

Referenzarchitekturen für das IoT: Überblick zum Stand der Technik und wesentlichen Trends

Die Ziele des Internets der Dinge (IoT) sind die IT-Vernetzung von Gegenständen und die Bereitstellung von Funktionalitäten beziehungsweise Dienstleistungen, die es so noch nie gab. Eine große Schwierigkeit bildet allerdings der Mangel an Referenzarchitekturen und Standards für das neue „Industrial Internet“ und damit die Vernetzung im Internet der Dinge. Dieser Artikel gibt einen Überblick über aktuelle Betrachtungsmodelle, Referenzarchitekturen und ihre Bedeutung für Industrieprojekte.

Ein Anwendungsbeispiel: Digitalisierung bei einem Automobilzulieferer

Stellen Sie sich vor, Sie seien der Entwicklungsleiter für Motoren und Aggregate und wollen die Digitalisierung voranbringen. Durch jahrzehntelange Erfahrung in der Konstruktion von Motoren kennt Ihre Firma die Technik in- und auswendig. Allerdings ändern sich Motortechnologien schnell, zu schnell für viele Mitarbeiter Ihres Unternehmens, sei es in der Herstellung, der Weiterentwicklung oder im Service.

Zuerst machte eingebettete Elektronik aus den Motoren mehr als nur rein mechanische Komponenten und schaffte damit etwas Neues für Ihr Unternehmen und Mehrwertfunktionen für Ihre Kunden. Dann wurden die Motoren zunehmend mit anderen elektronischen Systemen des Automobils vernetzt. Das schaffte eine Vielzahl neuer Anwendungen für den optimierten Betrieb und die Diagnose, aber auch völlig neue Herausforderungen in der Technik. Eine große Anzahl an Geräten mit Konfigurationsmöglichkeiten bedeutet eine enorme Steigerung an möglichen Zuständen Ihres Systems, das Sie durch Updates auch im Betrieb noch verändern können.

Um diese Komplexität zu verwalten, braucht man sowohl Integrations- und Prüfmöglichkeiten als auch tiefe Kenntnisse der Motoren, um diese in einem definierten Zustand zu halten und somit einen störungsfreien Betrieb zu gewährleisten. Zudem benötigen Sie neue Verfahren für prädiktive Diagnose und effiziente weltweite Reparaturen. Eine Vernetzung mit Warenwirtschaftssystemen sowie Big-Data-Analysetools zur Unterstützung der Entwicklung und der Instandhaltung während des gesamten Lebenszyklus ist möglich und sinnvoll.

Vernetzung im Internet of Things

Die Vorteile einer Vernetzung sind offensichtlich. Man erhält als Betreiber Kenntnis typischer Nutzerbedürfnisse und kann diese in Echtzeit in das Produkt beziehungsweise den Arbeitsablauf einbinden. Das schafft Mehrwert in verschiedenen Bereichen:

- **Flexibilität:** Produkte passen sich selbstständig an Anwendungsszenarien, wie intelligente Gebäude, intelligentes Transportwesen, verteilte Erzeugung von Energie, Gesundheitswesen oder Lieferkettenmanagement und Logistik, an.
- **Benutzerfreundlichkeit:** Produkte sind einfach zu bedienen, wodurch sich die Benutzerfreundlichkeit erhöht, obwohl diese Produkte eventuell komplex sind.
- **Produktivität:** Der Kundendienst wird um prädiktive Instandhaltung und proaktive Upgrades erweitert, wodurch sich die Verfügbarkeit und damit die Produktivität erhöhen und wirtschaftliche Risiken verringert werden.

Das Internet der Dinge (IoT) bietet Innovationen und bringt auch eine Steigerung der Effizienz und Qualität mit sich, da geschäftsrelevante Informationen verknüpft werden. Die Vernetzung der Industrieproduktion, medizinischer Geräte, Automobile oder des Transportwesens mit IT-Systemen stellt einen enormen Wertgewinn für Unternehmen dar. Große IT-Konzerne wie Cisco [Cisc] und SAP [SAP] sagen Milliarden von vernetzten Geräten und eine immense Vielfalt von IT-basierten Dienstleistungen voraus, die ein Milliardengeschäft versprechen.

Doch wer überblickt heute sowohl die Anforderungen an Software und IT und kennt auch die benötigten Architekturen und Technologie-Stacks? Geschäftsführer

sind mit der Wertschöpfungskette vertraut, interessieren sich allerdings nicht für die Details der Informationstechnologien. Die Fertigung scheut zurück, sobald sie mit Softwaretechnologien konfrontiert wird. IT-Abteilungen übersehen durch eine distanzierte Perspektive leicht, dass es auch reale Produkte und Kunden gibt. Entwicklungsabteilungen fokussieren sich auf die Erstellung von Gesamtsystemen und betrachten Software gelegentlich als etwas, das sowieso nie recht funktioniert.

Es bedarf IoT-Architekturen und Modellierungslösungen, um die heterogene Landschaft der Entwicklungspartner, deren gegenseitiges Verständnis und gemeinsames Arbeiten zu unterstützen.

Bei der Softwareentwicklung im IoT ergeben sich neue Herausforderungen in Hinblick auf Anwendungen, Geräte und Dienstleistungen. Mobilität, benutzerorientierte Entwicklung, intelligente Geräte, E-Services, Umgebungs-Monitoring, E-Health und Wearables oder sogar implantierte Geräte stellen spezifische Herausforderungen an die Spezifikation von Softwareanforderungen und die Entwicklung von zuverlässiger, sicherer Software.

Der Einsatz spezieller Softwareschnittstellen, agile Entwicklungsorganisation und Anforderungen an die Zuverlässigkeit von Gesamtsystemen benötigen eine neuartige Herangehensweise. Erklärungsmodelle und Referenzarchitekturen für das IoT unterstützen hierbei Entwickler durch Vorgabe von Strukturen bei der Bewältigung dieser Herausforderungen.

Rückblick

Der Begriff „Internet der Dinge“ wurde zum ersten Mal 1999 von Kevin Ashton, im Rahmen eines Fachartikels zu Standards zur Etikettierung unter Verwendung von RFID im Logistikbereich, verwendet. Die

Kategorie	Initiative	Kurzbeschreibung	Status	URL
IoT-Referenz-architekturmodelle	Reference Architecture Model Industry 4.0 (RAMI 4.0)	Eine Referenzarchitektur für intelligente Fabriken mit dem Schwerpunkt IoT-Standards, die in Deutschland begonnen wurde und mittlerweile von allen größeren Unternehmen und Stiftungen der relevanten Industriesektoren getragen wird.	Version 1 vom 1. Juli 2015	www.zvei.org/en/association/specialist-divisions/automation/Pages/default.aspx
	Industrial Internet Reference Architecture (IIRA)	Das Industrial Internet Consortium (gegründet von AT&T, Cisco, General Electric, IBM und Intel) lieferte ein Referenzarchitektur zur weiteren Diskussion.	Version 1.7 vom Juni 2015	www.iiconsortium.org
	Internet of Things-Architecture (IoT-A)	Die IoT-A lieferte eine detaillierte Architektur und ein Modell aus der funktionalen und der Informationssichtweise. Das Projekt erstellte auch eine detaillierte Analyse zu Systemanforderungen.	Die abschließende Version wurde im Juli 2013 veröffentlicht	www.iot-a.eu/public/public-documents/d1.5/view
	Standard for an Architectural Framework for the Internet of Things (IoT)	Das IEEE-P2413-Projekt hat eine Arbeitsgruppe zum architektonischen IoT-Framework, mit den Schwerpunkten Datenschutz, Safety, Security und Sicherheitsproblemen.	Ein laufendes Projekt ohne White Papers oder Dokumente bis zum Mai 2016	https://standards.ieee.org/develop/project/2413.html
	Arrowhead Framework	Diese Initiative ermöglicht eine kollaborative Automatisierung durch offen vernetzte, eingebettete Geräte. Dies ist ein großes EU-Projekt, um Best Practices für kooperative Automatisierungen zu definieren.	Kontinuierliche Updates und Veröffentlichung von Materialien bis zum Frühjahr 2016	www.arrowhead.eu
Machine-to-Machine-Standards (M2M) mit IoT-Relevanz	European Telecommunications Standards Institute Technical Committee (ETSI TC) für M2M	Das TC bietet IoT-Kommunikations-Standards.	Unterschiedliche Standards und Entwürfe verfügbar	www.etsi.org/technologies-clusters/technologies/m2m
	International Telecommunication Union Telecommunication Standardization Sector (ITU-T)	Der ITU-T ist koordinierend im Bereich von Identifikationssystemen für M2M tätig.	Unterschiedliche Standards und Entwürfe verfügbar	www.itu.int/en/Pages/default.aspx
Weitere Aktivitäten	European Research Cluster zum Internet of Things (IREC)	Das IREC ist in vielen Themen im IoT-Bereich involviert, unter anderem in den Bereichen vernetzte Objekte, das „Web der Dinge“ und die Zukunft des Internets.	Kontinuierliche Updates	www.internet-of-things-research.eu
	Smart Appliances (SMART) Study	Diese EU-finanzierte Studie legt ihren Fokus auf „Semantic Assets“ für die Interoperabilität von intelligenten Geräten.	Definition der Smart-Appliance REFERENCE ontology vom März 2015	https://sites.google.com/site/smartappliancesproject/home oder http://ontology.tno.nl/saref

Tabelle 1: Internet-der-Dinge-Referenzarchitekturen (IoT) entwickeln sich in enger Zusammenarbeit von Forschung und Industrie.

Idee einer allgegenwärtigen Datenverarbeitung (sog. Ubiquitous Computing) gibt es jedoch schon seit den späten 80er Jahren. Wissenschaftler arbeiten seit Langem an Verfahren der Objektidentifikation, Sensor- und Kommunikationsnetzwerken sowie an Middleware- und Cloud-Technologien.

Als ein wichtiger Meilenstein auf dem Weg zum IoT gilt die Verabschiedung des IPv6, eines neuartigen Internetprotokolls mit sehr großem Adressraum, durch die „Internet Engineering Task Force“ im Jahr 1998. Das Interesse am IoT wurde in letzter Zeit durch die Entwicklung von Komponenten, Systemen und Referenzarchitekturen vorangetrieben. Große Konzerne haben in letzter Zeit beispielsweise folgende Ankündigungen gemacht:

- Google hat mit Brillo ein Betriebssystem für IoT-Geräte vorgestellt und Windows 10 unterstützt eingebettete Systeme für weitverbreitete Mikrocontroller wie Raspberry Pi 2.
- Geräte mit Machine-to-Machine-Kommunikationsstandards (M2M) wie Bluetooth, ZigBee, IPC Global Standards und Low-Power WiFi sind erhältlich und werden durch Werbung in den Markt gebracht.
- Bosch, SAP, Siemens, Telekom und andere Unternehmen haben IoT-Clouds lanciert und arbeiten intensiv an Anwendungen zur Vernetzung

Ein Gang über die CeBit oder Hannovermesse Industrie 2016 machte deutlich, dass sich die IT-Branche sehr stark an den neuen Technologien orientiert.

IoT-Architekturen und Modellierung

Bisher basierten IoT-Anwendungen auf fragmentierten Softwareimplementierungen für spezifische Systeme und Anwendungsfälle. Die Notwendigkeit von Referenzarchitekturen in der Industrie wird durch die wachsende Anzahl an Initiativen, die auf standardisierte Architekturen hinarbeiten, deutlich. Diese Initiativen zielen darauf ab, Interoperabilität zu ermöglichen, die Entwicklung zu vereinfachen und die Implementierung zu erleichtern.

Tabelle 1 gibt einen Überblick zu Referenzarchitekturen und deren Entwicklungsstand.

Das *Reference Architecture Model Industry 4.0 (RAMI 4.0)* beispielsweise geht über das IoT hinaus, indem es Produktions- und Logistikdetails mitberücksichtigt. Die In-

	Verwendete Protokolle	IIRA	RAMI 4.0
Semantische Orientierung	Service-Protokolle wie OPC UA, uPnP, DDS, DPWS, CoAP, EXI, ...	Funktionalitäten der Industriedomäne wie Geschäft, Betrieb, Informationen und Anwendungen	Wie IIRA und Erweiterung um zwei Dimensionen (Lebenszyklus und Wertstrom sowie Hierarchieebenen)
Internet-Orientierung	Vernetzbarkeit und Protokollkonvertierung basierend auf UDP vs. TCP mit HTTP oder MQTT	Dichter an der Beschreibung von Geschäfts-Anwendungsfällen als an IT-Betrachtungen	Modellierung und Strukturierung der Systeme und insbesondere deren Komponenten
Dinge-Orientierung	Bitübertragungsschicht und Sicherungsschicht mit niedrigen Kommunikationsprotokollen	Konzentration auf Assets wie Sensoren, Aktoren und Objektidentifikation	Techn. Assets, d.h. „Industrie 4.0 Komponenten“ mit Sensoren oder Aktoren und einer „Verwaltungsschale“ zur Administration

Abb. 1: Unterschiede der Architekturen aus drei Sichtweisen.

dustrial Internet Reference Architecture (IIRA) legt hingegen den Schwerpunkt auf die Industrie und die *Internet of Things-Architecture (IoT-A)* bietet eine detaillierte Sicht auf Aspekte der Informationstechnologien im IoT. Eine grundlegende Standardisierung findet derzeit in der M2M-Kommunikation unter Verwendung von effizienten, skalierbaren und sicheren Kommunikations-Stacks statt. Diese Standardisierung basiert auf einem modifizierten Open-Systems-Interconnection-Stack (OSI-Stack) und schlägt Spezifikationen für die Sicherungs-, die Vermittlungs- und die Transportschicht vor.

Im Herbst 2015 trafen sich Vertreter von RAMI 4.0 und des IIC (IIRA), um diese sehr sichtbaren Architekturen anzunähern und zu verbessern. Dabei betrachtet heute die amerikanische Architekturvariante IIRA hauptsächlich die Perspektive der Netzwerke und hebt zum Beispiel Gateways, die Middleware-Plattform usw. im Sinne von Implementierungs-Knotenpunkten hervor. Das RAMI-4.0-Modell blickt hingegen auf die einzelnen Komponenten im Netzwerk der Industrieautomatisierungssysteme und beschreibt deren Eigenschaften. Insbesondere nach Intervention der Politik ist es zu erwarten, dass sich die beiden komplementären Ansätze zukünftig besser abstimmen und eine einheitliche Sicht der unterschiedlichen Perspektiven erarbeiten.

Anforderungen an Referenzarchitekturen

Eine Referenzarchitektur beziehungsweise ein Referenzmodell zu bestimmen und zu strukturieren, ist ein langwieriger, mühsamer Prozess mit vielen Iterationen, um eine Abgrenzung von spezifischen Anforderun-

gen und Technologien zu erreichen. Eine Referenzarchitektur kann als allgemeine, generische Richtlinie dienen, wobei nicht alle Anwendungen jedes Detail für eine Umsetzung benötigen.

Trotzdem sind die Anforderungen einfach zu formulieren:

- Konnektivität und Kommunikation sind wichtig. Dies beinhaltet sowohl Eins-zu-Eins-Verbindungen (Unicast) als auch Datenerhebung und Informationsverbreitung mit mehreren Partnern (Multicast oder Anycast).
- Falls ein Gerät hinzugefügt wird oder Änderungen an der Konfiguration eines Gerätes vorgenommen werden, welche an andere Geräte weitergegeben werden müssen, muss die Geräteverwaltung Lösungen anbieten.
- Datenerhebung, -analyse und -aktivierung sind relevant, um Informationen und Wissen zu extrahieren, damit Dienste angeboten werden können.
- Skalierbarkeit ist erforderlich, um der steigenden Größe bei verschiedenen Systemausführungen gerecht zu werden.
- Funktionalitäten der IT-Sicherheit sind notwendig, um Datenschutz zu gewährleisten und Vertrauen in Produkte zu schaffen, und werden in allen Bereichen des IoT benötigt.

Eine IoT-Referenzarchitektur bewältigt diese Anforderungen und bietet eine Obermenge an Funktionalitäten, Informationsstrukturen und Mechanismen. Eine zusätzliche Berücksichtigung von Entitäten und deren Interaktionen führt zu einem Referenzmodell, welches Aspekte der voneinan-

der abhängigen Entitäten, wie menschliche Benutzer, Geräteausführungen und Serverstrukturen, integriert und eine vollständige Sicht und Vorlagen für den kompletten Aufbau und seine Umsetzung bietet. Sowohl Architektur als auch Systemmodell helfen dabei, Technologien zu beschreiben und mit Geschäftsfällen zu verknüpfen.

Praxis: Verfügbare Architekturen

RAMI 4.0 und IIRA sind zwei große Referenzarchitekturen, wobei beide Architekturvorschlüsse sorgfältig vorbereitet wurden, RAMI 4.0 allerdings deutlich detaillierter beschrieben wurde und die IIRA eher ein Erklärungsmodell als eine Architektur darstellt. Seit der Vorstellung von RAMI 4.0 im Jahr 2015 wurde sie mit der IoT-Community diskutiert und unterschiedliche Sichtweisen vereinigt. Im Gegensatz dazu ist die IIRA immer noch in intensiver Abstimmung und wird voraussichtlich zukünftig noch zahlreiche weiterführende Strukturen vorstellen.

Diese Architekturen sollen nun in Hinsicht auf ihre Schichten und ihr jeweiliges Potenzial unter Einnahme von drei Perspektiven [Atz10] verglichen werden. **Abbildung 1** zeigt die architektonischen Schichten und Protokolle sowie die Unterschiede der Architekturen im Überblick.

Der erste Blickwinkel ist die *semantische Orientierung*, das heißt die Interpretation von Daten und Informationen, um Wissen für Geschäftsfälle zu erzeugen. Bei der „Semantik“ geht es um die Bedeutung für das Geschäft oder den Betrieb. IoT-Protokolle auf dieser Ebene müssen einen Bezug zur Anwendung entwickeln. Dies ist eine sehr schwierige Aufgabe, die das IIRA-Modell unter Einnahme einer Managementperspektive angeht und dabei einen allgemeinen Bezug zu Funktionen in den Industriedomänen beschreibt. RAMI 4.0 greift hingegen gängige Industrienormen der International Electrotechnical Commission (IEC 62890, 62264 und 61512) auf und setzt diese in Beziehungen zueinander, um Lebenszyklus, Wertstrom und Hierarchie zu betonen. Die Forschung an der Verbindung dieser Bedeutungszusammenhänge auf System- und Komponentenebene wird noch viele Diskussionen erfordern, auch wenn es erste Protokollstandards bereits heute gibt.

Der zweite Blickwinkel ist die *Internet-Orientierung* mit zwei Aspekten. Einerseits ist die Middleware zur Serviceunterstützung in Verbindung mit der Datenverwaltung in der Cloud und Servern zu nennen.

Andererseits sind Vernetzung, Datentrans-

port und Datenverbindungen zu betrachten, was beide Architekturen kurz anschneiden, dann aber dabei lediglich auf die M2M-Kommunikation verweisen. Sobald es um die unteren Schichten des sogenannten OSI-Stacks geht, kommen M2M-Ansätze zum Einsatz, die nicht durch die Referenzarchitektur beschrieben werden. Die Vermittlungsschicht zum Beispiel kann mit IPv6 umgesetzt werden, während die Transportschicht auf UDP (User-Datagram-Protocol) und die Anwendungsschicht auf CoAP (Constrained-Application-Protocol) basiert. Als Alternative kann das MQTT-Protokoll, anstelle von HTTP, mit TCP/IP als Transport- beziehungsweise Vermittlungsschicht verwendet werden.

Der dritte Blickwinkel ist die *Dinge-Ori-*

entierung, welche sich auf Assets wie Sensoren, Aktoren und Objektidentifikation konzentriert. Dies ist der klassische Ansatz der Automatisierungsindustrie, welcher versucht, per bottom-up eine Referenz für physische Objekte und deren individuelle Datenquellen und Informationsbedarf zu definieren.

IIRA und RAMI 4.0 haben Managementmechanismen über alle Schichten hinweg und helfen die Gesamtstruktur des IoT zu beschreiben und zu definieren. Sie stellen, unter Einbeziehung von M2M-Kommunikationsstandards, anschauliche Modelle bereit, die beschreiben, wie Komponenten (d.h. IoT-Geräte) und Menschen interagieren und Daten verarbeiten, aber verschiedene Perspektiven und Granularitäten in ihrer

Titel	Beschreibung
Die Eclipse Foundation, welche für ihre Java-IDE.	
Eclipse Smart Home: Open Home Automation Bus (sogenanntes OpenHAB)	Kombiniert Komponenten verschiedener Anbieter aus der Gebäudeautomatisierung und integriert diese mittels einer neutralen Plattform, welche unabhängig von Herstellern und Protokollen ist. OpenHAB ist eine nützliche Hilfe in der Integration, welche typischerweise Komponenten von mehreren Anbietern vereint.
Eclipse Vorto: semantische Beschreibungssprache für IoT-Geräte	Trotz der vielen wissenschaftlichen Ansätze hat Vorto bereits eine Community, unterstützt durch ernst zu nehmende Anwendungen, gefunden.
Eclipse Equinox: Implementierung eines OSGi-Frameworks	Implementiert ein komplettes und dynamisches Komponentenmodell, wobei mit Hilfe der OSGi-Spezifikation modulare Systeme und eine Serviceplattform spezifiziert und in Java implementiert werden können.
Eclipse Paho: Implementierung eines Open-Source-Clients mit MQTT	Das Message Queue Telemetry Transport Protocol (MQTT) ist ein zuverlässiges, lightweight, publish-subscribe Messaging-Transport-Protokoll, welches von OASIS unterstützt wird und nur geringe Anforderungen an Codierung und Netzwerkbandbreite hat.
Auch Apache ist im IoT aktiv:	
Apache Spark: Cluster Computing	Framework, welches sich für die Analyse von Big-Data und das Streaming in Fast-Echtzeit eignet.
Apache Cassandra: Datenbank	Skalierbare und hochverfügbare Cloud-Infrastruktur, welche von der linearen Skalierbarkeit und der nachgewiesenen Fehlertoleranz von Standardhardware profitiert.
Auch die OMG (Object Modelling Group) hat einige Aktivitäten im IoT.	
Die OMG managt die Tätigkeiten des Industrial Internet Consortium (IIC), welches ein gemeinnütziges Konsortium ist, das die Interoperabilität im IoT zum Ziel hat.	
Weitere Aktivitäten der OMG sind:	
Interaction Flow Modeling Language	IFML ist eine standardisierte Modellierungssprache, die graphische Notationen für visuelle Modelle von Nutzerinteraktionen miteinschließt.
Unified Component Model	Modellierungsschema für Real-Time, Embedded und verteilte Systeme.

Tabelle 2: Open-Source-Initiativen im IoT.

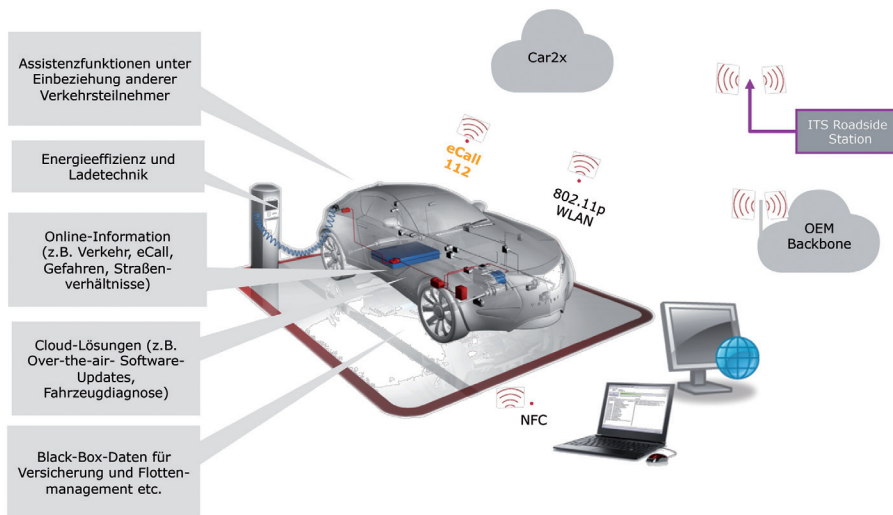


Abb. 2: Vernetzte Fahrzeugsysteme.

Beschreibung des IoT aufweisen.

Open-Source-Initiativen

Open-Source-Initiativen haben sich als zusätzliche treibende Kraft in der De-facto-Standardisierung etabliert, da viele Entwickler die Technologien ständig anwenden und weiterentwickeln. Eine Übersicht über Open-Source-Initiativen kann **Tabelle 2** entnommen werden.

Open-Source-Aktivitäten sind typischerweise allerdings eher bottom-up-orientiert und sehr stark auf die Implementierung ausgerichtet, statt sich einer übergreifenden Perspektive anzunehmen, die die Konsortien der IoT-Referenzarchitekturen auszeichnet. Bei der zukünftigen Entwicklung von Standards ist die „Normative Kraft des Faktischen“ allerdings nicht zu unterschätzen,

die Situationen hervorbringen kann, die später zu einer Akzeptanz der Vorgehensweise führt, die über eine langwierige Standardisierung eventuell nicht zu bewirken gewesen wäre.

Erste Praxisanwendungen: Vernetzte Fahrzeugsysteme

Vernetzte Fahrzeuge sind ein interessanter praktischer Anwendungsfall für die Umsetzung von IoT-Technologien (siehe **Abbildung 2**). Fahrzeuge sind zunehmend mit der Außenwelt vernetzt. Intern gilt das beispielsweise für Multi-Sensor-Fusion und sich auf viele einzelne Steuergeräte überlagernde Funktionen, wie beispielsweise komplexe Assistenzsysteme. Extern findet eine rasante Evolution durch Software-Aktualisierungen Over-the-Air (OTA) sowie

die Kommunikation verschiedener Verkehrsteilnehmer in car2x-Funktionen statt. Bedingt durch den Einsatzzweck tauschen die Verkehrsteilnehmer und Geräte, wie Ladestationen oder Verkehrszeichen, Informationen aus, beispielsweise die Warnung vor einer Gefahrenstelle. Die zunehmend offene Architektur eines Fahrzeugs muss demnach Performanz, Robustheit, funktionale Sicherheit, Integrität und Authentizität der Nachrichtenübermittlung gewährleisten.

Die Umsetzung der Anforderungen soll in einem sicherheitskritischen Anwendungsfall gezeigt werden. Heterogene Netze wie bei car2x können keine verlässliche Quality-of-Service (QoS) liefern. Eine risikoorientierte Cyber Security ist zunehmend wichtig, denn ein vollständiger Schutz kann nicht gewährleistet werden. Informationen von Systemen, die potenziell nicht verlässlich sind, müssen bei sicherheitskritischen Funktionen durch Redundanz und Plausibilität abgesichert werden. Die Entscheidungsbefugnis muss maßgeblich durch verlässliche Sensoren erzeugt werden. Beispiele sind Informationen über Funkverbindungen, wie Mobilfunk oder car2x, über Straßenzustand und Verkehrslage an einer stark befahrenen Straße. Ein darauf basierender Kollisionsschutz ist jedoch damit noch nicht verlässlich gewährleistet. Authentifizierung und Informationszugriff von einem externen Netz oder von car2x-Kommunikation dürfen weder Voraussetzung für Schutz sein, noch dürfen relevante Informationen für sicherheitskritische Assistenzsysteme ausschließlich von außen kommen.

Deutlich werden an diesem Fallbeispiel zwei Aspekte für IoT: Anwendungsfälle gehen über Einzelfunktionen hinaus und machen ein System im Zusammenspiel von Funktionen und Komponenten angreifbar. Sicherheit ist aufgrund diversitärer Fehlerursachen sehr viel schwieriger zu gewährleisten als bei Fehlfunktionen einzelner Komponenten, wie sie traditionell bei funktionaler Sicherheit betrachtet werden.

Architekturen für derartige IoT-Systeme verlangen ein System- und Lebenszyklusübergreifendes Konzept, vor allem, wenn deren Wirksamkeit zu einem späteren Zeitpunkt aus rechtlichen Gründen nachgewiesen werden soll. Wie bereits in der Kommunikationstechnik vor einigen Jahren erkannt wurde, reichen isolierte Mechanismen allein, wie die Aufteilung in separat agierende Teilsysteme, der Schutz einzelner Komponenten, definierte Protokolle zwi-

Die weitere Entwicklung des IoT wird von vielen Aspekten abhängen: Können standardisierte IoT-Stacks das Geschäft mit Individualsoftware in der Produktion, der Logistik und Energiewirtschaft ändern? Wie entwickelt sich der für Deutschland sehr wichtige Automobil-Sektor in Sachen Connected Car und automatisiertes Fahren? Was wird zum kommerziellen Produkt und was Open Source beziehungsweise Public Domain? Sind einheitliche Standards zum Beispiel für Schnittstellen im Sinne einer Verwaltungsschale von IoT-Geräten überhaupt technisch definierbar? Werden große Anbieter Standards für IoT-Clouds schaffen oder diese sogar dominieren? Wie wird das Thema IT-Sicherheit geopolitisch und gesellschaftlich gemeistert?

Diese vielen Fragen zeigen die Vielschichtigkeit und Tragweite rund um das Thema „Digitalisierung“, das durch das IoT befördert wird. Neben technischen Fragen der Referenzarchitekturen existiert eine Fülle von Seitenthemen, die sich in den nächsten Jahren formieren werden.

Die deutsche Politik hat diesen Aspekt erkannt und sorgt für einen Abgleich zwischen der Industrial Internet Reference Architecture (IIRA) des Industrial Internet Consortium (IIC) aus den USA und der deutschen Initiative RAMI 4.0 mit ersten Erfolgen.

Kasten 1: IoT-Evolution – Ein Ausblick

Literatur & Links

[Atz10] L. Atzori, A. Iera, G. Morabito, The Internet of Things, A survey, Computer Networks 54, 15, 2010, 2787–2805

[Cisc] D. Evans, The Internet of Things, How the Next Evolution of the Internet is Changing Everything, 2011, siehe:

http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[SAP] R. Howells, The business case for IoT, SAP, 2015, siehe:

<http://scn.sap.com/community/business-trends/blog/2015/06/18/the-business-case-for-iot>

[VDI] Status Report: Reference Architecture Model Industrie 4.0 (RAMI4.0), VDI, 2015, siehe:

https://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gma_dateien/5305_Publikation_GMA_Status_Report_ZVEI_Reference_Architecture_Model.pdf

schen den Komponenten und das Testen von kritischen Funktionen, nicht aus. Referenzarchitekturen müssen übergeordnete Anforderungen an Performanz, Robustheit, funktionale Sicherheit, Integrität und Authentizität der Nachrichtenübermittlung gewährleisten. Realisiert wird dies unter anderem durch eine zertifikatsbasierte Architektur, bei der jede Meldung mit einer digitalen Unterschrift versehen wird, und somit von den Empfängern auf Gültigkeit überprüft werden kann.

Fazit: IoT braucht Referenzarchitekturen

Das IoT nimmt Gestalt an! Industrie- und Hausautomatisierung, car2x-Kommunikation oder eingebettete Medizintechnik nutzen schon heute technische Ansätze, Konzepte und Strukturen, die sich allerdings in vielen Fällen derzeit isoliert entwickeln. Nötig sind Abstraktionen für das IoT auf Basis von Architekturen und skalierbaren Komponenten-Schnittstellen und Werkzeugen. Dazu müssen sich die heute abstrakt wirkenden Architektur-Modelle auf die An-

wendung zubewegen, um schrittweise Akzeptanz in der Praxis zu erlangen. Neben einem Henne-Ei-Problem wirft dies Fragen nach den entscheidenden Treibern auf.

Auch wirtschaftliche Interessen sind offenkundig: IoT-taugliche Gerätehardware ist heute leicht verfügbar. Offen ist, mit welcher Geschwindigkeit sich die Technologie-Stacks, Schnittstellenbeschreibungen und Cloud-Lösungen weiterentwickeln. Echtzeitbetriebssysteme und Komponenten allein sind nicht die Antwort, eher komplette Entwicklungsumgebungen, die fall-spezifisch angepasst werden können. Dies gilt für die M2M-Technologien, Cloud-Lösungen sowie für Entwicklungswerkzeuge. AUTOSAR ist ein Beispiel aus dem Automobilbereich, der solch eine standardisierte und skalierbare Echtzeit-Umgebung bereits realisiert hat. Mangels tragfähiger Alternativen wird diese Plattform auch in anderen Anwendungsfeldern, wie dem Bahnbereich, auf ihre Einsatztauglichkeit hin geprüft.

In Deutschland hat hier die Politik bereits das Heft in die Hand genommen und sorgt für eine Synchronisation der Anwendungs-

orientierten RAMI-4.0-Architektur mit der wichtigen amerikanischen Initiative IIRA des IIC. Denn ein wichtiger Antrieb ist eine effiziente und sichere Kommunikation und Datenhaltung. Ein durchgängiger Kommunikations-Stack und Datenhaltungslösungen in der Cloud haben das Potenzial, Referenzarchitektur anzutreiben. Neben den technischen Fragen zu Performanz und Stromverbrauch ist dabei die IT-Sicherheit eine kritische Randbedingung.

Dieser Beitrag zeigte anhand von Anwendungsfällen des IoT, wie sich die Anforderungen verdichten, und wie mögliche Referenzarchitekturen für IoT-Systeme aussehen werden. Wir haben bewusst eine breite Palette dieser Architekturen vorgestellt und bewertet, wohl wissend, dass beispielsweise Open-Source-Umgebungen nicht überall zum Einsatz kommen können. Zukünftige Anwendungen aus dem Bereich der Big-Data-Analyse und virtuelle Mensch-Maschine-Schnittstellen machen diese Betrachtung noch komplexer.

Aufgrund der individuellen Charakteristiken der genannten Anwendungen ist bisher

Die Autoren



|| Michael Weyrich
(michael.weyrich@ias.uni-stuttgart.de)
lehrt an der Universität Stuttgart und ist Leiter des Instituts für Automatisierungstechnik und Softwaresysteme der Universität Stuttgart. Prof. Dr. Weyrichs Forschungsschwerpunkte liegen im Bereich von Flexibilität und Verlässlichkeit von Automatisierungssystemen und Engineering von Cyber-physischen Automatisierungssystemen.



|| Tobias Jung
(tobias.jung@ias.uni-stuttgart.de)
ist Wissenschaftlicher Mitarbeiter am Institut für Automatisierungstechnik und Softwaresysteme der Universität Stuttgart und absolvierte ein Masterstudium in Elektro- und Informationstechnik an der Universität Stuttgart.



|| Christof Ebert
(christof.ebert@vector.com)
ist Geschäftsführer der Vector Consulting Services GmbH. Er unterstützt Unternehmen weltweit bei der Optimierung ihrer Produktentwicklung und Produktstrategie sowie im Veränderungsmanagement. Prof. Dr. Ebert lehrt an der Universität Stuttgart und arbeitet in verschiedenen industriellen Aufsichtsgremien.

noch keine umfassende Standardisierung, die auch viele Facetten des IoT betreffen wird, verfügbar. Stattdessen gibt es derzeit viele Insellösungen und erste „Testbeds“ integrierter Anwendungen. Ein erster Schritt in Richtung Standardisierung könnten semantische Beschreibungen insbesondere der Schnittstellen von IoT-Komponenten sein. Standardisierte Sprachen wie Vorto oder Weave sind wichtig, um Geräte, Parameter, Benutzerschnittstellen und so weiter, zu beschreiben.

Das IoT ist heute die disruptive Technologie, die sowohl die Software als auch unsere Gesellschaft verändert. Geschäfte, Städte und sogar Staaten steigen derzeit in diese vernetzte Digitalisierung ein und versuchen, die Entwicklung gerade auch anhand politischer Randbedingungen wie Informationssicherheit und Überbrückung des „Digital Divide“ zu gestalten. Vernetzung ist nicht genug. Vernetzung hängt von der Software, die die Informationen sammelt und aufbereitet, ab. Diese Software muss so entwickelt werden, dass sie den spezifischen Bedürfnissen des IoT und seiner rasch wachsenden Anwendungsfelder und Benutzer genügt. ||