Was steckt hinter dem Internet der Dinge?

Alles neu oder doch nur Embedded Business as usual?

Dipl.-Ing. Günter Obiltschnig
Applied Informatics Software Engineering GmbH
Maria Elend 143
9182 Maria Elend
Austria
guenter.obiltschnig@appinf.com

Das Internet der Dinge (Internet of Things, kurz IoT) ist derzeit das Trendthema schlechthin. Doch was steckt dahinter? Sind es doch nur netzwerkfähige Embedded Systeme oder steckt doch mehr dahinter? Dieser Artikel vermittelt die wichtigsten Grundlage, Begriffe und Technologien zum Internet der Dinge und gibt Antworten auf folgende Fragen: Wie unterscheiden sich "Dinge" von normalen Embedded Systemen? Welche neuen Technologien sind für das Internet der Dinge relevant? Was braucht man neben Embedded Systemen noch, um das Internet der Dinge zu realisieren? Wie sieht eine typische Architektur eines IoT Systems aus? Wie steht es um die Sicherheit? Welche neuen Geschäftsmodelle werden möglich?

Das Internet der Dinge (englisch: Internet of Things, kurz IoT) und die damit verbundenen Begriffe Cyber-Physical Systems, Industrie 4.0 und Industrial Internet sind derzeit in aller Munde. Doch was steckt dahinter? Laut Wikipedia ist das Internet der Dinge "das Netzwerk physikalischer Objekte oder 'Dinge' mit eingebetteter Elektronik, Software, Sensoren und Konnektivität, welches Wertschöpfung und neue Dienste ermöglicht, in dem Daten mit dem Hersteller, Betreiber, oder anderen verbundenen Geräten ausgetauscht werden. Jedes 'Ding' ist durch das eingebaute Computersystem eindeutig identifizierbar und kann mit der existierenden Internet Infrastruktur zusammenarbeiten."

Der Begriff "Internet der Dinge" wurde erstmals 1999 vom Briten Kevin Ashton im Zusammenhang mit RFID Technologie (Funktechnologie zur berührungslosen Identifikation von Objekten) dokumentiert. Die Idee war, physikalische Objekte mit einem RFID Transponder zu versehen, um sie so eindeutig elektronisch identifizierbar zu machen. Jedes physikalische Objekt sollte praktisch ein Gegenstück im „Cyberspace" haben wobei die Verbindung zwischen realer und virtueller Instanz über einen eindeutigen Code, z. B. in Form einer URL, erfolgt.

Nachdem der anfängliche Hype um RFID am Anfang des vorherigen Jahrzehnts bald wieder abflaute verschwand der Begriff „Internet der Dinge" für einige Zeit in der Versenkung bis er Anfang dieses Jahrzehnts in neuer Bedeutung wieder auftauchte.

Dinge, Kommunikation und Computer

Was steckt nun hinter dem Internet der Dinge? Zunächst einmal braucht man „Dinge“, also vernetzte „Smarte Produkte“ und andere Gegenstände, welche ein Computersystem (Microcontroller), Sensoren und Software mit Kommunikationstechnik kombinieren. Weiters benötigt man Kommunikationsinfrastruktur, welche Dinge mit dem Internet verbindet. Das beinhaltet energiesparende drahtlose PANs (Personal Area Networks) wie z. B. ZigBee oder Bluetooth, lokale Netzwerke (WLAN, Ethernet), bis hin zu weitläufigen Breitbandnetzwerken (ADSL, UMTS, 4G). Schlussendlich benötigt man eine leistungsfähige Computerinfrastruktur, um alle angebundenen Dinge zu verwalten, sowie um die anfallenden Daten zu verarbeiten. Gerade erst durch die Verarbeitung aller in massiver Form anfallenden Daten – Stichwort „Big Data“ – durch neuartige Datenerfassungs- und Analyse-Software ergeben sich neue Arten der Wertschöpfung, bzw. neue Geschäftsideen.

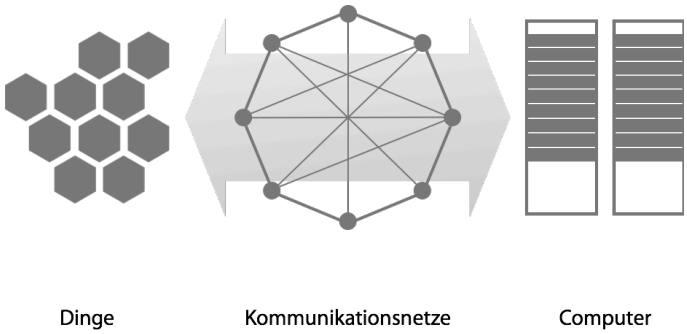

Abbildung 1: Das Internet der Dinge: Dinge, Kommunikationsnetze, Computer

Das Internet der Dinge ist die logische Fortführung einer Entwicklung, die mit der weitläufigen Verbreitung des Internets Mitte der 1990er Jahre begann. Mit der Verfügbarkeit des iPhone und anderer Smart Phones ab 2007, sowie entsprechender Entwicklungen im Mobilfunkbereich machte das Internet den Schritt von örtlich gebundener Verfügbarkeit (PC) hin zu ständiger, mobiler Verfügbarkeit, allerdings immer noch beschränkt auf spezielle Endgeräte (Smart Phones, Tablets). Das Internet der Dinge schlussendlich integriert das Internet in Dinge, bzw. Geräte und Maschinen des alltäglichen Gebrauchs und macht es somit unabhängig von speziellen Endgeräten.

Industrial Internet und Industrie 4.0

Industrial Internet bezeichnet die Anwendung von IoT Technologien im Bereich der Industrie wobei mit Industrie in diesem Zusammenhang nicht nur die industrielle Fertigung gemeint ist sondern alles was nicht in den Konsumbereich fällt. Somit fallen neben herkömmlicher Automatisierungstechnik auch die Bereiche Medizintechnik, Gebäudetechnik, Smart Grid, Logistik, usw. unter Industrial Internet. Der Begriff ist somit nicht direkt mit dem in Deutschland geprägten Industrie 4.0 vergleichbar, welcher einen wesentlich engeren Bezug zur industriellen Produktion, insbesondere der Optimierung des Fertigungsprozesses bis zur theoretischen Losgröße 1 mit Hilfe von neuen Technologien, hat, quasi die 4. Industrielle Revolution. Generell leidet der Begriff Industrie 4.0 darunter, stark politisch vereinnahmt zu sein und hauptsächlich Arbeitsgruppen und viel Papier zu produzieren. Einen pragmatischeren Weg geht das US-lastige, aber mittlerweile

international besetzte Industrial Internet Consortium, welches konkret an Testbeds und Quasi-Standards arbeitet.

Um auch gleich ein mögliches Missverständnis auszuräumen: Industrial Internet, bzw. Industrie 4.0 bedeutet nicht, jetzt quasi die gesamte Fertigung „ans Internet zu hängen“. Vielmehr ist die Nutzung von Internet-Technologien gemeint, die sehr wohl auch in einem vom offenen Internet möglichst gut abgesicherten Firmennetz erfolgen kann. Ziel ist dabei eine verbesserte Integration der Automatisierungsebene und des entstehenden Produktes untereinander, sowie mit den IT Systemen (z. B. ERP und CRM) des Unternehmens (über den gesamten Lebenszyklus des Produktes).

Hohe Erwartungen, große Herausforderungen

Betrachtet man diverse Marktstudien zum Thema IoT wird man zwangsläufig mit gigantischen Fantasiezahlen überschüttet. Je nach Studie erwartet man für 2020 zwischen 5 und 50 Milliarden „connected devices“. In wie weit sich diese Prognosen bewahrheiten werden sei dahingestellt. Was jedoch mit Sicherheit gesagt werden kann ist, dass die Konzepte hinter IoT bleiben werden, auch wenn der Begriff IoT in ein paar Jahren vielleicht durch einen neuen Marketingbegriff abgelöst werden wird.

Aus technischer Sicht ist zu erwähnen, dass alle für das IoT notwendigen Technologien bereits verfügbar sind. Das IoT ist somit kein vornehmlich technisches Problem mehr. Die eigentliche Herausforderung ist die vollständige Umstrukturierung von Geschäftsmodellen und Geschäftsprozessen, welche Unternehmen meistern werden müssen.

Neue Geschäftsmodelle

Am Beispiel eines Herstellers von Hygieneprodukten (Seifen- und Handtuchspender, etc.) ist ersichtlich, wie ein solcher Transformationsprozess eines Geschäftsmodells aussehen kann. Das Unternehmen hat damit begonnen, Seifen- und Papierspender mit Sensoren und Funkmodulen auszustatten, welche Füllstands- und Nutzungsdaten über eine Basisstation an einen Server des Unternehmens senden. Dies hilft dem lokalen Facility Management schon einmal dafür zu sorgen, dass leere Seifen, bzw. Papierspender der Vergangenheit angehören. In Kombination mit einem ebenso eingebundenen Besucherzähler lassen sich weiters interessante Daten ableiten. So weiß das Unternehmen dank einer recht großen Datenbasis mittlerweile sehr genau, wie viel ein Toilettenbesuch im Endeffekt kostet. Dies wiederum ermöglicht eine komplette Umstellung des Geschäftsmodells. Anstatt Handtücher und Seife zu verkaufen, und sich dabei mit möglichen billigeren Alternativanbietern konkurrieren zu müssen, verrechnet das Unternehmen nur mehr die Anzahl der Toilettenbesuche. Dies ist einerseits für den Kunden bequemer, da einfacher zu kalkulieren, und der Kunde sich nicht mehr um die rechtzeitige Nachbestellung des Verbrauchsmaterials kümmern muss. Andererseits verschafft sich das Unternehmen natürlich einen Vorteil gegenüber möglichen Konkurrenten, die diese Art der Kundenbetreuung und Kundenbindung gar nicht bieten können.

Im gerade angeführten Beispiel ist eine deutliche Verschiebung des Geschäftsmodells vom Produktverkauf (Seife, Papiertücher) zur Dienstleistung (Toilettenbesuch) zu erkennen. Diese Verschiebung ist bezeichnend für das Internet der Dinge. Besonders hervorgehoben werden muss in diesem Zusammenhang die Bedeutung von Software. Vom der Firmware im Seifenspender, über die

Basisstation, bis hin zur Unternehmenssoftware welche die gesamte Logistik von der automatischen Nachbestellung bis zur Lieferung steuert, sowie die anfallenden Daten auswertet (Business Intelligence), Software überall.

Technische Aspekte

Betrachten wir nun das Internet der Dinge von der technischen Seite. In den letzten Jahren entstand eine Vielzahl neuer Technologien welche verschiedene Aspekte, bzw. verschiedene Ebenen des IoT abdecken. Eine typische Referenzarchitektur für ein IoT System besteht aus folgenden Komponenten: Sensoren, bzw. Aktoren welche z. B. über ein drahtloses Sensornetzwerk mit einem IoT Gateway (auch Basisstation genannt) verbunden sind. Dieser IoT Gateway hat die Aufgabe, mit den angeschlossenen Sensoren, bzw. Aktoren zu kommunizieren, und in weiterer Folge die Verbindung zur nächst höheren Ebene, oft als „Cloud“ bezeichnet, herzustellen. In der Cloud wiederum laufen all jene Applikationen, welche die anfallenden Daten auswerten und in die Geschäftsprozesse des Unternehmens integrieren. Ob diese Applikationen jetzt auf einem „public“ Cloud Service im Internet laufen, oder im privaten Rechenzentrum ("private" Cloud) eines Unternehmens ist hier zweitrangig, da die Kommunikation in beiden Fällen gleich abläuft. Security-Aspekte, insbesondere verschlüsselte Kommunikation und Datenschutz, sind aber unbedingt zu berücksichtigen. Diese Architektur ist natürlich nicht in Stein gemeißelt. So können die Rollen von IoT Gateway und Sensor/Aktor vom selben Gerät übernommen werden. Der Kommunikationsfluss ist in beide Richtungen möglich. Dinge können Informationen aus der Cloud beziehen und auch lokal untereinander, ohne Umweg über die Cloud, kommunizieren.

Unternehmens-IT, Cloud, Big Data	Intel Xeon, SPARC	Linux, Solaris, Windows Server
Internet (LAN, WAN)	Ethernet, Wi-Fi, xDSL, UMTS/HSPA/LTE	MQTT, HTTP, REST, SOAP, Web Services
IoT Gateway	ARM 9, Cortex A8/9, Intel Quark/Atom	Linux, Windows Embedded
Sensor Netzwerk	IEEE 802.15.4, Wi-Fi, Bluetooth, Enocean	ZigBee, Z-Wave, 6LoWPAN, CoAP, LWM2M, Thread
Sensor, Aktor, “Thing”	Atmel AVR ARM Cortex M	Contiki, Tiny OS, RIOT, mbed

Abbildung 2: Der „IoT Technology Stack“

Sensoren und Aktoren

Beginnen wir bei den kleinsten Geräten, typischerweise Sensoren oder Aktoren, welche über ein sogenanntes Sensornetzwerk miteinander, sowie mit einem IoT Gateway (Basisstation), verbunden sind. Diese Devices basieren üblicherweise auf einem kleinen 8, 16 oder 32-bit Microcontroller wie einem Atmel AVR oder einem ARM Cortex M. Zur Vernetzung kommt ein typischerweise auf IEEE 802.15.4-basiertes Funknetzwerk zum Einsatz. Für diese Devices wurden eine Reihe von kleinen, spezialisierten Betriebssystemen entwickelt, wie z. B. Contiki, Tiny OS, RIOT oder mbed. Diesen Betriebssystemen ist gemeinsam, dass sie von Grund auf

für Vernetzung, als auch Energieeffizienz ausgelegt sind. 6LoWPAN und CoAP dürften sich hier als Standard-Netzwerkprotokolle zu etablieren, da diese Protokolle offen und frei verfügbar sind. Technologien wie ZigBee, Z-Wave, Bluetooth, Enocean, aber auch schon Wi-Fi kommen hier ebenfalls zum Einsatz. Gerade im Industriebereich sind hier aber auch Feldbussysteme anzutreffen, OPC-UA und DDS sind ebenso von Bedeutung.

IoT Gateway als Vermittler

Der IoT Gateway stellt das Bindeglied zwischen den kleinen Devices, den Sensornetzwerken und der Internet-Welt dar. IoT Gateways sind oft Linux-basierte Geräte mit leistungsfähigen ARM Cortex A oder Intel Quark/Atom CPUs. Verschiedene Netzwerkschnittstellen sorgen für Konnektivität, ein UMTS/4 G Modul für mobilen Internetzugang kann integriert sein. Neben Ihrer Funktion als Übersetzer und Vermittler zwischen Sensor und Cloud/IT-Welt können Gateways ebenso komplexere Applikationen ausführen. Beispiele sind die Filterung, Vorverarbeitung und Protokollierung von Sensordaten, (unkritische) Steuerungsaufgaben, Alarmierungen per SMS oder E-Mail, Visualisierungen von Anlagenzuständen über eine Webseite, usw. Der sichere Fernzugriff über VPN oder Relay Services wie my-devices.net ist ebenso hier angesiedelt. Schlussendlich ist es jedoch meistens das Ziel, die erfassten Daten an einen Server weiterzusenden, wo sie dann in einer Datenbank gespeichert, mit anderen Daten kombiniert und analysiert werden. Zur Kommunikation zwischen Gateway und Server haben sich zwei Protokolle etabliert. Zunächst einmal werden HTTP/REST Web Services verwendet, die sich im Internet-Bereich weitgehend als Standard etabliert haben. Ausgezeichnet für das Internet der Dinge eignet sich allerdings das MQTT Protokoll.

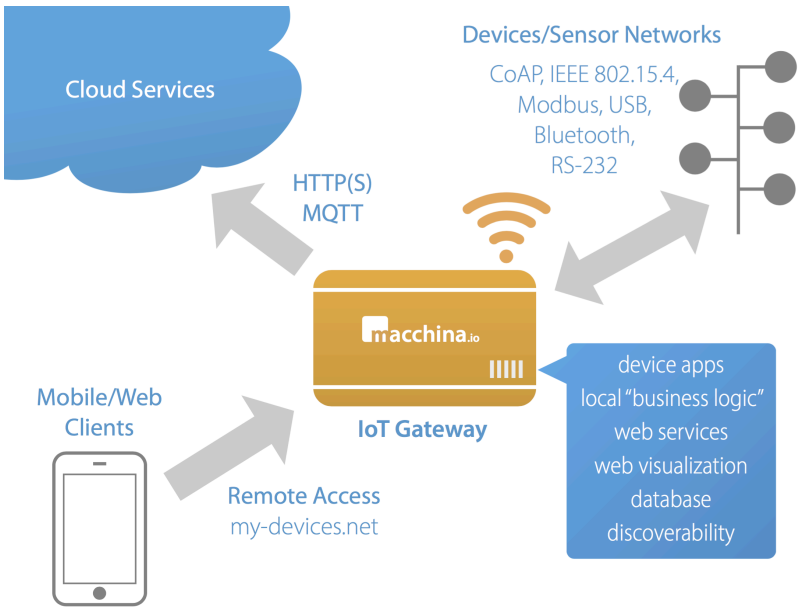

Abbildung 3: Typische Architektur eines IoT Systems

Obwohl bereits seit 1999 entwickelt erfreut es sich erst jetzt großer Beliebtheit. Ein Grund dafür ist einerseits die Effizienz, speziell im Vergleich zu HTTP. Andererseits ist MQTT sehr robust, was gerade im Fall schlechter Verbindungen (z. B. mobiles Internet) ein Vorteil ist. MQTT ist auf die Übertragung von Telemetriedaten

optimiert, was sich auch im Namen – Message Queueing Telemetry Transport – widerspiegelt. Eine spezielle Eigenschaft von MQTT ist, dass Sender und Empfänger einer Nachricht nicht direkt miteinander kommunizieren. Die Kommunikation läuft immer über einen sogenannten Broker, nach dem Publish-Subscribe Verfahren. Das heißt, ein Gerät oder eine Applikation welche Nachrichten senden möchte, sendet diese unter einem sogenannten „Topic“, ein hierarchisch aufgebauter Name. Geräte, bzw. Applikationen welche Daten empfangen möchten geben jene Topics an, zu denen sie Nachrichten empfangen möchten. Es ist dann Aufgabe des Brokers, alle Nachrichten den jeweils interessierten Empfängern zuzustellen. Jeder Teilnehmer (im MQTT Jargon „Client“) kann gleichzeitig Sender und Empfänger sein. Der MQTT Broker ist für die Authentifizierung und Autorisierung der Clients verantwortlich, und die Kommunikation erfolgt üblicherweise verschlüsselt (SSL/TLS), so dass auch ein hohes Maß an Datensicherheit erreicht werden kann. Ein wichtiger Grund für die Beliebtheit von MQTT ist die Verfügbarkeit qualitativ hochwertiger Open Source Implementierungen für eine Vielzahl von Plattformen.

Schneller Einstieg ins Internet der Dinge

Dank kostengünstiger Hardware wie Raspberry Pi und frei verfügbarer Open Source Software ist für experimentier- und spielfreudige Techniker ein Einstieg recht schnell möglich. So bietet z. B. das deutsche Unternehmen Tinkerforge diverse Sensoren und Aktoren an, die über USB einfach mit einem PC oder Kleincomputer, wie z. B. einem Raspberry Pi oder BeagleBone, der als IoT Gateway fungiert, verbunden werden können. Als Software für den IoT Gateway bietet sich das Open Source Projekt *macchina.io* an. Damit kann eine Applikation für Linux-basierte IoT Gateways in JavaScript entwickelt werden. Programmierschnittstellen zum Zugriff auf verschiedenste Sensoren, als auch Cloud Dienste ermöglichen rasche Erfolgserlebnisse.

Zusammenfassung

Zusammenfassend ist zu sagen, dass das Internet der Dinge keine ferne Zukunftsvision ist, sondern von den ersten Unternehmen bereits gewinnbringend eingesetzt wird. Dazu ist neben der Einführung neuer Technologien jedoch vor allem ein Umdenken auf Geschäftsprozessebene erforderlich. Der Einstieg in die neuen Technologien ist dank kostengünstiger Hardware und Open Source Software recht einfach zu schaffen.

Der Autor

Günter Obiltschnig ist Gründer der Open Source Projekte POCO C++ Libraries und macchina.io, IoT Consultant sowie Gründer und kreativer Kopf der Applied Informatics Software Engineering GmbH.