recht darauf hin, dass die Standardisierung eine wichtige Rolle für die weitere Entwicklung und Verbreitung des IoT spielt.

Beispiele für solche Standards sind Sicherheits-, Identifikations- und Kommunikationsstandards. So bezeichnet etwa das Kürzel 6Lowpan („IPv6 over Low-Power Wireless Personal Area Networks“) Bestrebungen, einen Standard für Nahbereichsfunknetze speziell für das IoT zu schaffen. Darum kümmert sich eine Arbeitsgruppe der Internet Engineering Task Force (IETF). Das Internet Protocol Version 6 hat nämlich den Vorteil, dass eine riesige Menge an Smart Objects, theoretisch 2¹²⁸, mit einer eigenen IP-Adresse versehen und angesprochen werden können. Mit 6Lowpan wird also die Basis dafür gelegt, drahtlose Sensornetzwerke mit dem Internet zu verbinden. Im Gegensatz dazu beschreiten Kommunikationstechnik-Anbieter einen anderen Weg, indem sie Mobilfunk als Plattform für das IoT etablieren wollen. Dies zeigen etwa die Entwicklungen zum Mobilfunk der fünften Generation (5G).

Standardisierung, Datenschutz und Datensicherheit

Die zweite große Herausforderung kann mit den Begriffen Datenschutz und Datensicherheit beschrieben werden. Das Problembewusstsein dafür im Zusammenhang mit dem Internet der Dinge ist sowohl in Wirtschaft und Wissenschaft als auch bei den Verbrauchern sehr ausgeprägt. Ein Beispiel: die Ankündigung des Bekleidungsherstellers Benetton, seine Kleidungsstücke mit insgesamt 15 Millionen Funketiketten auszustatten. Die Folgen waren massive Kritik bis hin zu Boykottaufrufen im Netz. Zweifellos stellt der Datenschutz ein Problem dar im IoT. Hier lautet der Anspruch, dass der Einzelne die Kontrolle darüber haben muss, welche persönlichen Daten gesammelt werden, wer sie sammelt und wann das geschieht. Zudem sollten die Daten nur für bestimmte Zwecke durch die dafür autorisierten Stellen erfasst werden. Und zuletzt sollten die Daten nur so