Trend Guide

INTERNET OF THINGS

Internet of Things

MicroConsult

Inhalt

Vorbemerkung/ Worum es geht 3
Orientierung im Begriffswirrwarr 4
IoT: Brutstätte neuer Chancen und Risiken 6
Industrie 4.0 revolutioniert die Wertschöpfung 6
Infrastrukturen, Produkte und Dienstleistungen 8
Sicherheit: Datenklau in der Cloud 10
Manipulation der Daten könnte verheerende Auswirkungen haben 11
Digitale Ökosysteme 12
Die Weltsprache für die Vernetzung 13
Geschäftsmodelle, Wertschöpfung und Wettbewerb 14
Das Internet of Things unternehmerisch nutzen 15
Knowhow für IoT 16
Flexibilität ist Trumpf 16
Learning by Doing 17
Nicht zu vergessen: Softskills 18
Fazit 18
Anhang: Weiterbildung zum Thema Embedded Software Engineering 20
Anhang: Literaturhinweise, Quellen 21
Anhang: Autoren, Impressum 22

Vorbemerkung

Wenn wir gewusst hätten, was wir uns antun, wenn wir etwas zum Thema Internet of Things (IoT) schreiben, hätten wir es vielleicht doch lieber gelassen. Es ist - wie das Internet - nicht nur ein bodenloses Loch, sondern es ist auch schwer, den Rand dieses Lochs zu erkennen. Man hat das Gefühl, man greift ein Thema auf und die ganze Welt hängt dran: Technik, Gesellschaft, Umwelt, Politik …. Die Globalisierung lässt grüßen. Auf den folgenden Seiten haben wir versucht, einerseits die Dimensionen dieses Themas zu umreißen und andererseits konkret zu fassen, was IoT im Kern für all diejenigen bedeutet, die Software entwickeln. Aus unserer Sicht stellt dieser Trend Guide einen Spagat dar, den jeder vollführt, der sich an dieses Thema heranwagt oder einfach so hineingeraten ist. Dahinter steckt letztlich eine entscheidende Frage: Wie schaffe ich es, im Universum des IoT meine konkreten Chancen zu entdecken und in die Tat umzusetzen?

Worum es geht

Internet of Things, Industrie 4.0, Cyber Physical Systems – Schlagworte, die uns mittlerweile oft begegnen, doch wird nur selten erläutert, was damit gemeint ist. Und wer versucht, sich zu informieren, stellt schnell fest, dass man den Wortschatz eines Digital Native braucht, um einen Text verstehen oder einem Gespräch folgen zu können. Ist alles nur ein Hype, eine Blase, die mit heißer Luft gefüllt ist? Wir denken, eher nicht. Die Begriffe beschreiben weniger eine neue Technologie, sondern vielmehr einen Trend, dessen Inhalt mehr in der Zukunft als in der Vergangenheit liegt. Will heißen – es ist hier erst wenig passiert, aber es ist noch sehr viel zu erwarten.

Das Internet of Things, Internet der Dinge, verspricht ziemlich viel. In zahlreichen Publikationen, Vorträgen und Seminaren wird ausführlich darüber diskutiert, wie wir von den aktuellen Entwicklungen profitieren. Alles soll einfacher, klarer, transparenter, effizienter und vor allem bequemer werden. Wir stehen mitten in der Entwicklung, die evolutionäre Züge hat und revolutionäre Züge annehmen kann.

Viel Spaß bei der Lektüre unseres Trend Guides!

Orientierung im Begriffswirrwarr

Die zugrunde liegende technische Entwicklung, die für das Aufkommen von Cyber Physical Systems, von Industrie 4.0 und des Internet of Things erforderlich war, ist eine leistungsfähige, technische Infrastruktur basierend auf bezahlbaren Internetverbindungen mit großer Bandbreite und der Möglichkeit, eine große Anzahl von Geräten zu adressieren. Dazu kommen noch Technologien, die Rechenleistung, Datenspeicher, Sensorik und Aktorik immer kompakter, energieeffizienter und kostengünstiger bereitstellen. Im Zusammenspiel mit immer effektiveren Energiespeichern eröffnen sich auf diese Weise ständig neue mobile Anwendungsmöglichkeiten. IoT erweitert das Prinzip vernetzter intelligenter Systeme konsequent auf immer neue Anwendungsfelder.

Die Entstehung des Internet of Things in seinen Varianten wurde überhaupt erst ermöglicht durch die Umstellung der IP-Adressen vom IPv4-System auf das hexadezimale System IPv6. Konnten mit IPv4 rund 4 Milliarden eindeutige Adressen für Netzwerkteilnehmer erzeugt werden, so sind es mit IPv6 rund 340 Sextillionen; eine unvorstellbar große Zahl mit 36 Nullen. Wie lange diese Menge ausreichen wird, kann heute niemand abschätzen, aber es wird wohl ein Weilchen dauern.

Hier die Zahl zum Ansehen: 340 000 000 000 000 000 000 000 000 000 000 000.

Im Zeitalter der vernetzten Dinge benötigt ja jedes Ding, also jeder Teilnehmer in einem Netzwerk, für die Kommunikation eine eigene und einmalige IP-Adresse. Daher war dieser Schritt einerseits unumgänglich und gleichzeitig eine Art Triggersignal für die Entstehung des IoT. Folgende Betrachtung, um die Möglichkeiten der IPv6-Bezeichnung zu veranschaulichen: Auf jedem Quadratmillimeter der gesamten Erdoberfläche (inklusive aller Seen und Ozeane) könnten damit mehrere tausend Adressen untergebracht werden, die eindeutig sind und kein zweites Mal vorkämen.

Daten sind das Gold von morgen.
Oliver Edinger, SAP

Definition und Abgrenzung der Begriffe

Der **Begriff Internet of Things** entzieht sich ziemlich gekonnt einer genauen Definition. Das IoT bedeutet alles und gleichzeitig auf gewisse Weise auch recht wenig. Dennoch lässt sich die Thematik einigermaßen eingrenzen und damit auch begreifbar machen.

Die nüchterne Definition sagt, dass im Internet of Things "Dinge" über das Internet miteinander kommunizieren, ohne dass der Mensch direkt tätig sein muss. Der Mensch wird im Wesentlichen dafür gebraucht, die Kommunikationswege der Dinge aufrechtzuerhalten. Das führt dazu, dass im Zusammenwirken von Mensch und Maschine die Rollen teilweise neu verteilt werden. Technische Systeme werden mehr und mehr zu Datensammlern und Dienstleistern. Menschen designen, optimieren und koordinieren diese Dienstleistungen mit Hilfe der Daten, die die Dinge liefern. Diese wiederum werden mit Hilfe hochentwickelter Algorithmen und leistungsfähiger IT genutzt, um aus Nutzerdaten Verhaltensmuster herauszufiltern. Diese werden schließlich zur Grundlage für neue Serviceangebote. Vereinfacht: Konsum führt zu neuen Angeboten, diese führen zu Konsum, diese wiederum zu neuen Angeboten, und so weiter.

Industrie 4.0 bezeichnet die derzeitige und andauernde 4. Industrielle Revolution, die aufgrund der durch das IoT zur Verfügung gestellten Möglichkeiten in Gang gekommen ist. Es ist sozusagen ein besonderer Anwendungsbereich des Internet of Things. Stichwörter wie Smart Manufacturing und Smart Fabrication gehören künftig vielleicht zum Standardvokabular in Industriebetrieben. Gemeint ist damit, dass beispielsweise Komponenten industrieller Fertigungssysteme über das Internet in Verbindung stehen, mit Steuerungssystemen, der Ersatzteilbeschaffung, dem Teilenachschub, der Produktionslogistik, ja mit den Produkten selbst.

Ziel ist es, wertvolle Produktionsressourcen optimal auszulasten und gleichzeitig individuelle Kundenwünsche in einem flexiblen Fertigungsprozess zu erfüllen. Mit anderen Worten: Es soll das Paradoxon hoher Effizienz bei hoher Flexibilität aufgelöst werden, indem sich Produktionsanlagen immer wieder neu an die Auftragssituation anpassen. Neben der Herausforderung, geeignete Algorithmen auf der koordinativen Ebene zu finden, stellt sich die Frage nach geeigneten und konsensfähigen Standards für die Maschine-Maschine-Kommunikation. Gleichzeitig werden Migrationsstrategien für bestehende Anlagen durch praktikable Schnittstellenlösungen dringend benötigt. Anspruchsvolle Aufgaben, die bis dato nur in Teilen gelöst sind. Und das Ende der Fahnenstange von Herausforderungen indes ist noch lange nicht erreicht.

Industrie 4.0 kann und sollte schrittweise eingeführt werden.

Prof. Dr.-Ing. Birgit Vogel-Heuser,
Technische Universität München

Niemand kann im Moment sagen, wie groß und welcher Gestalt dieser Einfluss auf unser Leben, die Gesellschaft, Wirtschaft und Politik sein wird. Ob das Internet of Everything (IoE) tatsächlich das ultimative Ziel ist, bleibt abzuwarten.

IoT: Brutstätte neuer Chancen und Risiken

In Literatur und Film werden immer wieder die nicht absehbaren Folgen einer zu intelligent und mithin zu selbstständig gewordenen Technik thematisiert. Das mag alles Fiktion sein, doch andererseits sind die Folgen solcher Entwicklungen heute nicht oder kaum absehbar.

60% des deutschen Mittelstandes haben sich mit Industrie 4.0 noch nicht beschäftigt.

Hans-Georg Krabbe, ABB

Viele technologische Erfolgsgeschichten und - leider auch - Katastrophen beruhen auf dem Evolutionsprinzip emergenter Eigenschaften. Es besagt, dass durch die Vernetzung von Einheiten zu einem System dieses System neue Eigenschaften und Fähigkeiten hervorbringt, die vorher noch nicht existierten und möglicherweise auch nicht vorhersehbar waren. Dies kann zu tiefgreifenden Veränderungen der Umgebungsbedingungen für alle führen, die mit diesem System direkt oder indirekt interagieren. Es kann Produkte, Branchen, Ökonomien verändern. Es beeinflusst das Verhältnis von Kunden und Lieferanten, die Verfügbarkeit von Waren und Dienstleistungen. Es kann einen Einfluss auf Gesellschaftssysteme und Ökosysteme, ja auf nahezu alles haben. Darin liegen Chancen und Gefahren. Emergente Eigenschaften neuer Systeme können zu tiefgreifenden Veränderungen führen und eine disruptive Wirkung entfalten. Es kann dann geschehen, dass vorhandene Technologien, Produkte, Methoden und Gewohnheiten in die Bedeutungslosigkeit zurückgedrängt werden.

Industrie 4.0 revolutioniert die Wertschöpfung

Industrie 4.0 ist eine vergleichsweise gut greifbare Dimension, die die Entwicklung hin zum IoT hervorgebracht hat. Der Einfluss auf die industrielle Produktion ist von größter ökonomischer Bedeutung und wird sowohl die Produktion als auch die Produkte selbst betreffen. Ebenso betroffen sind die Organisation von Unternehmen, deren Logistik und Vertrieb. Letztlich betrifft Industrie 4.0 alle, die der Wertschöpfungskette eines industriell gefertigten und vertriebenen Produkts angehören.

Die industrielle Produktion wird immer mehr mit vernetzten, miteinander kommunizierenden Anlagen und Komponenten erfolgen. Maschinen überwachen und

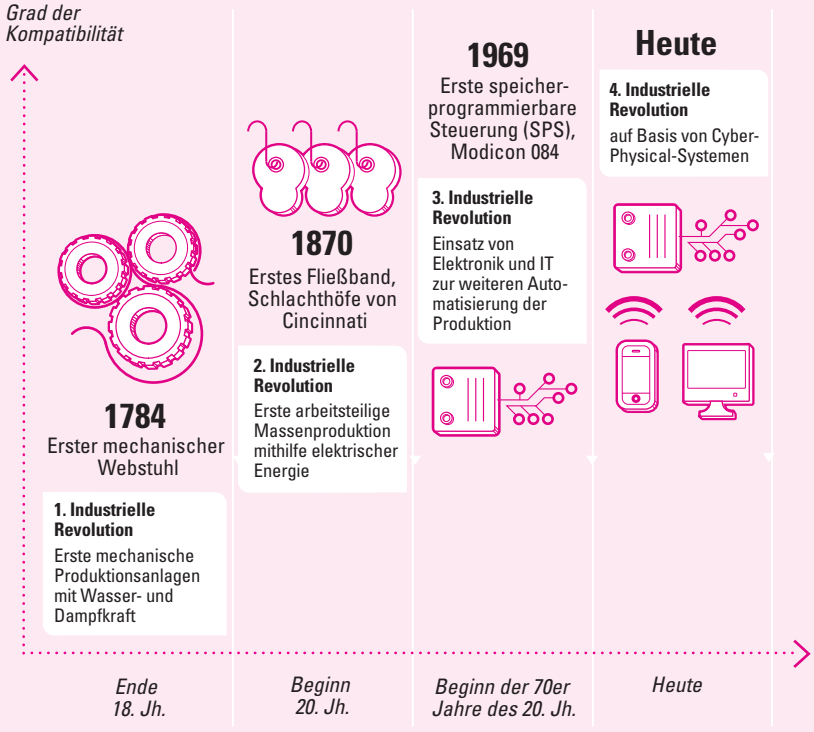
koordinieren sich selbst, melden Probleme, bevor diese zu Stillständen führen, fordern Nachschub an und veranlassen die Abholung fertiger Produkte. Auf Produktseite bekommt das herzustellende Gut beispielsweise von Anfang an die Information, wann und woraus es hergestellt werden soll. Die fertigen Produkte im Feld liefern Informationen, die den gesamten Wertschöpfungsprozess beeinflussen können. Die Liste der Informationen/Parameter auf beiden Seiten ist quasi beliebig erweiterbar.

Diese Daten effizient zu verwalten und daraus Muster herauszudestillieren, die immer wieder neue Aspekte des Kundennutzens einerseits und des Unternehmensnutzens andererseits sichtbar machen, ist eine Mammutaufgabe. Der immer häufiger genannte Begriff „Big Data“ spiegelt diese Tatsache wider.

Von der Industrie 1.0 zur Industrie 4.0

Die Evolution der Produktion

Quelle: DFKI (2011)



Infrastrukturen, Produkte und Dienstleistungen

Nach Angaben des amerikanischen Analystenhauses Gartner waren im Jahre 2014 bereits knapp vier Milliarden "Dinge" miteinander vernetzt, 2020 sollen es 25 Milliarden sein. Nach den Berechnungen der Gartner-Analysten werden Unternehmen dann mehr als 300 Milliarden Euro mit dem IoT erwirtschaften.[1] Dies kann aber nur gelingen, wenn die technische Infrastruktur dafür auch vorhanden ist. Der Nutzen der verfügbaren Infrastruktur wird durch ihre Verbreitung bestimmt. Eine schnelle Verbreitung wird allerdings nur dann möglich, wenn sich Standards für Datenaustausch und Sicherheit durchsetzen, auf die sich die wichtigsten Player im Cyberspace einigen können.

Das IoT eröffnet kreativen Gestaltern von Produkten und Services immer wieder neue interessante Chancen. Schon heute ist eine unüberschaubare Auswahl von Produkten erhältlich oder in Entwicklung, bei denen die Möglichkeit besteht, diese miteinander zu vernetzen und somit in ihren Funktionsweisen zu kombinieren. Durch diese Vielfalt der Kombinationsmöglichkeiten erschließen sich ganz neue Geschäftsmodelle, die mit erfolgreichen, zum Teil lange bestehenden Ertragssystemen in Konkurrenz treten. Das Smartphone greift beispielsweise durch seine Vielseitigkeit gleich mehrere Produkte an: Navigationssysteme, Fotoapparate, Diktiergeräte oder MP3-Player sind nur einige Beispiele dafür. Aktuelle Smartphones stellen die erforderliche Hardware bereit und können recht flexibel mit unterschiedlicher Software ausgestattet werden, was die Einsatzmöglichkeiten enorm erweitert. Ein einfaches Beispiel dafür ist eine Wetterstation, die eine Privatperson im Garten installiert hat. Die von der Station ermittelten Wetterdaten können über eine spezielle App des Smartphones gesammelt und betrachtet werden. Dank WLAN oder Bluetooth steht das Smartphone mit der entsprechenden Sensorik in Kontakt. Zudem leitet die App diese Daten weiter in die Cloud, wo sie anderen Nutzern zur Verfügung stehen oder zur Erfassung durch Wetterdienste herangezogen werden. Sie können für die Erstellung von Statistiken, Wetterprognosen etc. dienen.

Industrie 4.0 geht nur gemeinsam mit den Kunden.

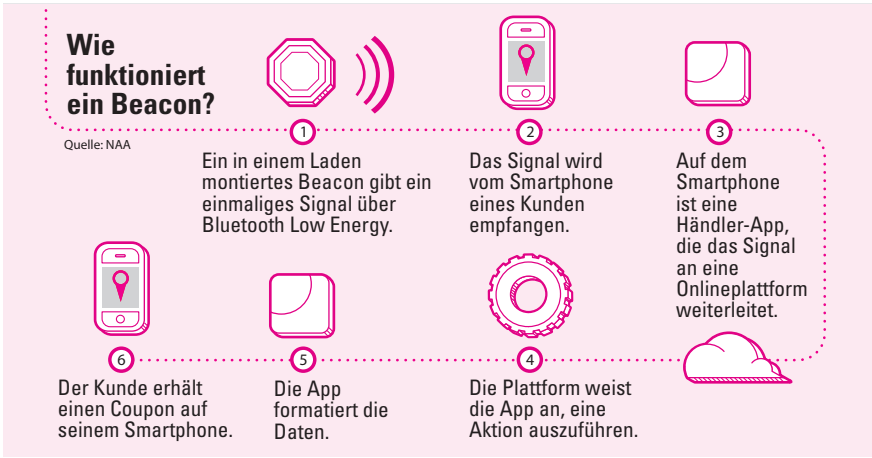
Prof. Dr.-Ing. Birgit Vogel-Heuser,
Technische Universität München

Andere Beispiele sind z.B. die Hausautomatisierung (Smart Home, Smart Meters), die Vernetzung von Fahrzeugen (Smart Mobility, Smart Logistics), die Anwendung in Belangen der gesunden Lebensführung oder der möglicherweise überlebenswichtigen Überwachung der grundlegendsten biologischen Vitalfunktionen des Menschen

[1] Computerwoche, 5.5.2015

(Smart Health) sowie die Veränderung von Produktionsabläufen im betrieblichen Umfeld (Smart Manufacturing, Industrie 4.0).

Eine weitere interessante Komponente im IoT könnten sogenannte Beacons (Englisch für "Leuchtturm") sein. Sie kommen innerhalb von Gebäuden oder auf kurze Distanzen zum Einsatz und kommunizieren im Umkreis von rund 100m mit Hilfe des Kommunikationsstandards Bluetooth Smart. Beacons treten beispielsweise mit Smartphones in ihrem Wirkungskreis in Kontakt und übermitteln Informationen, die für den Smartphone-Nutzer aufgrund seines bisherigen Such- oder Kaufverhaltens passen könnten: „Vegetarisches Restaurant gleich vorne links."



Wie auch immer die Lösung aussieht - erforderlich sind netzwerkfähige Hardware-Komponenten, die mittels WAN, WLAN, Bluetooth, GPS, GSM etc. und mittels Internet die Kommunikation ermöglichen.

Derzeit stehen der großflächigen Ausbreitung noch verschiedene Hindernisse im Weg, da die neue Dimension der Vernetzung zahlreiche juristische (Datenschutz, Verbraucherschutz, Haftung, etc.) und organisatorische Fragen (Standards, Zuständigkeiten, ...) aufwirft.

Die grundlegenden Technologien dagegen sind bereits vorhanden. Cloud Computing wird wohl die zentrale Technologie für die Verteilung der gigantischen Datenmengen sein. Intel, das amerikanische Chip-Schwergewicht, hat eine Plattform entwickelt, um Geräte, Systeme, lokale Datenbanken und Cloud-Infrastrukturen zu verbinden und mit Big Data und Real-time-Analytics sinnvolle und gewinnbringende Geschäftsmodelle und Services darauf aufzubauen. Mittlerweile dürfte es keinen wichtigen Player in der IT-Szene mehr geben, der nicht um seine Pole Position für den Start ins IoT-Rennen

kämpft. Development Kits sind dabei wichtige Lösungsbausteine, um den Einstieg in die IoT-Welt für möglichst viele Gerätehersteller zu erleichtern.[2]

Letztlich wird die Entscheidung für Standards wesentlich durch die in der Praxis geschaffenen Tatsachen, d.h. die installierte Basis im Feld, beeinflusst. Die Anbieter von Komponenten und Infrastrukturen, die ihren Kunden den Einstieg in die IoT-Welt durch kostengünstige und technisch einfache Lösungen erleichtern, haben einen strategischen Vorteil bei der Standardisierung. Sie könnten die weitere Entwicklung am stärksten beeinflussen. Hersteller, die ihre Systeme für IoT fit machen wollen, tun gut daran, ihre Systemarchitekturen offen und flexibel zu gestalten, um zu starke Abhängigkeiten von Lösungsanbietern zu vermeiden.

Gutes und zielgerichtetes System- und Softwareengineering ist hier gefragt: Smartes Engineering. Smart bedeutet in den meisten Fällen smarte Software bzw. Softwarearchitekturen, die Firmen in die Lage versetzen, schnell auf veränderte Kundenbedürfnisse oder Wettbewerbsverhältnisse zu reagieren oder diese Veränderungen sogar proaktiv voranzutreiben. Dies gilt für die Software in Embedded-Systemen genauso wie für CRM-Systeme und ERP-Systeme.

Sicherheit: Datenklau in der Cloud

Wer sich der Dimension der Sicherheitsanforderungen im IoT bewusst werden will, betrachtet dieses Thema am besten aus der Perspektive sensibler Industrieanlagen. Hier wird die Herausforderung sehr schnell deutlich.

Klassische Sicherheitstechnologie (…), wie man sie in heutiger Business-IT findet, wie Viren-Scanner, Firewalls, VPNs oder SSL/TLS-verschlüsselte Kommunikation zwischen Browsern und Servern in der Unternehmens-IT, oder aber auch Techniken zur Identifikation von agierenden Nutzern, wie Zugangscodes und Berechtigungsausweise, sind nicht für die ressourcenschonende, einfache Absicherung beschränkter, vernetzter Komponenten im Automatisierungs- und Produktionsumfeld geeignet. Die Komponenten müssen in der Lage sein, sich untereinander sicher zu identifizieren, Manipulationen zu erkennen und sicher miteinander zu kommunizieren. Sichere und überprüfbare Identitäten von Maschinen, der Schutz vor gefälschten und nachgemachten Produkten und die sichere Maschine-zu-Maschine-Kommunikation sind neue und wichtige Herausforderungen für die IT-Sicherheit in der Industrie 4.0. Benötigt werden neue Sicherheitstechniken, wie vertrauenswürdige Betriebssystem-Kerne für die beschränkten Komponenten, oder aber auch leichtgewichtige, aber dennoch starke Sicherheitsmechanismen, um Manipulationen zu verhindern bzw. unschädlich zu machen.

[2] Computerwoche, 5.5.2015

Zwar gibt es ausreichend bewährte Konzepte in der klassischen IT-Welt, doch lassen sich diese nicht ohne weiteres in den industriellen Kontext übertragen. Zum einen müssen die Sicherheitslösungen mit den bestehenden Standards der Systeme kompatibel sein. Zum anderen laufen die Industriesysteme unter sehr strikten Echtzeitbedingungen. Das Zeitfenster für die Ver- und Entschlüsselung der Daten oder die Authentifizierung von Nutzern und Geräten ist äußerst klein.

Erforderlich ist die Entwicklung von Sicherheitskonzepten für alle Ebenen. Dazu zählt zum Beispiel auch ein durchgängiges Berechtigungsmanagement. Damit wird klar geregelt, wer welche Aktionen an dem jeweiligen System vornehmen darf und kann. Neben dem Schutz vor Angriffen über das Internet muss auch die Sicherheit bei physikalischen Angriffen gewährleistet sein. Dies lässt sich durch die Integration von sicheren Hardware-Bausteinen erreichen, so dass ein System sich nicht mehr booten lässt, wenn eine manipulierte oder gefälschte Komponente (…) in das System eingebracht wurde.

Manipulation der Daten (Big Data) könnte verheerende Auswirkungen haben

Daten und Informationen können aber auch ein wertvolles Wirtschaftsgut sein, man denke beispielsweise an Produktionsdaten, die vor unberechtigten Zugriffen und Manipulationen zu schützen sind. Zudem werden eine Vielzahl von Aufenthaltsdaten, Bewegungsprofile, Nutzungsprofile oder auch Gewohnheiten von Nutzern der Anlagen und Maschinen erfasst. Dies stellt eine erhebliche Bedrohung der Privatsphäre dar. Die Gewährleistung einer datenschutzbewahrenden Verarbeitung von Daten ist eine zentrale sowohl gesellschaftliche als auch wirtschaftspolitische Aufgabe, hier ist noch ein erheblicher Forschungsbedarf erforderlich.

Die Arbeitnehmer in Industrie 4.0 sind mobil, organisieren sich global und handeln oft selbstständig. Arbeitszeiten und -orte sind flexibel. Dementsprechend muss die Informations- und Kommunikationstechnik (IKT) für die Arbeitnehmer mobil, vielseitig und sehr einfach verwendbar sein. Auch hinter diesen Anforderungen verbergen sich Herausforderungen für die IT-Sicherheit, von der Kommunikationssicherheit in mobilen Netzen über Konzepte wie „Bring your own device“ (…) bis hin zum Problem der einfachen Benutzbarkeit von IKT. Gerade die einfache, sichere Nutzbarkeit von IKT-gesteuerten Komponenten in produktiven Umgebungen wirft derzeit noch viele ungelöste Probleme auf.

Produktions- und Geschäftsprozesse werden in Industrie 4.0 entlang der Wertschöpfungskette aufgebrochen und auf unterschiedliche, oft voneinander wirtschaftlich unabhängige Parteien verteilt. Das Internet ist dabei das zentrale Kommunikationsmedium und Cloud Computing die zentrale technische Plattform zur Erbringung kostengünstiger, standardisierter IT-basierter Dienste. Damit dies gelingt, werden sichere und vertrauenswürdige Identitäten auch für Dienste und Menschen benötigt.

Dienste müssen sicher, dynamisch und über Organisationsgrenzen hinweg integrierbar sein. Die Kommunikation muss zuverlässig und sicher erfolgen, trotz diverser Angriffe und gezielter Industriespionage. Die Daten in der Cloud müssen gegen unerlaubten Zugriff geschützt sein und die Verarbeitung muss korrekt und sicher erfolgen.

Das sichere Cloud Computing ist für die sichere Industrie 4.0 eine zentrale Fragestellung. Den Nutzen von Cloud-Technologie hat die Forschungsunion in ihren Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 aufgearbeitet. Dabei steht Cloud Computing im Mittelpunkt und stellt die Plattform dar, über die alle Experten und Anwender in einem Szenario kommunizieren und an das sowohl die Akteure selbst als auch die Produktionsmaschinen angeschlossen sind.

Zentrale Anforderungen an sichere Cloud-Systeme sind die Verfügbarkeit der gespeicherten Daten und angebotenen Dienstleistungen, die Unversehrtheit der Daten sowie die Gewährleistung der Vertraulichkeit der Daten. Mögliche Einsatzszenarien für sicheres Cloud Computing, wie die sichere Fernwartung oder die sichere, zentrale Datenspeicherung und Analyse, werden diskutiert.

Angriffssicherheit / Datensicherheit / Informationssicherheit (engl.: *Security* oder auch *IT-Security* / *Cyber-Security*): der Schutz von Daten und Diensten in (digitalen) Systemen gegen Missbrauch, wie unbefugten Zugriff, Veränderung oder Zerstörung. Die Ziele von Maßnahmen zur Angriffssicherheit sind die Erhöhung der Vertraulichkeit (engl.: *Confidentiality*; Einschränkung des Zugriffs auf Daten und Dienste auf bestimmte technische / menschliche Nutzer), der Integrität (*Integrity*; Korrektheit / Unversehrtheit von Daten und korrekte Funktion von Diensten) und Verfügbarkeit (*Availability*; Maß für die Fähigkeit eines Systems, eine Funktion in einer bestimmten Zeitspanne zu erfüllen). Je nach konkretem technischen System und den darin enthaltenen Daten und Diensten bildet Angriffssicherheit sowohl die Grundlage für Datenschutz (*Information Privacy*), also den Schutz des Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechtes in Bezug auf personenbezogene Daten, als auch eine Maßnahme für Know-how-Schutz (Schutz der *Intellectual Property Rights*).

Digitale Ökosysteme

Gemäß der Definition von James F. Moore kann ein Business Ecosystem als Zweckgemeinschaft verstanden werden, in der wirtschaftliche Akteure durch und für den Zustand und das Wohl von Unternehmen und der Gemeinschaft der Beteiligten kooperieren.[3] Im Zusammenhang mit Industrie 4.0 als Teil des Internet of Things kommen zu dieser Zweckgemeinschaft zahlreiche Beteiligte hinzu.

[3] James F. Moore - The Death of Competition: Leadership and strategy in the age of business ecosystems. New York: HarperBusiness. ISBN 978-0887308093.

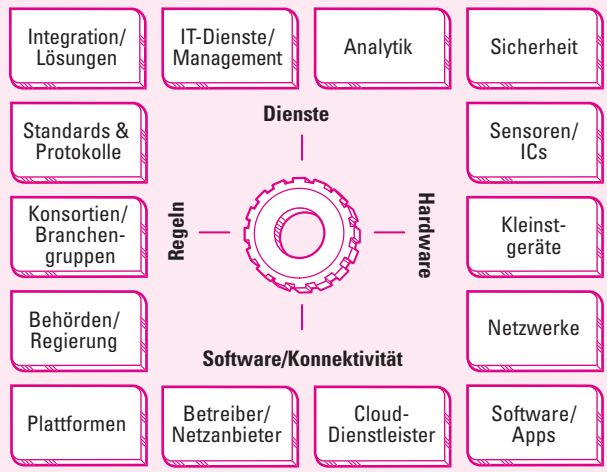
Unternehmen, die im oder mit Hilfe von IoT bzw. mit Industrie 4.0 ihre Geschäfte bzw. einen Teil davon machen, stehen vor der Herausforderung, Anpassungen in vielerlei Hinsicht vorzunehmen. Das betrifft Organisationsfragen, die Strategie und die Unternehmensausstattung; es trifft Unternehmen in ihrer ökonomischen Gesamtheit. Deterministische Systeme, die starr vernetzt sind, gehören zunehmend der Vergangenheit an und werden abgelöst von smarten Wertschöpfungsnetzwerken. Ad-hoc-Entscheidungen und selbstständige Steuerung charakterisieren die neuartigen Systeme; sie bieten hohe Effizienz und große Flexibilität für unterschiedlichste Geschäfts- und Ertragsmodelle.

Diese Veränderungen werden mittlerweile auch von den großen Telekommunikationsdienstleistern erkannt. Es kommen entsprechende Serviceangebote auf den Markt, die Firmen bei den anstehenden Veränderungen unterstützen sollen. Mit dem Produkt CIP (Connected Industry Platform) bietet die Telekom AG beispielsweise standardisierte IT-Lösungen, um industrielle Objekte aller Art untereinander zu vernetzen.

Die Darstellung ist naturgemäß nicht vollständig und deckt nicht die Gesamtheit eines umfassenden Ecosystem-Frameworks ab. Verdeutlicht werden sollen die Vielzahl der unterschiedlichen Faktoren, die einander bedingen und eine Möglichkeit, wie diese interagieren können.

Das IoT-Ecosystem entwickelt sich weiter

Quelle: ComTIA



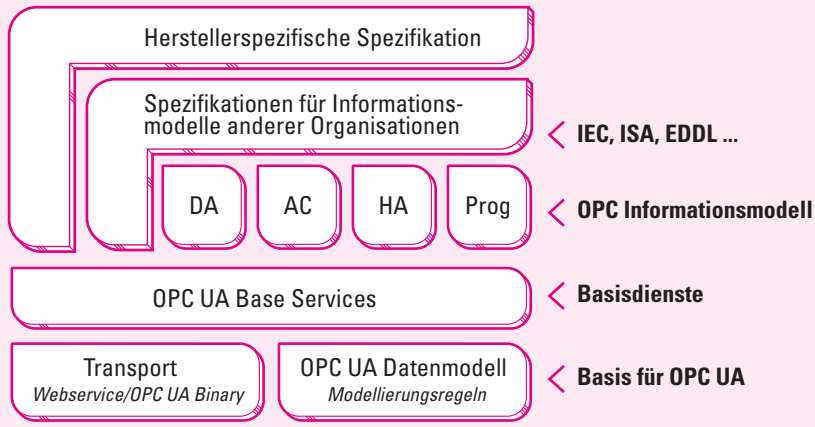
Die Weltsprache für die Vernetzung

Die überaus wortreich beschriebene Vernetzung von Dingen unterschiedlichster Mach- und Bauart erfordert einen gemeinsamen Standard für die Kommunikation, damit die Informationen auch untereinander ausgetauscht werden können. OPC UA ist der derzeitige, plattform- und herstellerunabhängige sowie betriebssystemübergreifende Standard, der für den zuverlässigen Datenaustausch zwischen Produkten und von Maschine zu Maschine (M2M) verwendet wird.

OPC UA ist von grundlegender Bedeutung für den internetbasierten Austausch in automatisierten Systemen, für Authentic- und Soft-SPS-basierte Maschinen und Anlagen, für MES und weitere Anwendungen. OPC UA gewinnt immer mehr an Bedeutung, je weiter die Vernetzung und Integration voranschreiten. Es ist ein offener Standard, der beliebig verwendet kann und ursprünglich für die Automatisierungstechnik entwickelt wurde.

OPC UA: Der Protokollstack für IoT?

Die effektive Kommunikation vieler Systeme erfordert eine gemeinsame Kommunikationsplattform, mit der sich auch herstellerspezifische Lösungen integrieren lassen. Ist OPC UA die Lösung für IoT und Industrie 4.0?



OPC UA kann sowohl für die Kommunikation unterschiedlichster Produkte verwendet werden, bietet aber auch die Möglichkeit der Implementierung vieler aktueller Programmiersprachen. Diese bekommen über das Protokoll OPC UA die Möglichkeit, miteinander zu kommunizieren, was bislang nicht möglich war. Es stellt gewissermaßen eine semantische Essenz verschiedener Programmiersprachen dar. Schnittstellen zwischen den unterschiedlichen Sprachen und Plattformen sowie vor allem zu dem

älteren DCOM OPC, gewissermaßen der OPC UA Vorgänger, werden über sogenannte OPC Wrapper realisiert.

Geschäftsmodelle, Wertschöpfung und Wettbewerb

Flexibilität ist nicht nur auf der Ebene von Komponenten und Infrastrukturen gefragt, sie ist generell eine der größten Herausforderungen. Geschäftsmodelle können sich im IoT sehr schnell verändern - weg von der Lieferung von Produkten hin zu Dienstleistungen. Oder die Schwerpunkte im Portfolio verschieben sich in die eine oder andere Richtung. Oder Produkte gewinnen durch zusätzliche Services an Attraktivität oder Nutzen. Beispiel: Ein Hersteller von Kompressoren für Druckluft hat in sein Angebot eine Dienstleistung aufgenommen – Druckluft. Der Kunde kauft nicht mehr einen Kompressor, stellt ihn auf und macht damit, was alle damit machen. Der Kunde bestellt Druckluft, der Lieferant wiederum stellt einen Kompressor zur Verfügung und der Kunde bezahlt für die entnommene Menge an Druckluft. Dies wird über I4.0-Komponenten überwacht und abgerechnet. Ein gänzlich neues Geschäftsmodell mit möglicherweise "dramatischen" Auswirkungen. Der bisherige Kompressoren-Anbieter und jetzige Druckluftservice-Provider hat plötzlich kein Interesse mehr, alle paar Jahre einen neuen Kompressor zu liefern oder sich des Öfteren Serviceeinsätze wegen Betriebsstörungen oder Wartungsarbeiten bezahlen zu lassen. Er wird vielmehr versuchen, einen langlebigen Kompressor zu liefern, der möglichst wenig Störanfälligkeit aufweist. Der Kunde wiederum hat Interesse daran, mit der Ware "Druckluft" möglichst sparsam umzugehen und Druckluftleitungen möglichst ohne Druckverlust zu verwenden.

Die Verschiebung des Geschäftsmodells vom Produkt zu Services oder neuen Kombinationen von Produkten und Services kann große Chancen mit sich bringen, was die nachhaltige Nutzung unserer begrenzten Rohstoffressourcen betrifft.

Der hohe Nutzen der Services kann allerdings auch dazu führen, dass Serviceanbieter ins Produktgeschäft einsteigen, um die Dienste über eigene Endgeräte anzubieten und die Geräte wiederum zu nutzen, um mehr über das Nutzerverhalten zu lernen. Dieses Wissen wird dann verwendet, um wieder neue Angebote zu kreieren. Das hört sich ein bisschen wie eine Gelddruckmaschine an. Es ist genauso denkbar, dass Firmen aus dem Produktgeschäft sukzessive aussteigen, um sich in Richtung Infrastruktur- und Serviceprovider zu entwickeln. Alles ist denkbar, die Grenzen zwischen materiellen und immateriellen Leistungen und Branchen verschwimmen.

Doch eines vereint alle Geschäftsmodelle, wie immer sie auch gestrickt sein mögen: Der Dreh- und Angelpunkt ist Software, die in der Lage ist, die Anforderungen an diese Dynamik, Flexibilität und Sicherheit abzubilden. Jetzt kommt das große WENN: Wenn die Projektteams in der Lage sind, Prozesse, Methoden und Tools so auszuwäh-

len und einzusetzen, dass sie damit Softwarearchitekturen und Code hervorbringen, die diese Potenziale der Software auch erschließen. Professionelles Software Engineering gehört somit zu den wesentlichen Erfolgsfaktoren für den Einstieg ins und das Überleben im IoT.

Das Internet of Things unternehmerisch nutzen

Im Bereich der industriellen Fertigung sind häufig Produktionsanlagen mit Robotern zu vernetzen. Darüber hinaus muss die Kommunikation mit hauseigenen CAD/CAM-Systemen, Warenwirtschaftssoftware und ERP-Systemen gewährleistet werden. Nicht zu vergessen, über die HMI (Human Machine Interfaces) sollen die Menschen, die an diesen Anlagen arbeiten, die Produktion auch direkt beeinflussen können. Ein vielversprechender Ansatz für die Vernetzung zahlreicher Teilnehmer mit komplexen und sich stark unterscheidenden Aufgaben ist die Steuerung mittels eines Agentensystems. Die Agenten stellen einerseits eigenständige Softwarebestandteile dar, die wiederum jeweils einen Teilnehmer repräsentieren. Die jeweiligen Informationen werden gewissermaßen vom/im Agenten gekapselt und auf diese Weise durch das System transportiert. Aktuelle Zustände können jederzeit erfasst und weitergereicht werden; die Produktion wird auf diese Weise hinsichtlich aller erfassten Kriterien optimiert. Durch die Kapselung sind die Daten sicher, und dank der hohen Entscheidungsbefugnis der Agenten kann ein solches System jederzeit flexibel reagieren, auch auf Störungen und Ausfälle.

Und die hohe Sicherheit dieses Ansatzes macht eine solche Lösung noch charmanter. Hohe Sicherheit im Zusammenhang mit gründlichem Software Engineering zeigt sich hinsichtlich aller wesentlichen Aspekte - Safety, Security und Zukunftssicherheit. Schließlich sind Industrieanlagen bis zu 25 Jahre im Einsatz.

In USA, Korea & China spricht man bereits von der Industrie 5.0.

Martin Zeil, bayer. Wirtschaftsminister a.D.

Knowhow für IoT

Die Betrachtung der verschiedenen Aspekte von IoT deutet auf die große Vielfalt von Herausforderungen hin, die damit verbunden sind. Im Kern geht es um vernetzte kleine, große und sehr große intelligente Einheiten, die mit ihrer Umgebung interagieren und dabei Daten sammeln, verarbeiten und miteinander kommunizieren, um einen

Nutzen zu erzeugen. Das kann einerseits der intelligente Sensor in einem Gebäude und andererseits die Serverfarm sein, die Daten in unvorstellbaren Mengen sammelt und durch Algorithmen jagt. Dieses IoT-System verändert sich durch seine Vielzahl von immer neuen Interaktionsmöglichkeiten und Interaktionspartnern praktisch ständig und erzeugt so immer neue Chancen - aber leider auch Risiken. D.h. wer im IoT-Spiel mitspielen will, muss hohe Flexibilität und eine gesunde Risikobereitschaft mitbringen.

Flexibilität ist Trumpf

Da wir nicht wissen, welche neuen Chancen und Risiken in diesem System entstehen, spielt die Flexibilität der Unternehmen auf allen Ebenen eine Rolle. Auf der Ebene der Unternehmensleitung ist beispielsweise strategische Flexibilität und Offenheit für neue Geschäftsmodelle und Partnerschaften gefragt. In den Projekten gewinnt die agile Anpassung an neue Anforderungen und Rahmenbedingungen an Bedeutung. Beim Engineering kommt es darauf an, flexible System- und Softwarearchitekturen zu entwerfen und den Entwicklungsprozess immer mehr als Lern- und Veränderungsprozess zu begreifen.

Als Schulungsanbieter mit dem Schwerpunkt im Bereich Embedded Software Engineering liegt uns die Situation der Entwicklungs- und Projektteams besonders am Herzen. Was könnte IoT für sie bedeuten?

Die Flexibilität einer Software wird einerseits durch ihre Architektur und andererseits durch die Art und Qualität der Implementierung (innere Qualität) bestimmt. Objektorientierung, Modellierung, Design Patterns, aber auch Programmierprinzipien wie Clean Code und Standards wie MISRA gewinnen in diesem Zusammenhang noch mehr Bedeutung als es heute schon der Fall sein sollte. Bei der wachsenden Komplexität und dem gleichzeitigen Innovationsdruck wird es immer schwieriger werden, Neuentwicklungen direkt auf dem Mikrocontroller aufzusetzen und rechtzeitig am Markt zu platzieren, zumal es immer häufiger Multicore-Controller sein werden. APIs und Betriebssysteme sind wichtige Hilfsmittel, um hier schneller zum Ziel zu kommen, ohne Funktionen selbst zu entwickeln, die so bereits verfügbar sind. Gleichzeitig bieten moderne Controller mit ihrer Peripherie unendlich viele Möglichkeiten der Optimierung auf bestimmte Anwendungsfälle und Betriebssituationen, wie beispielsweise die gezielte Abschaltung von Funktionen, um bei mobilen Geräten Energie zu sparen.

Es gilt immer wieder, anhand der Qualitätsanforderungen und Wettbewerbsbedingungen zu entscheiden, was der Lösung mehr dient - hardwarenahe Programmierung oder Aufsetzen auf einer höheren Abstraktionsebene, Eigenentwicklung oder Lösung von der Stange. Die Frage ist: Wie und wo lassen sich Alleinstellungsmerkmale am effektivsten umsetzen und sichtbar machen?

Das war im Prinzip schon immer so. Nur die Rahmenbedingungen, die uns zwingen, all das noch schneller und besser zu machen, verschärfen sich durch IoT. Deshalb können wir es uns auch nicht mehr leisten, erst am Ende des Entwicklungsprozesses zu testen, ob das Ergebnis unseren Vorstellungen oder besser der des Kunden entspricht. Qualitätssicherung wird zum kontinuierlichen Begleiter des Entwicklungsprozesses. Genauso wie die Änderung der Anforderungen zur Normalität des Entstehungsprozesses von Software wird.

Wir müssen immer mehr davon ausgehen, dass wir viele Anforderungen erst im Laufe der Entwicklung erkennen oder diese durch veränderte Rahmenbedingungen neu entstehen. Damit wächst die Bedeutung von agilen Prozessen und Entwicklungsmethoden sowie Entwicklungsumgebungen (Tools), die diese Dynamik abbilden können.

Learning by Doing but …

Wer dieser Dynamik gewachsen sein will, kann es sich nicht leisten, Programmiersprachen, Methoden, Architekturdesign, Projektmanagement und die Entwicklungsumgebung im Try-and-Error-Verfahren kennenzulernen. Zumal viele Designfehler, schlechte innere Qualität oder ungenutzte aber nützliche Funktionen von Mikrocontrollern und Tools oft erst erkannt werden, wenn es zu spät ist oder Änderungen mit hohen Zusatzkosten oder Zeitverlusten bezahlt werden müssen. Es ist wichtig, dass wir unseren Werkzeugkasten an Methoden, Tools und Prozessgestaltungsmöglichkeiten kennenlernen, bevor wir anfangen, Embedded-Systeme zu basteln, denn darauf läuft es ohne eine gute Wissensbasis hinaus. Schulungen oder anderweitige professionelle Projektunterstützung machen zwar aus einem Einsteiger noch keinen Profi, aber eine Person, die weiß, worauf es ankommt und wie Professionalität tatsächlich erreichbar ist.

Flexibilität entsteht vor allem durch Professionalität. Sie sorgt dafür, dass wir Risiken besser einschätzen können und Chancen gleich richtig nutzen - oder zumindest sehr schnell dazulernen.

Nicht zu vergessen: Softskills

Die gerade beschriebene professionelle Flexibilität erfordert auch professionelle Führung. Hochqualifizierte Mitarbeiter, die unter hohem Innovations- und Leistungsdruck stehen, sollten nicht gleichzeitig Versuchskaninchen von Projektleitern und Führungskräften sein, die auf ihre Führungsaufgabe nicht vorbereitet wurden. Die Auswirkungen auf Verantwortungs-, Einsatz- und Leistungsbereitschaft können nicht nur für das laufende Projekt katastrophal sein. Projektleiter erfüllen eine der anspruchsvollsten Führungsaufgaben, da sie in der Regel keine direkte disziplinarische Gewalt ausüben können. Umso mehr sind sie auf ihre Kommunikationsfähigkeit und den geschickten Einsatz führungspsychologischer Methoden angewiesen.

Je härter und komplexer die technischen Herausforderungen werden, desto mehr werden auch die Softskills der Projektleiter den Erfolg bestimmen. Dies gilt natürlich gerade in agilen und selbstorganisierenden Teams auch für jedes Teammitglied.

Fazit

Das IoT und sein spezieller Sonderfall Industrie 4.0 werden eine Fülle neuer Chancen, Risiken und Veränderungen technologischer, ökonomischer aber auch gesellschaftlicher, politischer und ökologischer Art hervorbringen, die sich schwer hervorsagen lassen. Das praktisch unendlich vernetzte System von intelligenten Einheiten wird uns ständig und oft spontan völlig neuen Situationen aussetzen. Veränderungsbereitschaft und Lernfähigkeit auf allen Ebenen der Unternehmen werden noch wichtiger als bisher. Wer die paradoxe Herausforderung nach Flexibilisierung UND Optimierung am besten bewältigt, hat die Nase vorn.

Was die vernetzten intelligenten Embedded-Systeme angeht, wird das Embedded Software Engineering in Kombination mit agilen Methoden und Prozessen immer mehr zum entscheidenden Wettbewerbsfaktor. Der Professionalisierung der Softwareentwicklung sollte deshalb hohe Priorität eingeräumt werden.

Dank

Wir bedanken uns beim Lehrstuhl für Automatisierung und Informationssysteme der Fakultät für Maschinenwesen der Technischen Universität in München, namentlich Frau Prof. Dr.-Ing. Birgit Vogel-Heuser und Frau Dr.-Ing. Dorothea Pantförder, für die sehr hilfreiche fachliche Unterstützung und die Bereitstellung von Informationsmaterial und Quellen zum Thema Industrie 4.0.

Anhang

Weiterbildung zum Thema Embedded Software Engineering

Folgende Trainings- und Beratungsangebote der Firma MicroConsult bieten Ihnen unter anderem das richtige Knowhow für zukunftsorientiertes Embedded Software Engineering:

- Internet of Things (IoT): Technologien und Entscheidungsgrundlage für das Internet der Dinge
- Software-Architekturen für Embedded-Systeme und Echtzeitsysteme
- Design Patterns (nicht nur) für Embedded-Systeme
- Requirements Engineering und Requirements Management für die Entwicklung in der Industrie
- Embedded C: Programmiermethoden und -tools für Embedded-Anwendungen
- Embedded C++: Objektorientierte Programmierung für Mikrocontroller mit C++/EC++ und UML
- Renesas Synergy™ Applikationsprogrammierung
- Netzwerke: Grundlagen und Einsatz
- TCP/IP/Ethernet Protokoll IPv4/IPv6
- HTML5: Plattformunabhängige App-Entwicklung
- Funktionale Sicherheit (Safety) von Elektronik und deren Software - Umsetzung nach IEC 61508 und ISO 26262
- Usability: Produkte benutzerfreundlich entwickeln
- Embedded-Software-Test für C: Best Practices für den Unit-/Modul-/Komponenten-Test

Detaillierte Informationen zu diesen und anderen Trainings finden Sie auf www.microconsult.de.

Literaturhinweise

- Michael Porter: Wie smarte Produkte Unternehmen verändern, Harvard Business Manager, Dez. 2015
- Michael Porter: Wie smarte Produkte Unternehmen verändern, Harvard Business Manager, Dez. 2014
- Timothy Kaufmann: Geschäftsmodelle in Industrie 4.0 und dem Internet der Dinge: Der Weg vom Anspruch in die Wirklichkeit, Springer Vieweg, 2015, ISBN-10: 3658102713
- Regulin, Daniel; Vogel-Heuser, Birgit: Agentenorientierte Verknüpfung existierender heterogener automatisierter Produktionsanlagen durch mobile Roboter zu einem Industrie-4.0-System. In: Handbuch Industrie 4.0. Springer, Berlin, Germany, 2016
- Thomas Bauernhansl, Michael ten Hompel, Birgit Vogel-Heuser: Industrie 4.0 in Produktion, Automatisierung und Logistik, Springer Vieweg 2014, ISBN 978-3-658-04681-1

Quellen

Quellen werden an den relevanten Stellen direkt im Text genannt. Darüber hinaus wurden Informationen aus einer Vielzahl weiterer Quellen eingearbeitet:

- Harvard Business Manager
- PTC – Dr. Harzenetter
- Kontron – J. Behammer
- Telekom AG
- Siemens AG
- Microsoft
- unternehmerTUM – Center for Innovation and Business Creation - Technische Universität München
- Forum4Industry – Paul Kho
- Computerwoche
- Heise.de
- Wikipedia
- etc.

Impressum

Herausgeber

MicroConsult GmbH
Charles-de-Gaulle-Str. 6
81737 München
Tel. +49 89 450617-0
info@microconsult.de
www.microconsult.de

Projektleitung und Redaktion:
Peter Siwon, MicroConsult
p.siwon@microconsult.de

Autoren

Alexander Sedlak, freier Journalist
alexander.sedlak@arcor.de

Alexander Sedlak lebt in München und schreibt als Fachjournalist über Technikthemen, aus Sicht von Unternehmen und aus Sicht von Nutzern/Verbrauchern. Als Technischer Redakteur im Maschinenbau weiß er, dass die wichtigen Fragen nach Produkten und Technik oft unter der Oberfläche der Produktpräsentationen zu suchen sind. Und als Marketingleiter in einem global agierenden Maschinenbaukonzern lernte er, dass die richtige Technik verbunden mit einer guten Strategie im industriellen Umfeld die besten Chancen hat, sich durchzusetzen. Für MicroConsult schreibt Alexander Sedlak regelmäßig Fachartikel und Trend Guides, unter anderem zu den Themen Sicherheit, Management und Führung.

Peter Siwon, MicroConsult
p.siwon@microconsult.de

Dipl.-Ing. Peter Siwon kennt die Embedded-Branche aus vielen Perspektiven: Forschung, Entwicklung, Projektleitung, Schulung und Beratung, Vertrieb, Marketing und Geschäftsführung. Er lehrt an der University of Applied Science in Nordhausen und Braunschweig und ist Trainer und Coach für Führungskräfte in der Industrie mit dem Schwerpunkt Softskills und Projektmanagement. Er ist Mitgründer des Embedded Software Engineering Kongress sowie Kolumnen- und Buchautor.

Lektorat:
Sabine Pagler, MicroConsult