Quality Engineering für das Internet der Dinge

Ina Schieferdecker, Axel Rennoch, Michael Wagner

Abstrakt

Vom Internet der Dinge (Internet of Things, kurz IoT) werden umfassende Weiterentwicklungen und Umbrüche erwartet, wie sie entlang der Verbreitung des „traditionellen“ Internets in Kombination mit der Mobilkommunikation geschehen sind. So durchdringt das IoT alle Arbeits- und Lebensbereiche und liefert neue Ansätze für das Monitoring und die Steuerung der physischen Welt inklusive geschäftskritischer als auch sicherheitskritischer Systeme und Prozesse wie Energie- oder Verkehrsnetze. Daher sind die Qualitätsanforderungen an IoT-Komponenten und -Lösungen sehr hoch und müssen durch moderne Methoden zur Konstruktion und Absicherung der Qualitäten adressiert werden. Dieser Artikel gibt einen Überblick zum Verständnis von IoT und skizziert Qualitätsanforderungen und grundlegende Testansätze. Abschließend wird auf den beim ASQF und GTB in Entwicklung befindlichen Lehrplan zum IoT-Quality Engineering (IoT QE) eingegangen.

Einleitung

Nachdem das Netz der Netze ausgebaut wurde, um neben dem Austausch von Dokumenten auch den Austausch von Information und Kommunikation zwischen Personen zu ermöglichen, entwickelt es sich nun weiter zu einem Netz der Dinge und Prozesse. Damit erhalten die Elemente der realen Welt – neben Dokumenten und Personen nun auch Dinge und Prozesse – digitale Abbilder und lassen sich über die digitale Welt verketten. Nach Gartner werden im Jahr 2017 8.4 Milliarden „Dinge“ miteinander verbunden sein, im Jahr 2020 werden es 20.4 Milliarden sein [1]. Neben der Digitalisierung tritt so die Vernetzung immer mehr in den Vordergrund: Die digitale Vernetzung bezeichnet die durchgehende und durchgängige Verknüpfung der realen Welt mit der digitalen Welt. Dazu gehören die digitale Erfassung, Abbildung und/oder Modellbildung der realen Welt sowie die Vernetzung dieser Informationen. Dies ermöglicht die zeitnahe Beobachtung, Auswertung und/oder Steuerung der realen Welt mithilfe von digitalen (Teil-)Automatismen [2].

Dabei gilt nach dem Metcalfe'schen Gesetz [27], 1980: „Der Nutzen eines Kommunikationssystems ist proportional zur Anzahl der möglichen Verbindungen zwischen den Teilnehmern, während die Kosten proportional zur Teilnehmerzahl stehen. So wächst der Nutzen quadratisch, die Kosten wachsen nur linear.“ Und nach dem dritten Reedschen Gesetz [28], 1998, gilt: „Die Nützlichkeit großer Netzwerke steigt exponentiell mit ihrer Größe.“ So wirken derzeit verschiedene technische Trends auf die zunehmende Vernetzung ein:

- Cyberphysische Systeme [4] adressieren sowohl Sensorik und Aktuatorik als auch deren sichere Identifikation und Vernetzung mit der digitalen Welt.
- Mobile Edge Computing [5] optimiert die Maschine-zu-Maschine Kommunikation und Virtualisierung.

- Taktiles Internet [6] wird die Echtzeit-Steuerung von Maschinen ermöglichen.
- Software und System Quality Engineering [7] ermöglichen die Entwicklung vertrauenswürdiger IKT-basierter Produkte und Dienstleistungen.
- Smart Data und Analytik [8] erlauben Vorhersagen auf neuer qualitativer Stufe und unterstützen so Predictive Maintenance und andere Anwendungen.

Das Verständnis des Internets der Dinge hat sich über die Jahre entwickelt: 1991 formuliert Mark Weiser in „The Computer for the 21st Century“: „Das Internet der Dinge bezeichnet die Verknüpfung eindeutig identifizierbarer physischer Objekte (things) mit einer virtuellen Repräsentation in einer Internet-ähnlichen Struktur“ [9]. Im EU-Project IoT-A [13], das sich mit einer Referenzarchitektur für IoT beschäftigt, heißt es dann 2013: „The Internet of Things (IoT) is an emerging network superstructure that connects physical resources and people together with software. It will enable an ecosystem of smart applications and services that will improve and simplify the life of the citizen and will contribute to sustainable growth, provided it combines and guarantees trust and security for people and businesses.” Marktschätzungen gehen bereits für das Jahr 2016 von weltweiten Umsätzen mit Technologien und Services rund um das IoT von 235 Milliarden Dollar aus [10]. Allein für Deutschland bis 2025 eröffnet sich der Digitalisierung der Industrie ein zusätzliches kumuliertes Wertschöpfungspotenzial von 425 Milliarden Euro, für Europa sind es sogar 1,25 Billionen Euro [3]. Dabei ist das IoT nicht eine Technologie, sondern erfährt in seinen Anwendungsgebieten verschiedene Ausprägungen, die in verschiedenen Qualitätsanforderungen münden.

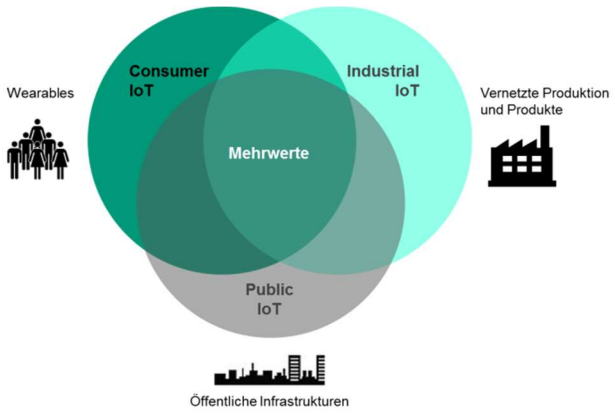

Abb. 1: IoT-Varianten

Während es im Consumer-Bereich im Wesentlichen um die Aufbereitung medialer Inhalte von sowohl persönlichen und Smart Home-Geräten als auch von sozialen Netzwerken geht, beschäftigt sich Industrial IoT entlang Industrie 4.0 mit der vernetzten Produktion und vernetzten Produkten. In Public IoT geht es vor dem Hintergrund smarter Städte und Regionen um die digitale Vernetzung öffentlicher Infrastrukturen. Dabei muss sich jede IoT-Lösung um Fragen der erzeugten bzw. generierten Daten und Metadaten und ihrer Nutzungsbestimmungen, der sicheren Identifikation, der Daten- und Systemqualität inklusive Datenschutz, IT-Sicherheit und Vertrauenswürdigkeit kümmern. In Hinblick auf die Lösungen unterscheiden sich die Anforderungen beispielsweise in Bezug auf Umgebungsanforderungen (geschützte Indoor-Bereiche oder harsche, unzuverlässige Outdoor-Verhältnisse, Leistungsanforderungen wie Echtzeit oder Skalierung und Integrations- und

Interoperabilitätsanforderungen). Gleichsam entwickelt sich eine gemeinsame Technologiebasis zu der u.a. Konnektivität unter Nutzung von CoAP (Constrained Application Protocol) [29], MQTT (vormals Message Queue Telemetry Transport) [30] oder LwM2M (Lightweight M2M) [31] gehören. Neben der Konnektivität spielen Fragen der Semantik der Dinge eine immer größere Rolle, so dass Komponenten wie die SSN (Semantic Sensor Network Ontology) erarbeitet werden.

Was ist IoT?

Aber wie genau ist eigentlich das Internet der Dinge definiert? Die IEEE hat im Mai 2015 ein bald 100 Seiten langes Dokument [11] zur Suche nach einer Definition veröffentlicht. Diese Suche ist nicht nur bei der IEEE noch nicht abgeschlossen, so dass 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 u.a. relevante Standards reflektiert, wie z.B. (in alphabetischer Reihenfolge):

- ETSI (European Telecommunications Standards Institute, http://www.etsi.org/) – u.a. M2M
- ISO (International Organization for Standardization, http://www.iso.org)/IEC (International Electrotechnical Commission, http://www.iec.ch) – Internet of Things Reference Architecture
- 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
- 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/) – u.a. 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, und
- W3C (World Wide Web Consortium, https://www.w3.org/) – Web of Things.

IEEE gibt in [1] anstelle einer Definition eine Beschreibung für IoT:

> „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 "Thing" can be collected and the state of the 'Thing' can be changed from anywhere, anytime, by anything.*"

und eine Sammlung von Eigenschaften zur Charakterisierung der Dinge in IoT:

- 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 und
- Programmierbarkeit der Dinge.

Auch wenn das IoT maßgeblich die Dinge in den Blick nimmt, so 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 [12]:

> *"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: Die IoT Principal Communication Architecture

Die wesentlichen Komponenten einer IoT-Lösung und deren Vernetzung ist in Abb. 1 dargestellt. Diese grobe Vernetzungsarchitektur nutzt Anleihen der IoT-Architekturvorschläge des europäischen F&E-Projekts IoT-A [13], von CISCO [14] und Eclipse [21].

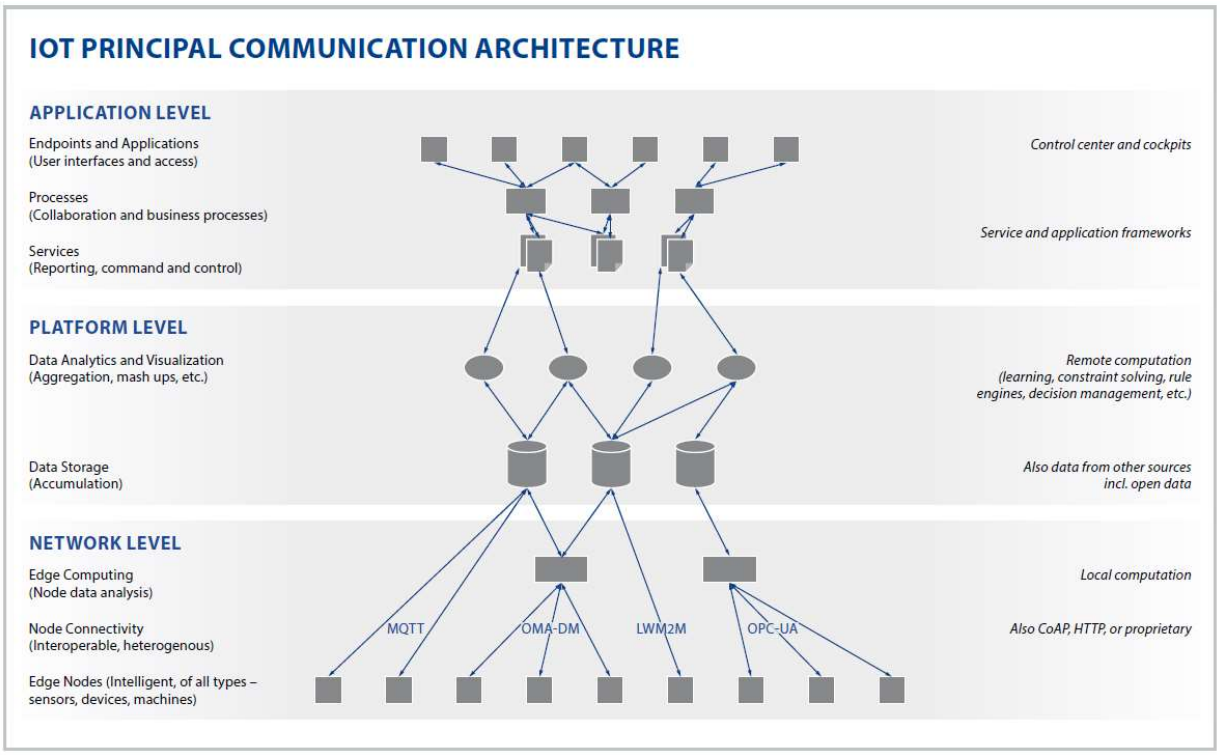

Abb. 2: Grobarchitektur der Kommunikationswege in IoT-Lösungen der IoT-QE Arbeitsgruppe

Die eigentliche Netzwerkschicht geht von Knoten und deren Konnektivität bis hin zu Gateways, die auch für das Edge Computing [32] genutzt werden können, d.h. einer Datenverarbeitung am Netzwerkrand nahe der Datenquelle. Darüber werden Daten und Informationen in das Backbone, der 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 grobe Vernetzungsarchitektur 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. 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, z.B. auch den Autoverkehr.

Diese Herausforderungen ergeben im Wesentlichen eine erhöhte Bedeutung von Tests auf extra-funktionale, d.h. nicht-funktionale, Eigenschaften wie Sicherheit oder Leistungsfähigkeit. Eine erste Analyse der Ähnlichkeiten und Unterschiede beim Testen von IoT-Lösungen ist in Tabelle 1 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
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

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 alleinig während der Entwicklung und im Labor getestet und abgesichert werden können. Es erfordert eine

Verlängerung der Qualitätssicherung in die Laufzeitumgebung hinein. Dazu sind Laufzeittests (sogenannten Online-Tests), die über ein traditionelles Monitoring hinausgehen und auch als Safe Guards funktionieren können, zu entwickeln. 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) [15] 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 [16] zu vergleichen.

IoT-Testarchitekturen

Aus der IoT Principle Communication Architecture lassen sich verschiedene Testkonfigurationen herleiten.

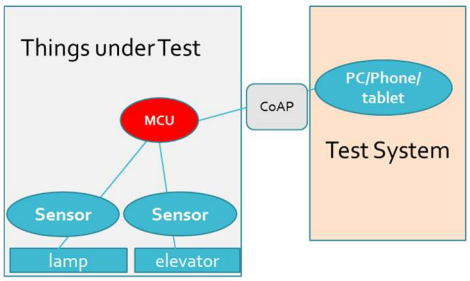

Abb. 3: IoT-Sensorkit-Testarchitektur

Bei der einfachen IoT-Testarchitektur (siehe Abb. 3) ist ein Sensorkit – eine MCU (Micro Control Unit) – das Testobjekt. Das Sensorkit wird dabei auf seine Funktions- und Kommunikationsfähigkeiten beispielsweise über CoAP, MQTT, oder LwM2M untersucht.

Die über das Internet erreichbaren IoT-Dienste stehen im Fokus der IoT-Dienst-Testarchitektur inAbb. 4. Dabei sind IoT-Gateways wie das Bosch XDK [17] oder die relayr Plattform [18] die Testobjekte. Sie werden insbesondere auf Vernetzungs-, Sicherheits- und Managementfunktionen untersucht.

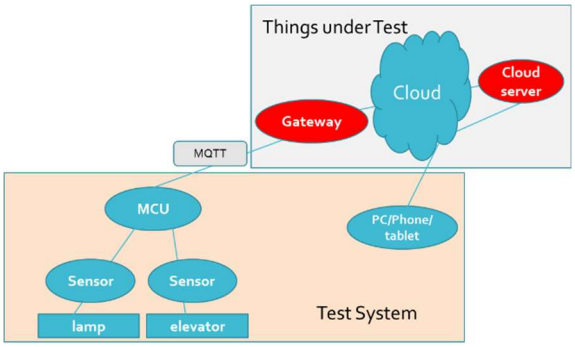

Abb. 4: IoT-Dienst-Testarchitektur

Ganze IoT-Infrastrukturen werden mit der IoT-Infrastruktur-Testarchitektur in Abb. 5 überprüft. Dabei sind die IoT-Betriebssysteme bzw. IoT-Plattformen wie die oneM2M Service Layer

Implementations [20], das RIOT Operating System [19] oder andere Plattform-Komponenten [21] die betrachteten Testobjekte.

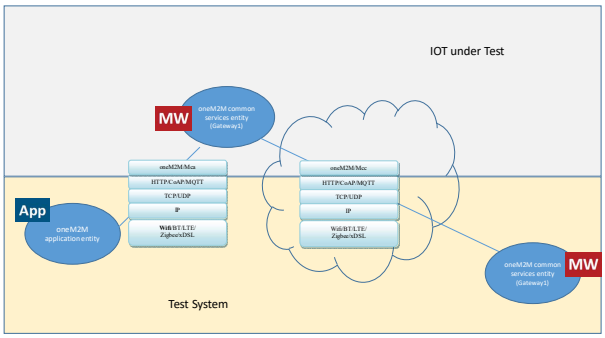

Abb. 5: IoT-Infrastruktur-Testarchitektur

Die Funktionalität, Skalierbarkeit und Sicherheit der auf IoT aufsetzenden Geschäftsprozesse kann Elemente aller drei genannten Testarchitekturen nutzen, um Zusatzinformationen auf Sensor/Aktuator-, Gateway- und/oder Plattform-Ebene zu nutzen. Testobjekte sind die Softwarekomponenten, die die Geschäftsprozesse beispielsweise unter Nutzung von kiwiw [22] realisieren.

Alle drei grundlegenden IoT-Testarchitekturen werden typischerweise virtualisiert in Cloud-Umgebungen realisiert, so dass großskalige Konfigurationen mit beispielsweise 100en oder 1000en Sensoren und Aktuatoren auf Skalierbarkeit und Leistungsfähigkeit getestet werden können.

Wie IoT basieren alle Testarchitekturen auf den Kommunikationsprotokollen des IoT und der Interoperabilität der beteiligten Hardware- und Softwarekomponenten, so dass ebenso klassische Protokolltests für MQTT, CoAP, LwM2M als auch für vergleichbare oder darunter liegende Protokolle (TCP, UDP, http, IPv4, IPv6, etc.) zum Ansatz kommen.

Das IoT-Quality Engineering-Schema

Auf Einladung des ASQF (Arbeitskreis Software-Qualität und Fortbildung [23]) und in Kooperation mit dem GTB (German Testing Board [24]) erarbeiten derzeit namenhafte Treiber und Experten der Digitalisierung in der Industrie wie von Festo, Deutscher Bahn oder Fraunhofer FOKUS 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 German Testing Boards 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 als auch Forschung und Entwicklung, welche durch IoT geprägt sind. Dadurch wird ein Schema entstehen, welches einen Foundation Level Einstieg ermöglicht, d.h. den Überblick und die Kenntnisse über die relevanten Aspekte des Themas Quality Engineering für das Internet der Dinge vermittelt.

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 wird im Unterschied zu anderen bereits bestehenden IoT-Zertifikaten [25] wie zur Entwicklung oder zur IT-Sicherheit von 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 2017/2018 herauszubringen. Sollten Sie interessiert sein bzw. beitragen wollen, schreiben Sie bitte an iot-qe@german-testing-board.info bzw. iot-qe@asqf.de.

Zusammenfassung

Die mit der zentralen Rolle von IoT-Komponenten und -lösungen verbundenen hohen Qualitätsanforderungen erfordern neue Ansätze bei deren Entwicklung, Absicherung und kontinuierliche Weiterentwicklung. Dazu gehört nicht nur die Ausbildung von Expertisen, was durch das IoT-QE-Weiterbildungsschema des ASQF und GTB adressiert wird.

Zudem sind konkrete Prüfmethoden und -werkzeuge für qualitativ hochwertige IoT-Lösungen als auch Produkt-Zertifizierungsangebote nötig, die über diverse IoT-Testlabs angeboten werden sollten. Dafür entwickelt Fraunhofer FOKUS eine IoT-Testware unter Weiterentwicklung der Testtechnologie TTCN-3 um Virtualisierungskonzepte und als Anbindung an den Eclipse Open IoT Stack for Java [26]. Die IoT-Testware wird aktuell auch als Eclipse-Projekt im Rahmen der Eclipse IoT-Projekte etabliert und wird so Open Source Test Suiten für IoT bereitstellen [33]. Zudem wird zusammen mit DEKRA und IoT-Anbietern ein Produktzertifizierungsprogramm [34] erarbeitet, dass das Weiterbildungs- und Personenzertifizierungsschema des ASQF und GTB ergänzt.

Referenzen

[1] Gartner: Internet of Things Forecast, siehe http://www.gartner.com/newsroom/id/3598917, besucht Juni 2017.

[2] Fraunhofer Leistungszentrum Digitale Vernetzung, siehe http://www.digitale-vernetzung.org/, besucht Apr. 2017.

[3] Roland Berger: Digitale Transformation in Europa, siehe http://www.rolandberger.de/pressemitteilungen/515-press_archive2015_sc_content/digitale_transformation_in_europa.html, besucht Apr. 2017.
[4] acatech: Integrierte Forschungsagenda Cyber-Physical Systems, siehe http://www.acatech.de/?id=1405, besucht Apr. 2017.
[5] ETSI: Key Technologies towards 5G, siehe http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf, besucht Apr. 2017.
[6] ITU: Tactile Internet, siehe http://www.itu.int/en/ITU-T/techwatch/Pages/tactile-internet.aspx, besucht Apr. 2017.
[7] Münchner Erklärung: Software Standort Deutschland, siehe http://muenchner-erklaerung.de/, besucht Apr. 2017.
[8] FZI et al: Smart Data Memorandum, siehe http://smart-data.fzi.de/memorandum/, besucht Apr. 2017.
[9] Wikipedia: Internet der Dinge, siehe https://de.wikipedia.org/wiki/Internet_der_Dinge, besucht Apr. 2017.
[10] Computerwoche: Internet der Dinge, siehe http://www.computerwoche.de/a/das-internet-of-things-waechst-rasant,3219970, besucht Apr. 2017.
[11] IEEE: Towards a definition of the Internet of Things (IoT), Revision 1, 27. Mai 2015, siehe http://iot.ieee.org/definition.html, besucht Apr. 2017.
[12] 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.
[13] EU FP7 Projekt Internet of Things Architecture, Updated reference model for IoT, siehe http://www.meet-iot.eu/deliverables-IOTA/D1_3.pdf, Juli 2012, besucht Juni 2017.
[14] Maciej Kranz: IoT Meets Standards, Driving Interoperability and Adoption, CISCO Blog, siehe http://blogs.cisco.com/digital/iot-meets-standards-driving-interoperability-and-adoption, Juli 2015, besucht Apr. 2017.
[15] Mike Loukides: What is DevOps?. O'Reilly Radar, 7. Juni 2012, siehe http://radar.oreilly.com/2012/06/what-is-devops.html, besucht Apr. 2017.
[16] TTCN-3 (Testing and Test Control Notation), siehe http://www.ttcn-3.org/, besucht Apr. 2017.
[17] Bosch IoT XdK, siehe https://xdk.bosch-connectivity.com/, besucht Apr. 2017.
[18] Relayr Plattform, siehe https://relayr.io/en/iot-middleware-platform/, besucht Apr. 2017.
[19] RIOT IoT Betriebssystem, siehe https://riot-os.org, besucht Apr. 2017.
[20] Eclipse OneM2M Implementierung, siehe https://eclipse.org/om2m/, besucht Apr. 2017.
[21] Eclipse IoT Framework, siehe http://iot.eclipse.org/, besucht Apr. 2017.
[22] KIWIW IoT Business Processes, siehe http://kiwiw.de/, Apr. 2017.
[23] Arbeitskreis Software-Qualität und Fortbildung (ASQF), siehe http://asqf.de/, besucht Apr. 2017.
[24] German Testing Board (GTB), siehe http://www.german-testing-board.info/, besucht Apr. 2017.
[25] Mike O. Villegas: 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, besucht Apr. 2017.
[26] Eclipse IoT-Projekte in Java, siehe http://iot.eclipse.org/java, besucht Apr. 2017.
[27] Wikipedia: Metcalfesches Gesetz, siehe https://de.wikipedia.org/wiki/Metcalfesches_Gesetz, besucht Juni 2017.
[28] Wikipedia: Reedsches Gesetz, siehe https://de.wikipedia.org/wiki/Reedsches_Gesetz, besucht Juni 2017.

[29]IETF RFC 7252, siehe https://tools.ietf.org/html/rfc7252, besucht Juni 2017.
[30]OASIS MQTT, siehe http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html.
[31]OMA LwM2M, siehe http://openmobilealliance.org/iot/lightweight-m2m-lwm2m.
[32]Wikipedia: Edge computing, siehe https://en.wikipedia.org/wiki/Edge_computing.
[33]Eclipse IoT-Testware, siehe https://projects.eclipse.org/projects/technology.iottestware, besucht Juni 2017.
[34]BMWi-Projekt IoT-T, siehe http://www.iot-t.de, besucht Juli 2017.