Prof. Dr.-Ing. Ina Schieferdecker
(ina.schieferdecker@german-testing-board.info)
ist Präsidentin des ASQF und leitet gemeinsam mit Prof. Dr. Manfred Hauswirth das Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS), Berlin. Sie ist Mitglied des German Testing Board und hat die IoT-QE Arbeitsgruppe beim ASQF und GTB initiiert. Ihr persönliches Engagement gilt darüber hinaus der Aus- und Weiterbildung von Softwaretestern sowie der Weiterentwicklung von Lehrplänen und Qualifizierungsschemata im Software Engineering.

Dr. Armin Metzger
(armin.metzger@asqf.de)
Seit mehr als 20 Jahren beschäftigt sich Dr. Armin Metzger, Referent des ASQF, mit der konstruktiven und analytischen Qualität von Systemen. Als Vorsitzender des German Testing Board ist er darüber hinaus seit vielen Jahren an der Entwicklung hochqualitativer Trainingsschemata wie zum Beispiel des Certified Tester beteiligt.

Axel Rennoch
(axel.rennoch@fokus.fraunhofer.de)
ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS) in Berlin. Als Projektleiter im Geschäftsbereich SQC ist er beteiligt an Validierungs- und Testprojekten künftiger Kommunikationsnetzwerke und Softwaretechnologien.

Das Ende der Unsicherheit – Quality Engineering für IoT

Das Internet der Dinge (Internet of Things, IoT) stellt Gesellschaft und Industrie vor große Herausforderungen. Ungeklärt ist beispielsweise, wie die mannigfaltigen Schnittstellen im IoT auch mit bestehenden IT-Systemen verbunden, genutzt und nicht zuletzt getestet und weiterentwickelt werden können. Auch die gesellschaftlichen Rahmenbedingungen wie Fragen der Sicherheit, des Datenschutzes und sogar der Ethik werden das Thema IoT formen. Um der Industrie Hilfe in Form von Methoden, Leitlinien zur Qualitätssicherung und Absicherung von IoT-Lösungen durch Qualifizierungsschemata und ein Glossar als De-facto-Standard anzubieten, hat sich ein Expertengremium führender Unternehmen in Deutschland gebildet, unter anderem mit DB Systel GmbH, SAP Deutschland und Atos Deutschland sowie mit namhaften Dienstleistern wie Sulzer GmbH, imbus AG, tecmata GmbH, sepp.med GmbH und dem Konsortium Testing4You.

Gründung der Arbeitsgruppe IoT-QE

Auf Einladung des ASQF und in Kooperation mit dem German Testing Board (GTB) und Fraunhofer FOKUS erarbeiten namhafte Treiber und Experten der Digitalisierung in der Industrie ein neues Ausbildungsschema für IoT. Wichtig ist der Gruppe „Quality Engineering für das Internet der Dinge (kurz IoT-QE)“ nicht die reine Validierung „am Ende“, sondern die vorausschauende Erlangung von Qualitätskriterien für das Internet der Dinge von den ersten Entwicklungsschritten an. So spielt beispielsweise die Priorisierung der relevanten Qualitätskriterien einer IoT-Lösung eine entscheidende Rolle.

Die Zusammensetzung der Arbeitsgruppe – alles Mitglieder des GTB oder des führenden Software- und System-Qualitäts-Gremiums ASQF – soll sicherstellen, dass das Thema aus allen relevanten Blickwinkeln betrachtet wird: Geschäftsprozesse, Systementwicklung, Absicherung, Betrieb wie auch Forschung und Entwicklung, die durch IoT geprägt sind. Dadurch wird ein Schema entstehen, das einen Foundation-Level-Einstieg ermöglicht. Es vermittelt einen Überblick und die Kenntnisse über die relevanten Aspekte des Themas Quality Engineering für das Internet der Dinge.

Was ist IoT?

Aber was ist eigentlich das Internet der Dinge? Die IEEE hat im Mai 2015 ein bald 100 Seiten langes Dokument zur Suche nach einer Definition veröffentlicht. Diese Suche ist nicht nur bei der IEEE noch nicht abgeschlossen, sodass es ein wesentliches Ziel der IoT-QE-Arbeitsgruppe ist, aus Qualitätssicht einen gemeinsamen Nenner und eine gemeinsame Sprechweise aus den unterschiedlichen Aussagen zu IoT zu extrahieren. Dazu werden unter anderem relevante Standards reflektiert, wie zum Beispiel (in alphabetischer Reihenfolge):

- ETSI (European Telecommunications Standards Institute, http://www.etsi.org/) – u.a. M2M
- IEEE (Institute of Electrical and Electronics Engineers, https://www.ieee.org/) – IoT Definition
- IETF (Internet Engineering Task Force, https://www.ietf.org/) – Internet Protocols for IoT
- IIC (Industrial Internet Consortium, http://www.iiconsortium.org/) – Industrial Internet
- ISO (International Organization for Standardization, http://www.iso.org) / IEC (International Electrotechnical Commission, http://www.iec.ch) – Internet of Things Reference Architecture

- ITU (International Telecommunication Union, http://www.itu.int) – Internet of Things Global Standards Initiative
- NIST (National Institute of Standards and Technology in den USA, http://www.nist.gov/) – unter anderem IoT-Enabled Smart City Framework
- OASIS (Advancing Open Standards for the Information Society, https://www.oasis-open.org/) – u.a. IoT/M2M und Security
- OneM2M (Global Initiative for Machine-to-Machine Standardization, http://www.onem2m.org/) – M2M für IoT
- W3C (World Wide Web Consortium, https://www.w3.org/) – Web of Things

Anstelle einer Definition liefert IEEE eine Beschreibung für IoT [IEEE]:

„An IoT is a network that connects uniquely identifiable ‚Things' to the Internet. The ‚Things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the ‚Things' can be collected and the state of the ‚Things' can be changed from anywhere, anytime, by anything."

und gibt eine Sammlung von Eigenschaften zur Charakterisierung der Dinge im IoT an:

- Verbindung von Dingen untereinander
- Verbindung von Dingen mit dem Internet
- Eindeutige Identifizierbarkeit von Dingen
- Allgegenwärtigkeit der vernetzten Dinge
- Fähigkeit zum Messen und Steuern durch die Dinge
- In die Dinge eingebettete Intelligenz
- Interoperable Kommunikation zwischen den Dingen
- Selbstkonfigurierbarkeit der Dinge
- Programmierbarkeit der Dinge

Auch wenn das IoT maßgeblich die Dinge in den Blick nimmt, muss eine Definition weiter greifen: Neben der Vernetzung, Identifikation, Beobachtung und Steuerung von Dingen geht es ebenso um die Vernetzung, Identifikation, Beobachtung und Steuerung von Daten und Prozessen. Damit muss eine Definition für IoT auch Automatismen einer neuen Qualität und Reichweite umfassen. In diese Richtung schaut auch ISO/IEC JTC1 [ISO]:

„An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react."

Kurz vorgestellt: IoT Principal Communication Architecture

Die IoT-QE-Arbeitsgruppe um ASQF, GTB und Fraunhofer FOKUS nimmt daher in einem ersten Ansatz die wesentlichen Komponenten einer IoT-Lösung und deren Vernetzung in den Blick. Die entsprechende initiale Grobarchitektur (vgl. Abbildung) nutzt Anleihen der IoT-Architekturvorschläge des europäischen F&E-Projekts IoT-A [FP7], von CISCO [Kra] und Eclipse [Ecl].

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, die Plattformschicht, gegeben bzw. aus der Plattformschicht empfangen. Auf den Plattformen setzt die Anwendungsschicht mit ihren Diensten, automatisierten Prozessen, Applikationen und Endgeräten auf.

Auch wenn die Grobarchitektur Ebenen nutzt, ist sie nicht hierarchisch und statisch

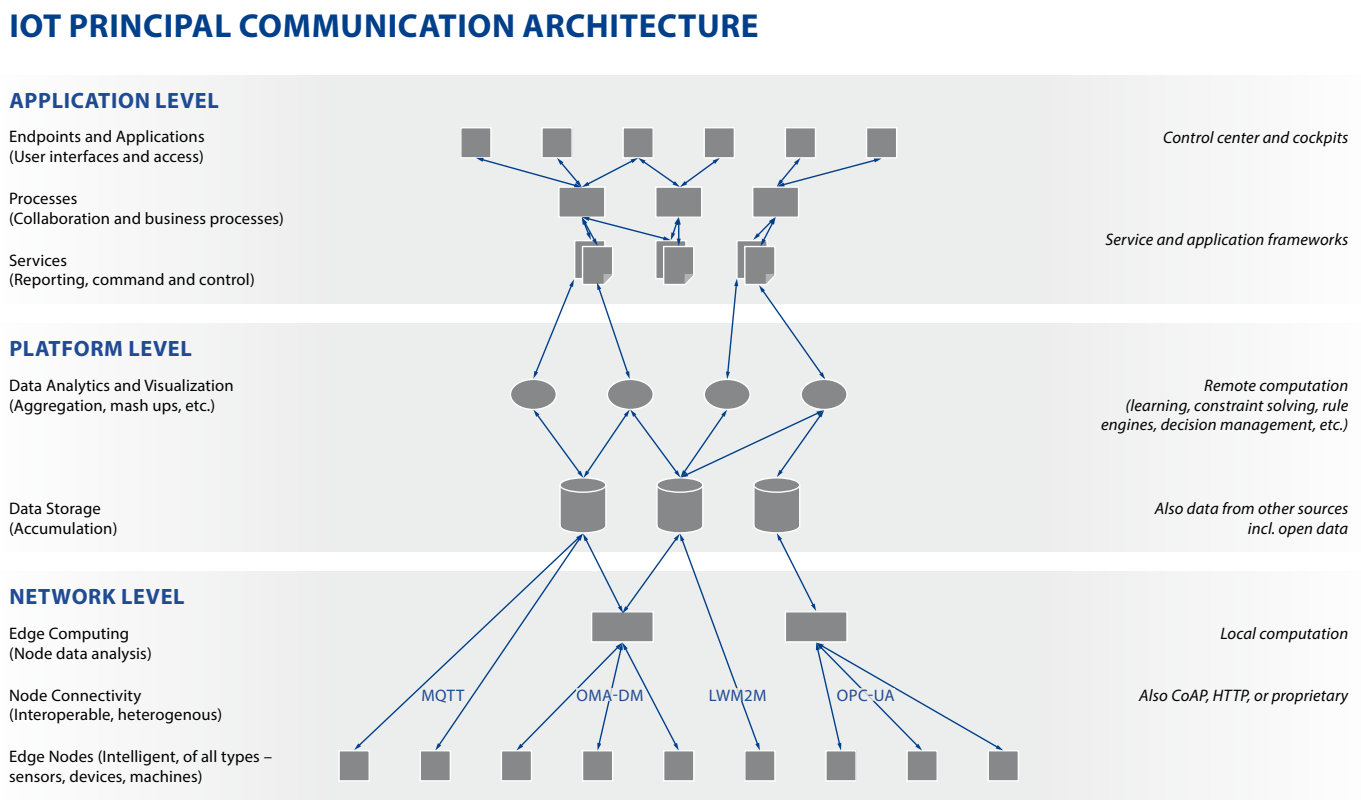

Abb.: Grobarchitektur der Kommunikationswege in IoT-Lösungen der IoT-QE-Arbeitsgruppe

wie beispielsweise bei SCADA-(Supervisory Control and Data Acquisition-) Systemen zu verstehen, sondern dienstbasiert, offen und flexibel. Damit können die Komponenten, Dienste und Systeme einer IoT-Lösung in sich dynamisch ändernden Umgebungen verschiedene Verbindungen und Konfigurationen eingehen. Die strukturelle Dynamik ist hierbei eine der wesentlichen spezifischen Eigenschaften, die ein effektives Quality Engineering für IoT beachten muss.

Qualitätsmanagement für IoT

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 und werden in Zukunft auch verstärkt in alle Bereiche des täglichen Lebens eindringen, zum Beispiel auch den Autoverkehr.

Diese Herausforderungen resultieren im Wesentlichen in einer erhöhten Bedeutung von Tests auf extrafunktionale Eigenschaften wie Sicherheit oder Leistungsfähigkeit. Eine erste Analyse der Ähnlichkeiten und Unterschiede beim Testen von IoT-Lösungen ist in Tabelle beschrieben. 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 zum Beispiel 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, stellt eine Herausforderung dar. Letztendlich führt das dazu, dass IoT-Lösungen nicht mehr alleinig während der Entwicklung und im Labor getestet und abgesichert werden können, sondern eine Verlängerung der Qualitätssicherung in die Laufzeitumgebung hinein erforderlich ist.

Dazu sind Laufzeittests (sogenannte Online-Tests) zu entwickeln, die über ein traditionelles Monitoring hinausgehen und auch als Safe Guards fungieren können. Zudem sind Predictive-Maintenance-Aspekte qualitätsorientiert abzusichern. Dabei nutzen die Komponenten einer IoT-Lösung Wissen (in Komponenten-internen Modellen repräsentiert) über ihre Konfiguration und Umgebung zur Herleitung oder Anpassung der Laufzeittests. Die noch relativ junge Initiative zum kombinierten Entwickeln und Betreiben von Software-basierten vernetzten Systemen DevOps (Development and Operations) [Lou] adressiert genau diese Herausforderung des engen Beieinanders von kontinuierlicher, häufiger und systematischer Weiterentwicklung, Betrieb und Absicherung. Darüber hinaus sind die neuen Anforderungen auch mit den Möglichkeiten vorhandener Testbeschreibungstechniken wie TTCN-3 [Test] zu vergleichen.

Das IoT Quality Engineering-Schema

Zur Erarbeitung der wesentlichen Aspekte zur konstruktiven und analytischen Qualitätssicherung für IoT-Lösungen wird sich die Arbeitsgruppe mit den folgenden Themenblöcken beschäftigen:

- **Motivation:** Warum Quality Engineering für das Internet der Dinge?
- **Kontext:** Welche Architekturen werden für IoT-Lösungen genutzt? Welche Qualitätsmerkmale werden gefordert?
- **Prozesse:** Wie werden IoT-Lösungen mit Blick auf die Geschäftsprozesse konzipiert, entwickelt, betrieben, weiterentwickelt und abgesichert? Wie wird dabei mit der Interdisziplinarität und der Kritikalität der IoT-Lösungen umgegangen?
- **Konstruktive Qualitätssicherung:** Wie können IoT-Lösungen von vornherein robust, skalierbar, funktional sicher, IT-sicher und vertrauenswürdig entwickelt werden? Welche Methoden und Werkzeugklassen können genutzt werden?
- **Analytische Qualitätssicherung:** Wie können die geforderten Qualitätsmerkmale in der (Weiter-)Entwicklung und im Betrieb überprüft und abgesichert werden? Welche Methoden und Werkzeugklassen können genutzt werden?

Das IoT-Quality Engineering-Schema (kurz IoT-QE) wird im Unterschied zu anderen bereits bestehenden IoT-Zertifikaten [Vil] wie zur Entwicklung oder zur IT-Sicherheit von

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 ▪ Service Testing ▪ GUI und Usability Testing (für Management-Software) ▪ Security Testing
Applikationen (Analytics, Visualization und Control)	Hoher Stellenwert der Sicherheit und Nutzbarkeit	▪ GUI, Usability und (mobile) App Testing ▪ Performance und Scalability Testing ▪ Security Testing ▪ Crowd Testing

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

IoT-Lösungen die Sicht der Qualitätsanforderungen an IoT-Lösungen, deren Erstellung und Gewährleistung einnehmen.

Die Arbeitsgruppe hat sich im Juni 2016 konstituiert und plant einen ersten Lehrplan in etwa einem Jahr herauszubringen. Sollten Sie interessiert sein bzw. dazu beitragen wollen, schreiben Sie bitte an iot-qe@german-testing-board.info bzw. iot-qe@asqf.de. ■

Der Beitrag wurde ebenfalls in der Ausgabe des Online-Themenspecials JAVAspektrum 2016 veröffentlicht.

Literatur & Links

[Ecl] Eclipse IoT Framework, siehe http://iot.eclipse.org/, Mai 2016

[FP7] EU FP7 Projekt Internet of Things Architecture, siehe http://www.iot-a.eu/public, Mai 2016

[IEEE] IEEE: Towards a definition of the Internet of Things (IoT), Revision 1, 27.5.2015, siehe http://iot.ieee.org/definition.html

[ISO] ISO/IEC JTC1, Information technology: Internet of Things (IoT), Preliminary Report 2014, siehe http://www.iso.org/iso/internet_of_things_report-jtc1.pdf, 2015

[Kra] Kranz, Maciej: IoT Meets Standards, Driving Interoperability and Adoption, CISCO Blog, siehe http://blogs.cisco.com/digital/iot-meets-standards-driving-interoperability-and-adoption, Juli 2015

[Lou] Mike Loukides: What is DevOps?. O'Reilly Radar, 7.6.2012, siehe http://radar.oreilly.com/2012/06/what-is-devops.html

[Test] Testing and Test Control Notation für das Testen vernetzter, real-time und embedded systems, siehe http://www.ttcn-3.org/

[Vil] Villegas, Mike O.: What are the best IoT certifications for security? IoT Agenda, TechTarget, März 2016, siehe http://internetofthingsagenda.techtarget.com/answer/What-are-the-best-IoT-certifications-for-security