Prof. Dr. Ina Schieferdecker *14. Juni 2016*

Herausforderungen des IoT-Testings

© everythingpossible / Fotolia.com

Das Internet of Things (IoT) ist in aller Munde. Marktschätzungen gehen für das Jahr 2016 von weltweiten Umsätzen mit Technologien und Services rund um IoT von 235 Milliarden Dollar aus [1]. Allein für Deutschland eröffnet sich bis 2025 bei der Digitalisierung der Industrie ein zusätzliches kumuliertes Wertschöpfungspotenzial von 425 Milliarden Euro, für Europa sind es sogar 1,25 Billionen Euro [2]. Nach der Studie von VisionMobile in 2014 [3] beschäftigen sich 2016 bereits 1,5 Mio. Entwickler mit IoT. Bis 2020 werden es 4,5 Mio. sein. Entsprechend dem aktuellen Survey der IoT Communities bei Eclipse, IEEE und der EU werden sich die Mehrzahl mit Java, JavaScript, C oder Python beschäftigen und offene Hardware nutzen oder zu offener IoT-Software beitragen. Als Top-Anforderungen werden hierbei Sicherheit, Interoperabilität und Konnektivität gesehen, wobei unter den Antwortenden, die bereits eigene IoT-Lösungen am Markt haben, die Leistungsfähigkeit der IoT-Lösungen an die dritte Stelle rückt.

Lassen Sie uns diese vier Anforderungen – also Sicherheit, Interoperabilität, Konnektivität und Leistungsfähigkeit – aus Test-Sicht beleuchten und dazu mit einer Grobarchitektur für IoT-Lösungen mit Blick auf Kommunikationsstrukturen beginnen. Diese Grobarchitektur nutzt Anleihen der IoT-Architekturvorschläge des europäischen F&E-Projekts IoT-A [4], von CISCO [5] und Eclipse [6].

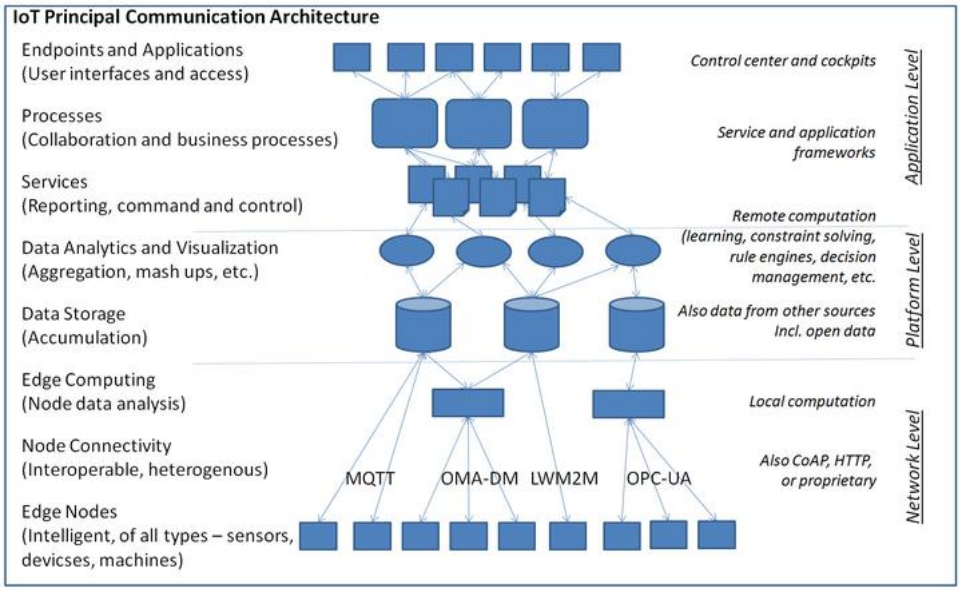

Abb.1: Grobarchitektur der Kommunikationswege in IoT-Lösungen. © Prof. Dr. Ina Schieferdecker

Die eigentliche Netzwerkschicht geht von Knoten und deren Konnektivität bis hin zu Gateways, die auch für das Edge Computing genutzt werden können. Darüber werden Daten und Informationen in das Backbone, der Plattformschicht, gegeben bzw. aus der Plattformschicht empfangen. Auf den Plattformen setzt die Anwendungsschicht mit ihren

Autor

Prof. Dr. Ina Schieferdeck

Prof. Dr.-Ing. Ina Schieferdecke
Director of Fraunhofer FOKUS, B
and is Professor for Model-Drive
Engineering and Quality…
>> Weiterlesen

Publikationen

Model-Based Testing for Embe
Systems Computational Analys
Synthesis, and Design of Dyna
Systems

Testing of Communicating Sys
XIV: Application To Internet
Technologies And Services IFI
Advances in Information and
Communication Technology, Ba

Model-Driven Testing: Using th
Testing Profile by Paul Baker

Newsletter

Unser Newsletter informiert regelmäßig und kostenlos üb Neuigkeiten, Artikel und Veranstaltungen zu aktuelle Themen.

Diensten, automatisierten Prozessen, Applikationen und Endgeräten auf.

Fragen der Konnektivität beziehen sich insbesondere auf die Protokolle im Anschluss der einzelnen Knoten, wobei nach der IEEE/Eclipse-Studie [6] der Hauptteil TCP/IP (70.9%) nutzt, was über WiFi (67.0%), Ethernet (54.7%), Bluetooth (54.7%) und Cellular (32.6%), aber auch ZigBee (25.4%), Serial (24.5%) und zunehmend LPWAN (17.3%) und 6LoWPAN (16.2%) geht. Für die IoT-Nachrichten werden insbesondere HTTP (61.2%) und MQTT (52.4%) genutzt, aber auch CoAP (21.2%), HTTP/2 (19.2%) AMQP (13.9%) und XMPP (13.2%) als auch proprietäre Protokolle (15.5%).

Auch wenn die Grobarchitektur Ebenen nutzt, ist sie nicht hierarchisch und statisch wie beispielsweise bei SCADA (Supervisory Control and Data Acquisition)-Systemen zu verstehen, sondern dienstbasiert, offen und flexibel, so dass die Komponenten, Dienste und Systeme einer IoT-Lösung in sich dynamisch ändernden Umgebungen verschiedene Verbindungen und Konfigurationen eingehen können.

Eine andere Sicht auf IoT-Architekturen bietet FIWARE (Future Internet Ware) [7], welches sowohl die zentrale Rolle der Daten und Dienste als auch den Kontext des gesamten IoT-Ökosystems, inklusive Sicherheit, Vertrauenswürdigkeit und Management, herausstellt. Diese Sicht verdeutlicht unter anderem, wie zentral für das IoT die Sicherheit der Lösungen und die genutzten Daten sind. Insbesondere auf Daten beruhen die IoT-Mehrwertdienste und -angebote. Technisch geht es hier um die Qualität der Daten und der sie beschreibenden Metadaten wie Aktualität, Genauigkeit, Passfähigkeit oder Integrität. Aus Sicht des Datenschutzes geht es ebenso um den Schutz der gesellschaftlich, unternehmerisch oder persönlich kritischen Daten, um die Wahrung der Privatheit und die Etablierung der Vertrauenswürdigkeit einer IoT-Lösung.

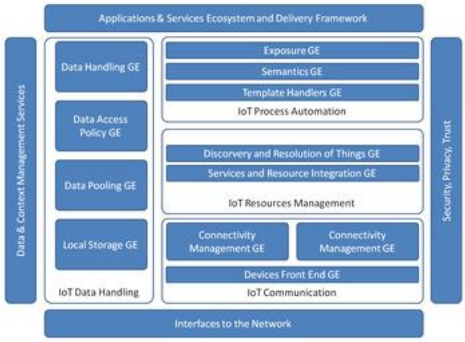

Abb.2: Generic Enables der FIWARE IoT-Dienstplattform. © Prof. Dr. Ina Schieferdecker

Unabhängig von den technologischen Ausprägungen, steht das Qualitätsmanagement für IoT vor völlig neuen Anforderungen. Entlang des IoT werden bisher geschlossene Systeme geöffnet und zu Systemen-von-Systemen verbunden. Dabei ist eine nachweislich gesicherte Ende-zu-Ende-Qualität für die Funktionalität, Interoperabilität, Robustheit, Sicherheit und Vertrauenswürdigkeit nötig, da sich IoT-Infrastrukturen zu kritischen Infrastrukturen entwickelt haben; sie sind beispielsweise untrennbar mit der Energieversorgung im Rahmen von Smart Grids, virtuellen Kraftwerken oder Smart Metering verknüpft.

Diese Herausforderungen ergeben im Wesentlichen eine erhöhte Bedeutung von Tests auf extra-funktionale Eigenschaften wie Sicherheit oder Leistungsfähigkeit. Eine erste Analyse der Ähnlichkeiten und Unterschiede beim Testen von IoT-Lösungen ist in der folgenden Tabelle beschrieben.

Tabelle 1: Besonderheiten des IoT-Testens in Ergänzung zu klassischem Protokoll-Testen (vor allem auf Konformität und Interoperabilität) und Software-Testen (vor allem auf Funktionalität)

IoT-Schicht	Besonderheiten	Testvarianten neben klassischem Software- und Protokoll-Testen
Geräte und Konnektivität	Hoher Stellenwert der Sicherheit, Konformität/Interoperabilität und Datenqualität	Real-Time Testing, Embedded Systems Testing, GUI Testing (für Management Software), Security Testing
Plattform (Computation-, Aggregation- und Storage-Dienste)	Hoher Stellenwert der Sicherheit, Konformität/Interoperabilität und Verfügbarkeit	Performance und Scalability Testing, Services Testing, GUI und Usability Testing (für Management Software), Security Testing

Nachrichten

31.01.2021
IT-Tage 365: Die Konferen die sich an Dein Leben anpasst
Du möchtest Dich fortbilden? Du möchtest Konferenz-Vorträge hö und sehen, wann und wo es für gut passt? Die IT-Tage 365 als...
>> Weiterlesen

31.01.2021
DevOps-Konferenz 2021: DevOps-Tage
DevOps-Konferenz: Am 24. und 25.02.2021 finden die DevOps-T statt. Das Besondere daran: Du kannst nicht nur von jedem Ort teilnehmen,...
>> Weiterlesen

13.01.2021
Fortbildung: Software-Entwicklung und IT-Betrie kostengünstig, remote und flexibel
On-Demand-Konferenz des Fachmagazins Informatik Aktue Software-Architektur und Entwi Datenbanken, Agile, DevOps un Betrieb...
>> Weiterlesen

IoT-Schicht	Besonderheiten	Testvarianten neben klassischem Software- und Protokoll-Testen
Applikationen (Analytics, Visualization und Control)	Hoher Stellenwert der Sicherheit und Nutzbarkeit	GUI, Usability und (mobile) App Testing, Performance und Scalability Testing, Security Testing

Neben den Software- und Vernetzungsaspekten einer IoT-Lösung ist zudem oftmals ihre Robustheit und Verlässlichkeit in harschen und unsicheren Umgebungen zu prüfen, beispielsweise dann, wenn eine IoT-Lösung im Außenraum, wie z. B. an Straßenlaternen oder Verkehrssignalanlagen, genutzt wird. Auch die Absicherung von IoT-Lösungen in dynamischen Konfigurationen, die sich beispielsweise aus dem Ausfall oder der Hinzunahme von IoT-Geräten ergeben, stellen eine Herausforderung dar. Letztendlich führt das dazu, dass IoT-Lösungen nicht mehr allein während der Entwicklung und im Labor getestet und abgesichert werden können. Es erfordert eine Verlängerung der Qualitätssicherung in die Laufzeitumgebung hinein – mit Laufzeittests (sogenannten Online-Tests), die über ein traditionelles Monitoring hinausgehen und auch als Safe Guards funktionieren können. Dabei nutzen die Komponenten einer IoT-Lösung Wissen (in Komponenten-internen Modellen repräsentiert) über ihre Konfiguration und Umgebung zur Herleitung oder Anpassung der Laufzeittests.

Wir kennen alle die 5-zeiligen Code-Fragmente, deren vollständiger Test selbst bei leistungsfähigsten Rechnern Jahre dauern würde. Entlang des IoT ergeben sich so weitere Dimensionen der Komplexität: Anzahl und Arten der Geräte, Protokollvarianten in den Netzstrukturen und deren Topologien, Varianten in den Edge Computing- und Cloud-Diensten, etc. So wird eine systematische Risikoanalyse zu einer notwendigen Voraussetzung für die sinnvolle Planung und Nutzung der Qualitätssicherungsressourcen. Ein modellbasiertes Verfahren zur Risikoanalyse haben wir beispielsweise im EU-Projekt RASEN [8] entwickelt.

Für die Automatisierung von Tests für die Absicherung von IoT-Lösungen setzen wir nach wie vor auf TTCN-3 [9]. Mit dieser Testtechnologie können hochkomplexe, vernetzte und verteilte Softwarebasierte Systeme, wie die oben beschriebenen IoT-Lösungen auf Komponenten-, Plattform- und Systemebene systematisch geprüft werden. TTCN-3 bietet neben der Möglichkeit, formalisierte Testspezifikationen in verschiedenen Präsentationsformaten zu beschreiben (textuell à la Skriptsprache oder graphisch in Form von Sequenzdiagrammen), auch eine Referenzimplementierungsarchitektur. Sie ermöglicht Testlösungsanbietern, z. B. Testgeräteherstellern, diese Teststandards effizient zu implementieren und Nutzern zur Verfügung zu stellen. Zum Testen von verteilten Systemen haben wir u. a. die Test Control Interfaces TCI [10] für TTCN-3 entwickelt. Für das Testen von eingebetteten Systemen haben wir Erweiterungen für Real-Time und für Streams [11] erarbeitet sowie eine Erweiterung zum Fuzz Testing für Sicherheitstests [12] entwickelt. So wird TTCN-3 u. a. von ETSI für die Absicherung von OneM2M-Implementierungen [13, 14] genutzt.

Mit der Öffnung der TTCN-3 Werkzeugumgebung Titan durch Ericsson in Eclipse [15], das bereits Teil des IoT-Frameworks von Eclipse6 ist, steht eine Grundlage zur Automatisierung von IoT-Tests zur Verfügung. Fraunhofer FOKUS entwickelt IoT-Testware unter Weiterentwicklung der Testtechnologie TTCN-38 und als Anbindung an das IoT Eclipse Framework6. Zusammen mit DEKRA und IoT-Anbietern wird zudem ein Produktzertifizierungsprogramm erarbeitet. Die Entwicklung eines Ausbildungsschemas für das Quality Engineering von IoT-Lösungen hat in einer Arbeitsgruppe von ASQF [16] und GTB [17] u. a. mit Experten von DB Systel, SAP Deutschland und Atos Deutschland, Sulzer GmbH, imbus AG und tecmata GmbH begonnen.

Quellen

[1] Computerwoche: Gartner-Studie - Das Internet of Things wächst rasant
[2] Roland Berger: Die digitale Transformation kann Europas industrielle Wertschöpfung bis 2025 um 1,25 Billionen Euro erhöhen – oder um 605 Milliarden Euro schmälern
[3] Vision mobile: What the Internet of Things is NOT about
[4] EU FP7 Projekt: Internet of Things Architecture
[5] Cisco-Blog: Maciej Kranz: IoT Meets Standards, Driving Interoperability and Adoption
[6] Eclipse IoT Framework
[7] EU Projekt: FI-WARE
[8] RASEN: Compositional Risk Assessment and Security Testing of Networked Systems
[9] Testing and Test Control Notation, eine bei ETSI und ITU standardisierte Testtechnologie
[10] Schieferdecker, I. K. & Vassiliou-Gioles, T.: Realizing distributed TTCN-3 test systems with TCI Testing of Communicating Systems, Springer, 2003, 95-109.
[11] Grossmann, J.; Serbanescu, D. A. & Schieferdecker, I. K.: Testing Embedded Real Time Systems with TTCN-3 Second International Conference on Software Testing Verification and Validation, ICST 2009, Denver, Colorado, USA, April 1-4, 2009, 2009, 81-90.

[12] Rennoch, A.; Schieferdecker, I. K. & Großmann, J.: Security Testing Approaches -- For Research, Industry and Standardization Trustworthy Computing and Services, Springer, 2014, 397-406
[13] oneM2M Organisation
[14] ETSI oneM2M TTCN-3 test specification
[15] Titan ist eine TTCN-3 Übersetzungs- und Ausführungsumgebung mit einer Eclipse-basierten IDE
[16] Arbeitskreis Software-Qualität und -Fortbildung
[17] German Testing Board

Autor

Prof. Dr. Ina Schieferdecker

Prof. Dr.-Ing. Ina Schieferdecker is Director of Fraunhofer FOKUS, Berlin and is Professor for Model-Driven Engineering and Quality Assurance of Software-Based Systems at Freie Universität Berlin.
>> Weiterlesen

Publikationen

- Model-Based Testing for Embedded Systems Computational Analysis, Synthesis, and Design of Dynamic Systems
- Testing of Communicating Systems XIV: Application To Internet Technologies And Services IFIP Advances in Information and Communication Technology, Band 82
- Model-Driven Testing: Using the UML Testing Profile by Paul Baker

Das könnte Sie auch interessieren

IoT Data Streaming – Warum MQTT und Kafka eine exzellente Kombination sind

IoT zum Anfassen – Von der Maschine in die Cloud

MQTT Deployments in containerbasierten Anwendungsplattformen wie OpenShift

Anomalie-Detektion in IoT-Traffic

RFID – Anwendungsgebiete

IoT-Security und der User-Experience-Fluch

Kommentare (0)

Neuen Kommentar schreiben

Name:

E-Mail-Adresse:

Kommentar:

Ich verstehe und akzeptiere die Datenschutzbestimmungen.

Absenden