QUALITY ENGINEERING FÜR DAS INTERNET DER DINGE (CPIoT) LEHRPLAN ZUM BASISKURS

ASQF/GTB CERTIFIED PROFESSIONAL FOR IoT FOUNDATION LEVEL

Lehrplan Version 1.1
2019

CC BY ND 4.0
Copyright und Nutzungsrechte
Dieses Werk ist unter einer Creative Commons Lizenz vom Typ Namensnennung - Keine Bearbeitungen 4.0 International zugänglich. Um eine Kopie dieser Lizenz einzusehen, konsultieren Sie http://creativecommons.org/licenses/by-nd/4.0/ oder wenden Sie sich brieflich an Creative Commons, Postfach 1866, Mountain View, California, 94042, USA.

Autoren
Aida Boukhris (Friedrich-Alexander-Universität Erlangen-Nürnberg), Vera Gebhardt (tecmata GmbH), Alexander Gladisch (T-Systems MMS GmbH), Daniel Hummel (IT-P GmbH), Günter Jung (imbus AG), Ralf Mack (Atos Information Technology GmbH), Matthias Pruksch (sepp.med GmbH), Axel Rennoch (Fraunhofer-Institut für Offene Kommunikationssysteme), Alfred Richter (DB Systel GmbH), Nils Röttger (imbus AG), Ina Schieferdecker (Fraunhofer-Institut für Offene Kommunikationssysteme / TU Berlin), Jessica Schiffmann, Günter Schneider (Sulzer GmbH), Armin Metzger (GTB)

Reviewer
Jan Markus Giesen (Brunel Car Synergies GmbH), Thomas Haase (T-Systems MMS GmbH), Anne Kramer (sepp.med GmbH), Helmut Pichler (Nagarro GmbH), Frederik Teichert (HILSTER Testing Solutions GmbH)

Änderungsübersicht

| Version | Datum      | Autor                  | Bemerkung               |
|---------|------------|                       |                        |
| 1.0     | 21.12.2017 | Autoren und Reviewer  | Erste freigegebene Version |
| 1.1     | 14.11.2018 | Autoren und Reviewer  | Zweite freigegebene Version |
| 1.1     | 14.02.2019 | Reviewanpassungen     |                        |
Inhaltsverzeichnis

Copyright und Nutzungsrechte ......................................................................................................................... 2
Autoren ............................................................................................................................................................. 2
Reviewer .......................................................................................................................................................... 2
Änderungsübersicht ....................................................................................................................................... 2
Liste der Lernziele ............................................................................................................................................. 5
0 Einführung ....................................................................................................................................................... 7

1 Motivation [130] .............................................................................................................................................. 8
1.1 Quality Engineering für das Internet der Dinge: Was ist das? [30] ............................................................... 8
   1.1.1 Was ist das Internet der Dinge? (10 Min) ......................................................................................... 8
   1.1.2 Was bedeutet Quality Engineering für IoT? (20 Min) ..................................................................... 8
1.2 Besonderheiten des QE4IoT [90] ...................................................................................................... 9
   1.2.1 Was verändert das Internet der Dinge für das Quality Engineering? (30 Min) ....................... 9
   1.2.2 IoT Business ist Datenbusiness – Aspekte für das QE (60 Min) .................................................. 10
1.3 Beispiel „Smart Home“ [10] ................................................................................................................. 12

2 Qualitätsmerkmale und Standards [285] ..................................................................................................... 13
2.1 Einführung [30] .......................................................................................................................................... 14
2.1.1 Überblick über die IoT relevanten Qualitätsmerkmale (10 Min) ...................................................... 14
2.1.2 Der Betrieb eines IoT Systems: Herausforderung bereits bei der Systemkonzeption (15 Min) ...... 14
2.1.3 Standards (5 Min) ............................................................................................................................. 15
2.2 Qualitätsmerkmale mit besonderer Bedeutung für IoT [135] .................................................................. 15
2.2.1 Funktionalität (5 Min) ....................................................................................................................... 15
2.2.2 IoT Sicherheit (75 Min) .................................................................................................................... 16
2.2.3 Kompatibilität (10 Min) .................................................................................................................... 18
2.2.4 Robustheit und Resilienz (10 Min) ................................................................................................. 18
2.2.5 Wartbarkeit und Übertragbarkeit (15 Min) ..................................................................................... 18
2.2.6 Performanz (10 Min) ......................................................................................................................... 19
2.2.7 Ethische Aspekte bei IoT (10 Min) ................................................................................................... 20
2.3 Qualitätsmerkmale und ihre Spannungsfelder in IoT Systemen [60] ...................................................... 20
2.3.1 Das Spannungsfeld von IT-Sicherheit und funktionaler Sicherheit (15 Min) .............................. 20
2.3.2 Das Spannungsfeld von Gebrauchstauglichkeit, Wartbarkeit und IT-Sicherheit (15 Min) ...... 21
2.3.3 Das Spannungsfeld von Resilienz, Robustheit und Performanz (15 Min) ............................... 21
2.3.4 Das Spannungsfeld Konnektivität, Interoperabilität und IT-Sicherheit (15 Min) .................... 21
2.4 Zusammenhang zwischen Qualitätsmerkmalen und Anforderungen [60] ........................................ 21
2.5 Beispiel „E-Health“ [10] ......................................................................................................................... 22

3 Konstruktives QE – IoT Architektur [165] .................................................................................................. 24
3.1 Was eine Architektur für IoT geeignet macht [15] ................................................................................... 24
3.2 IoT Referenzarchitekturen [150] ............................................................................................................ 24
   3.2.1 Überblick über bestehende IoT Referenzarchitekturen (10 Min) ................................................. 24
   3.2.2 AIOTI HLA (60 Min) ....................................................................................................................... 25
   3.2.3 RAMI 4.0 (25 Min) ......................................................................................................................... 26
   3.2.4 OneM2M (25 Min) .......................................................................................................................... 27
   3.2.5 Abbildung von IoT Systemen auf Referenzmodelle (30 Min) .................................................... 28
4 Konstruktives QE – Prozesse und Methoden [85] ............................................................29
4.1 Prozesse und Best Practices für die IoT Entwicklung [10] ........................................29
4.2 Ansätze zur kontinuierlichen Entwicklung [35] .........................................................30
4.2.1 Vorteile agiler Methoden (10 Min) .................................................................30
4.2.2 Vorteile automatisierter Methoden (10 Min) .....................................................30
4.2.3 DevOps für IoT (15 Min) ..................................................................................31
4.3.1 Varianten in IoT Systemen (15 Min) .................................................................31
4.3.2 Betrieb von IoT Systemen (15 Min) .................................................................32
4.4 Beispiel “Ladevorgang eines Elektroautos” [10] .........................................................33
5 Analytisches QE (inkl. Test) [240] ...........................................................................34
5.1 Einleitung [10] ........................................................................................................34
5.2 Für IoT spezifische Testvorgehen und Teststufen [20] ............................................34
5.3 Testziele, Priorisierung und Risikoanalyse [75] ......................................................36
5.4 Testbarkeit und Testautomatisierung [15] ...............................................................37
5.4.1 Besonderheiten des IoT Testens (10 Min) .........................................................37
5.4.2 Testautomatisierung (5 Min) .............................................................................38
5.5 Testprozess und Testarchitektur [15] .......................................................................38
5.5.1 IoT Testarchitekturen (15 Min) ..........................................................................38
5.6 Testmethoden [95] ..................................................................................................39
5.6.1 Wichtige IoT Testmethoden (20 Min) ...............................................................39
5.6.2 Sicherheitstest (20 Min) ..................................................................................39
5.6.3 Interoperabilitätstest (15 Min) ............................................................................41
5.6.4 Performanz Test (20 Min) .................................................................................42
5.6.5 Produktzertifizierung (20 Min) ........................................................................43
5.7 Zusammenfassung [10 Min] ....................................................................................43
6 Lifecycle [45] ..............................................................................................................44
6.1 Im IoT-Kontext verknüpfte Lebenszyklen mit ihren Phasen und ihre Bedeutung aus QE-Sicht [15] ..................................................................................44
6.2 Die besondere Bedeutung der Interdisziplinarität für den IoT-Lebenszyklus verstehen [30] ...45
6.2.1 Die interdisziplinäre Natur des IoT-Lebenszyklus (15 Min) ..................................45
6.2.2 Drittbeiligte im IoT-Lebenszyklus und ihre Bedeutung (15 Min) ..........................45
Liste der Lernziele

IoT-QE LZ 1  (K1) Wissen, was Internet der Dinge bedeutet [10]
IoT-QE LZ 2  (K2) Konstruktives und analytisches Quality Engineering im Kontext IoT erklären [15]
IoT-QE LZ 3  (K1) Wissen, dass Quality Engineering eine hohe Relevanz für das Internet der Dinge hat [5]
IoT-QE LZ 4  (K2) Die Besonderheiten des IoT und die damit verbundenen spezifischen Herausforderungen für das Quality Engineering erklären können [30]
IoT-QE LZ 5  (K3) Auswirkungen der datengetriebenen IoT Geschäftsmodelle beurteilen können [60]
IoT-QE LZ 6  (K2) Relevanz und Schwerpunkte von Qualitätsmerkmalen für IoT im Überblick erklären können [10]
IoT-QE LZ 7  (K2) Die Relevanz der Qualitätsmerkmale auch für den Betrieb erklären können [15]
IoT-QE LZ 8  (K1) Die Bedeutung von Standards und regulatorische Anforderungen kennen [5]
IoT-QE LZ 9  (K1) Funktionale Qualitätsmerkmale kennen [5]
IoT-QE LZ 10 (K2) Die Sicherheitsherausforderungen (sowohl Security als auch Safety) bei IoT Systemen erklären können. [15]
IoT-QE LZ 11 (K3) Eine Analyse der Auswirkungen der Qualitätsmerkmale IT-Sicherheit und funktionale Sicherheit auf Konstruktives QE vornehmen können [60]
IoT-QE LZ 12 (K2) Die Anforderungen an Interoperabilität für IoT Systeme erklären können [10]
IoT-QE LZ 13 (K1) Die für IoT Systeme wesentlichen Qualitätsmerkmale Robustheit und Resilienz kennen [10]
IoT-QE LZ 14 (K2) Die Anforderungen an Wartbarkeit und Übertragbarkeit für IoT Systeme erklären können [15]
IoT-QE LZ 15 (K2) Die besonderen Herausforderungen an das Qualitätsmerkmal Performance (Zeitverhalten und Verbrauchsverhalten) für IoT Systeme erklären können [10]
IoT-QE LZ 16 (K2) Die Relevanz Ethischer Aspekte für IoT erklären können [10]
IoT-QE LZ 17 (K2) Das Spannungsfeld von IT-Sicherheit und funktionaler Sicherheit erklären können [15]
IoT-QE LZ 18 (K2) Das Spannungsfeld von Usability, Wartbarkeit und IT-Sicherheit erklären können [15]
IoT-QE LZ 19 (K2) Das Spannungsfeld von Resilienz, Robustheit und Performance erklären können [15]
IoT-QE LZ 20 (K2) Das Spannungsfeld von Konnektivität, Interoperabilität und IT-Sicherheit erklären können [15]
IoT-QE LZ 21 (K3) Die Qualitätsmerkmale eines Systems bewerten und daraus Anforderungen an das IoT System ableiten können [50]
IoT-QE LZ 22 (K1) Wissen was eine Architektur für IoT geeignet macht [15]
IoT-QE LZ 23 (K1) Ausgewählte IoT Referenzarchitekturen kennen [10]
IoT-QE LZ 25 (K2) Die Schichten von IoT Architekturen am Beispiel AIOTI erklären können [15]
IoT-QE LZ 26 (K2) Die Funktionen der Schichten in IoT Architekturen am Beispiel AIOTI erklären können [15]
IoT-QE LZ 27 (K2) Den spezifischen Einfluss der Daten auf IoT Architekturen erklären können [15]
IoT-QE LZ 28 (K1) RAMI als spezifische IoT Architektur kennen [10]
IoT-QE LZ 29 (K2) Die Schichten von IoT Architekturen am Beispiel RAMI 4.0 erklären können [15]
IoT-QE LZ 30 (K1) oneM2M als spezifische IoT Architektur kennen [10]
IoT-QE LZ 31 (K2) Die Schichten von IoT Architekturen am Beispiel OneM2M erklären können [15]
IoT-QE LZ 32 (K3) Eine IoT Referenzarchitektur auf eine spezifische IoT Systemarchitektur abbilden können [30]
<table>
<thead>
<tr>
<th>IoT-QE LZ 33</th>
<th>(K1) Best Practices in IoT kennen [10]</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT-QE LZ 34</td>
<td>(K1) Die Vorteile agiler Methoden kennen [10]</td>
</tr>
<tr>
<td>IoT-QE LZ 35</td>
<td>(K1) Die Vorteile automatisierter Methoden kennen [10]</td>
</tr>
<tr>
<td>IoT-QE LZ 36</td>
<td>(K2) DevOps für IoT erklären können [15]</td>
</tr>
<tr>
<td>IoT-QE LZ 37</td>
<td>(K2) Die Bedeutung von Produkt- und Systemvarianten für IoT erklären können [15]</td>
</tr>
<tr>
<td>IoT-QE LZ 38</td>
<td>(K2) Die Bedeutung des Quality Engineering für die Betriebsphase bei IoT Systemen erklären können [15]</td>
</tr>
<tr>
<td>IoT-QE LZ 39</td>
<td>(K1) Die Notwendigkeit von Monitoring im Betrieb von IoT Systemen kennen [verteilt auf Kapitel]</td>
</tr>
<tr>
<td>IoT-QE LZ 40</td>
<td>(K2) Die Herausforderungen verteilter Tests für IoT Systeme erklären können [verteilt auf Kapitel]</td>
</tr>
<tr>
<td>IoT-QE LZ 41</td>
<td>(K2) Die besonderen Herausforderungen beim Testen von IoT Lösungen wie ihre Offenheit, Verteiltheit, Dynamik, Skalierung und Varianz erläutern können [10]</td>
</tr>
<tr>
<td>IoT-QE LZ 42</td>
<td>(K2) Für IoT spezifische Testvorgehens und Teststufen erläutern können [20]</td>
</tr>
<tr>
<td>IoT-QE LZ 43</td>
<td>(K3) Testziele für IoT definieren und deren Priorisierung durchführen können [30]</td>
</tr>
<tr>
<td>IoT-QE LZ 44</td>
<td>(K3) Risikobasierte Priorisierung von Testzielen durchführen können [30]</td>
</tr>
<tr>
<td>IoT-QE LZ 45</td>
<td>(K2) Die Besonderheiten beim IoT Testen benennen und Beispiele für IoT Tests auf verschiedenen Ebenen erläutern können [10]</td>
</tr>
<tr>
<td>IoT-QE LZ 46</td>
<td>(K2) Die Notwendigkeit der Testautomatisierung für den IoT Test erläutern können [15]</td>
</tr>
<tr>
<td>IoT-QE LZ 47</td>
<td>(K2) IoT Testarchitekturen und typische IoT Testobjekte erläutern können [15]</td>
</tr>
<tr>
<td>IoT-QE LZ 48</td>
<td>(K2) Wesentliche Aspekte der IoT Testarchitektur erläutern können [15]</td>
</tr>
<tr>
<td>IoT-QE LZ 49</td>
<td>(K2) Nutzbarkeit und Grenzen klassischer Testmethoden für IoT Systeme erläutern können [20]</td>
</tr>
<tr>
<td>IoT-QE LZ 50</td>
<td>(K2) Die besonderen Anforderungen an das Testen von IoT Lösungen auf Sicherheit und die Anwendungen entsprechender Testmethoden auf unterschiedlichen Ebenen der IoT Architektur erläutern können [20]</td>
</tr>
<tr>
<td>IoT-QE LZ 51</td>
<td>(K2) Die besonderen Anforderungen an das Testen von IoT Lösungen auf Interoperabilität und die Anwendungen entsprechender Testmethoden auf unterschiedlichen Ebenen der IoT Architektur erläutern können [15]</td>
</tr>
<tr>
<td>IoT-QE LZ 52</td>
<td>(K2) Die besonderen Anforderungen an das Testen von IoT Lösungen auf Performanz und die Anwendungen entsprechender Testmethoden auf unterschiedlichen Ebenen der IoT Architektur erläutern können [20]</td>
</tr>
<tr>
<td>IoT-QE LZ 53</td>
<td>(K2) Die Herausforderungen bei der Prüfung auf Konformität und Zertifizierung erläutern können [20]</td>
</tr>
<tr>
<td>IoT-QE LZ 54</td>
<td>(K2) Die Bedeutung der im IoT Kontext verknüpften Lebenszyklen für das QE verstehen [15]</td>
</tr>
<tr>
<td>IoT-QE LZ 55</td>
<td>(K2) Die interdisziplinäre Natur des IoT-Lebenszyklus verstehen [15]</td>
</tr>
<tr>
<td>IoT-QE LZ 56</td>
<td>(K2) Bedeutung von Drittbeteiligten im IoT Kontext verstehen [15]</td>
</tr>
</tbody>
</table>
0 Einführung

Qualifizierungsschema


Business Outcomes

Der Geschäftsnutzen (Business Outcomes) durch die Teilnahme an einer Ausbildung basierend auf vorliegendem Lehrplan für den Teilnehmer und dessen Organisation stellt sich wie folgt dar:

- **IoT-QE_BO01_Sensibilisierung**: Sensibilisierung: Verständnis der besonderen Herausforderungen des Quality Engineering im Kontext von IoT.
- **IoT-QE_BO02_Standards**: Reibungslose Zusammenarbeit in und mit IoT Teams durch Kenntnis von Standards und dem gemeinsamen Glossar.
- **IoT-QE_BO03_Expertise**: Anwenden und Meistern des Quality Engineering im IoT Kontext durch Übertragen „klassischer“ QE Expertisen als auch Erlangen spezifischer Expertisen des IoT QE.
- **IoT-QE_BO05_Persönliche-Entwicklung**: Persönliche Weiterentwicklung des Trainingsteilnehmers durch Expertise in einem anspruchsvollen Zukunftsthema.

Lernziele und kognitive Stufen des Wissens


In Basislevel-Kursen finden üblicherweise folgende Stufen Anwendung:

- K1: kennen
- K2: verstehen
- K3: anwenden.

Der Level hat auch Einfluss auf die Lehrdauer und die Art der möglichen Prüfungsfragen.
1 Motivation [130]

Begriffe

| Internet of Things, Internet der Dinge (IoT) | Infrastruktur von miteinander verbundenen Entitäten, Personen, Systemen und Informationsquellen zusammen mit Diensten, welche Informationen der physischen Welt und virtuellen Welt verarbeitet und darauf reagiert. |
| Konstruktives Quality Engineering | Ganzheitliches Ergreifen vorbeugender Maßnahmen zur Vermeidung, etwas Falsches, etwas auf ungeeignete Weise oder etwas mit mangelnder Sorgfalt zu entwickeln |

1.1 Quality Engineering für das Internet der Dinge: Was ist das? [30]

- Was ist das Internet der Dinge? (10 Min)

IoT-QE LZ 1 (K1) Wissen, was Internet der Dinge bedeutet [10]

Unter IoT wird eine Infrastruktur verstanden, die aus von miteinander verbundenen Entitäten, Personen, Systemen und Informationsquellen zusammen mit Diensten, welche Informationen der physischen Welt und virtuellen Welt verarbeitet und darauf reagiert.

Es handelt sich dabei weder um eine neue noch um eine fest definierte Technologie bzw. exakte Systemdefinition. Internet der Dinge bedeutet, dass physische Objekte zunehmend durch ihre digitalen Repräsentationen („Digital Twin“) in digitalen Umgebungen repräsentiert und so orchestriert oder auch integriert werden können. Dies verändert sowohl die technologische Basis als auch die Anwendungsszenarien von softwarebasierten Lösungen.


- Was bedeutet Quality Engineering für IoT? (20 Min)

IoT-QE LZ 2 (K2) Konstruktives und analytisches Quality Engineering im Kontext IoT erklären können [15]

Wirksame Qualitätsplanung und -sicherung verhindert oder erkennt frühzeitig Fehler im Entwicklungsprozess, in der Produktion, vor/nach Betrieb und trägt somit maßgeblich zur Akzeptanz des Produkts und letztlich zum wirtschaftlichen Erfolg von IoT Produkten und Dienstleistungen bei.

Berücksichtigung von Testbarkeit während der Entwicklung und Fertigung, sowie die Planung des späteren Betriebs hinsichtlich der Aufrechterhaltung der geforderten Service Levels gehört ebenfalls zur konstruktiven Qualitätsarbeit.

Das konstruktive Quality Engineering für IoT Systeme baut auf dem grundlegenden Verständnis der Architektur und der erforderlichen Qualitätsmerkmale von IoT Systemen auf und unterstützt die analytische Qualitätssicherung durch eine optimale Planung von Qualitätsmaßnahmen.

Analytische Qualitätsarbeit dient der frühzeitigen Aufdeckung von Fehlern. Dabei kommen statische Verfahren (z.B. die Nutzung von Review-Techniken zur frühen Fehleraufdeckung oder Modellprüfungen) und die dynamische Qualitätssicherung durch Tests (funktionale Tests, Lasttests, Akzeptanztests, Gebrauchstauglichkeits- und Sicherheitstests, Penetrationstests, etc.) zum Einsatz.

Das analytische Quality Engineering für IoT Systeme erfordert intensive Planungsphasen und kreative Methodenauswahl zur Sicherstellung der frühstmöglichen Fehleraufdeckung. Die Planung muss stetig auf Eignung und Anpassungsbedarf geprüft werden und Anpassungen sind zwingend durchzuführen und zu überwachen.

IoT-QE LZ 3 (K1) Wissen, dass Quality Engineering eine hohe Relevanz für das Internet der Dinge hat [5]


1.2 Besonderheiten des QE4IoT [90]

- Was verändert das Internet der Dinge für das Quality Engineering? (30 Min)

IoT-QE LZ 4 (K2) Die Besonderheiten des IoT und die damit verbundenen spezifischen Herausforderungen für das Quality Engineering erklären können [30]

IoT-Systeme sind gekennzeichnet durch:

- die Kombination sehr heterogener Hard- und Software und die große Zahl von miteinander interagierenden Komponenten,
- lokale Vernetzung im Intranet und globale Vernetzung über das Internet,
- die Vielfalt von unterschiedlichen Technologien und Protokollen auf Anwendungsebene und bei Verbindungen,
- mobile Endgeräte und Sensorik/Aktuatorik mit unterschiedlichsten Hardware-Ressourcen und Generationen von Betriebssystemen,
- die Erfassung, Kommunikation und Verarbeitung von volatilen, heterogenen und großen Datenmengen,
- die Dynamik der Strukturen und Komponenten (als „lebendes“ und offenes System) und
die nötigen horizontalen und vertikalen Integrationen unter Nutzung von verschiedenen Plattformen für das Edge- und Cloud-Computing.
Hieraus entstehen besondere Herausforderungen für das Quality Engineering in Bezug auf:


- Komplexe Betriebsszenarien – Testsituationen können die spätere Betriebssituation oft nur annähernd abdecken.

- Fehlende Zugänglichkeit der Geräte – Endgeräte sind häufig nicht einer Analyse oder Fehlerbeseitigung zugänglich.


- Stark konkurrierende Qualitätsanforderungen – Qualitätsanforderungen stehen oftmals im Widerspruch zueinander, so dass beispielsweise eine hohe Sicherheit zu Lasten der Performanz oder des einfachen Zugangs geht.

- IoT Business ist Datenbusiness – Aspekte für das QE (60 Min)

IoT-QE LZ 5 (K3) Auswirkungen der datengetriebenen IoT Geschäftsmodelle beurteilen können [60]

IoT Systeme ermöglichen neuartige und durch das Internet weitreichendere datengetriebene Geschäftsmodelle. Die essentielle Wertschöpfung entsteht durch die Gewinnung von Handlungsoptionen auf Basis selbst erhobener Daten bzw. ergänzender Daten von Drittanbietern. Beispiele dafür sind:

- Information und Kontrolle in Echtzeit (Dashboard, Tracing),

- Auswertung der Historie mit Anwendung auf Vorhersagemodelle (Predictive Maintenance, Machine Learning) oder

- hocheffiziente Verwaltung von Ressourcen (On Demand, Shareconomy) auf Basis von Nutzungsdaten.

Durch die Nutzung des Internets als Kommunikationsplattform können physische Komponenten in ein Netzwerk von Sensoren, Aktoren und zentralen sowie verteilten Systemen eingebunden werden. So stehen Daten aus der realen Welt zur Nutzung in Geschäftsprozessen zunehmend zeitnaher, umfangreicher, vollständiger, umfassender, aber auch heterogener zur Verfügung.

Die verfügbaren Komponenten sowie die Art und Qualität der durch sie bereitgestellten Daten, wird eine hohe Dynamik aufweisen und nicht in jedem Fall vollständig planbar sein. Die Analyse dieser Daten kann zu Erkenntnissen führen, die vorher nicht absehbar waren. Aspekte der Datenaggregation, der Filterung und der Schutzziele personenbezogener, geschäfts- und sicherheitskritischer Daten müssen bei der Planung und dem Betrieb von IoT Anwendungen beachtet werden.


Übung zur Datenorientierung in IoT

1.3 Beispiel „Smart Home“ [10]


# 2 Qualitätsmerkmale und Standards

## Begriffe

<table>
<thead>
<tr>
<th>Qualitätsmerkmal</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funktionale Sicherheit (Safety)</td>
<td>Schutz Dritter durch den sicheren Betrieb der Systeme. [ISTQB 16]</td>
</tr>
<tr>
<td>IT-Sicherheit (Security)</td>
<td>Eigenschaften der Software, die sich auf die Fähigkeit beziehen, nicht autorisierte Zugriffe auf Programme oder Daten zu verhindern, unabhängig davon, ob diese versehentlich oder vorsätzlich erfolgen. [ISO 9126]</td>
</tr>
<tr>
<td>Performanz</td>
<td>Zeitverhalten und Verbrauchsverhalten (z.B. Energieeffizienz), Skalierbarkeit. [ISTQB 16]</td>
</tr>
<tr>
<td>Interoperabilität</td>
<td>Die Fähigkeit eines Softwareprodukts, mit einer oder mehreren spezifizierten Komponenten zusammenzuwirken [ISTQB 16]</td>
</tr>
<tr>
<td>Wartbarkeit</td>
<td>Diagnostizierbarkeit, Aktualisierbarkeit, Restartfähigkeit – auch aus der Ferne. [ISTQB 16]</td>
</tr>
<tr>
<td>Produkt-Zertifikat</td>
<td>Unabhängiger fachkundiger Nachweis der Erfüllung von Anforderungen durch ein Produkt.</td>
</tr>
</tbody>
</table>
2.1 Einführung [30]


Dieser Lehrplan beschreibt Merkmale, die in verschiedenen Normen, im ISTQB-Glossar oder ähnlichem definiert werden. Der Lehrplan wird einzelne Merkmale aus einer Norm nicht auf Merkmale einer anderen Norm mappen oder die Unterschiede zwischen den einzelnen Merkmalen oder deren Unterkategorien diskutieren.

Stattdessen werden die Merkmale in Bezug auf IoT Architekturen, auf Prozesse und auf das Quality Engineering für IoT in den folgenden Kapiteln ausgeführt.

- Überblick über die IoT relevanten Qualitätsmerkmale (10 Min)

Iot-QE LZ 6 (K2) Relevanz und Schwerpunkte von Qualitätsmerkmalen für IoT im Überblick erklären können [10]


- Der Betrieb eines IoT Systems: Herausforderung bereits bei der Systemkonzeption (15 Min)

Iot-QE LZ 7 (K2) Die Relevanz der Qualitätsmerkmale auch für den Betrieb erklären können [15]

Bereits beim Design von IoT Systemen muss auf die betrieblichen Belange des Systems geachtet werden. So müssen Funktionalitäten zum Monitoring der Betriebssituation, Monitoring der Leistungsfähigkeit, des Wiederanlaufs und der Wartung berücksichtigt werden (Build to Run).

Die Konzeption der Betriebsphase muss unter anderem die folgenden Servicequalitäten im Blick haben:

**Verfügbarkeit** – die Voraussetzungen zur Einhaltung der zugesagten Verfügbarkeit müssen geschaffen werden. Bei Änderungen soll die Funktion des Dienstes während der Änderung nicht oder nur im festgelegten Rahmen unterbrochen werden. Die Änderungen dürfen keine negativen Seitenwirkungen auf andere Funktionalitäten haben.
**Performanz:** Zeitverhalten und Verbrauchsverhalten (z.B. Energieeffizienz), Skalierbarkeit [ISTQB 16], Angemessenheit der verfügbaren Kapazität – je nach Betriebssituation können Kapazitätserweiterungen notwendig sein, die vor Auftreten von Engpässen bereitgestellt werden müssen (siehe auch Abschnitt -).

**Zuverlässigkeit (Robustheit, Resilienz):** Betrieb in harschen Umgebungen, Aufrechterhaltung von (Teil-) Funktionalität bei Störungen z.B. durch Wetter, Vandalismus, gezielten Stör- und Manipulationsversuchen, Fehlbedienung, fehlerhafte Eingaben, etc. (siehe auch Abschnitt -).

Aufzeichnung der wichtigsten Betriebsparameter und Nachweisführung der Einhaltung vereinbarter Qualitätsmerkmale: Die Aufzeichnung ausgewählter Kennzahlen zu Performance und Ressourcenverbrauch muss geplant werden.

---

- **Standards (5 Min)**

IoT-QE LZ 8  (K1) Die Bedeutung von Standards und regulatorische Anforderungen kennen [5]

Die Sicherstellung der Einhaltung von Standards ist eine der grundlegenden Aufgaben des Quality Engineering:

- Identifikation relevanter Normen, Standards und Zertifizierungen und ihrer Weiterentwicklungen.
- Umsetzung in konkrete Spezifikationen für das Produkt, das System oder die Dienstleistung.
- Überprüfung der jeweiligen Anforderungen.


---

2.2 **Qualitätsmerkmale mit besonderer Bedeutung für IoT [135]**


- **Funktionalität (5 Min)**

IoT-QE LZ 9  (K1) Funktionale Qualitätsmerkmale kennen [5]

Funktionale Qualitätsmerkmale nach ISO/IEC 25010 beziehen sich auf die Erfüllung der Geschäftsanforderungen an ein System, ein Produkt oder einen Dienst.

- **Korrekttheit (Functional Correctness)** – Genauigkeit mit der das Produkt oder System die gewünschten Ergebnisse erzielt.
- **Angemessenheit (Functional Appropriateness)** – Ist die Ausführung der Funktionalität angemessen realisiert – nicht zu kompliziert oder aufwändig.

Insbesondere die Funktionalität von intelligenten selbstlernenden Systemen erfordert besondere Testverfahren, da sich das Systemverhalten kontinuierlich mit dem Training des Systems ändert.
IoT Sicherheit (75 Min)

IoT-QE LZ 10 (K2) Die Sicherheitsherausforderungen (sowohl Security als auch Safety) bei IoT Systemen erklären können. [15]

IoT-QE LZ 11 (K3) Eine Analyse der Auswirkungen der Qualitätsmerkmale IT-Sicherheit und funktionale Sicherheit auf Konstruktives QE vornehmen können [60]


- **Funktionale Sicherheit / Safety**, ([ISTQB 16]) bezeichnet den Schutz Dritter durch den sicheren Betrieb der Systeme.

Durch die Anbindung an das Internet steigt die Gefährdung durch manipulative Angriffe und Eindringversuche wie auch von ungewollten physischen Einwirkungen (Zerstörung, Entwendung, Manipulation) deutlich an.

Die Entwicklung sicherer Hard- und Software entsprechend aktueller Marktstandards (z.B. ISO 27034 [ISO 27034]) wirkt auf die Sicherheit des Gerätes und der Schutz der verarbeiteten Informationen.

Die folgenden Qualitätsmerkmale nach ISO/IEC 25010 sind diesem Umfeld zuzuordnen:

- **Vertraulichkeit (Confidentiality)** – Schutz der Informationen vor dem Zugriff unberechtigter Systeme oder Personen beispielsweise durch verschlüsselte Speicherung und Kommunikation.

- **Integrität (Integrity)** – Schutz der Informationen vor unberechtigter Veränderung beispielsweise durch Verschlüsselung oder Prüfsummen.

- **Verfügbarkeit (Availability)** – siehe Kapitel -.

- **Nachweiserbarkeit (Non-repudiation)** – Fähigkeit nachzuweisen, dass Aktionen oder Ereignisse tatsächlich stattgefunden haben und Schutz der Nachweise vor Verfälschung.

- **Verantwortlichkeit (Accountability)** – Fähigkeit, Aktionen einer Entität zu genau dieser Entität zurückzuverfolgen.


Vertraulichkeit, Integrität und Verfügbarkeit gelten als primäre Schutzziele, die anderen Qualitätsmerkmale als ergänzende Schutzziele.

Hinzu kommen gesetzliche Vorgaben zum Datenschutz, die unbedingt zu beachten sind. Der Schutz der Privatsphäre stellt eine äußerst wichtige Qualitätsanforderung dar, die über europäisches Recht und das bundesdeutsche Datenschutzgesetz (BDSG)gesetzlich reguliert ist. Die Nutzung **personenbezogener Daten** muss vertraglich festgehalten und durch den Kunden freigegeben werden. Eine vertraglich unzulässige Verknüpfung von Daten mit personenbezogenen Daten muss unterbunden werden. Hierbei ist darauf zu achten, dass auch die Dinge personenbezogene Daten speichern können, die dann entsprechend zu schützen sind.

**Ethische Aspekte** müssen berücksichtigt wie der Schutz der persönlichen Autonomie, der Privatsphäre oder des Vertrauens werden.
Anforderungen zur Gewährleistung der funktionalen Sicherheit (Safety) von IoT Systemen oder Produkten sind in allgemeiner Form in der Norm IEC 61508 sowie in verschiedenen branchenspezifischen Normen (z.B. ISO 26262 Road vehicles Functional Safety, ISO 50128 Bahnanwendungen, ISO 13849 Sicherheit von Maschinen, etc.) aufgeführt.

Von wesentlicher Bedeutung für die IT-Sicherheit der Architekturen ist die Kenntnis und Risikobewertung der für IoT typischen Angriffsvektoren auf den unterschiedlichen Architektur-ebenen und -elementen als Basis für die Implementierung entsprechender Schutzmechanismen:

<table>
<thead>
<tr>
<th>Architektur-ebe/n - element</th>
<th>Angriffsvektoren</th>
</tr>
</thead>
</table>
| Things (physikalische Geräte) | - Physikalische Geräteschnittstellen  
- Gerätespeicher und Speichererweiterung (z.B. SD-Karten)  
- Firmware der Geräte  
- Physikalische Manipulation oder Diebstahl der Geräte |
| Netzwerk-Schicht (Konnektivität) | - Webinterfaces der Geräte  
- Netzwerkschnittstellen der Geräte |
| IoT-Schicht (Computation-, Aggregation- und Storage-Dienste) | - Cloud Web Interfaces  
- Backend APIs  
- Update Mechanism (over the air updates)  
- Sonstige Kommunikation zwischen IoT-Schicht und Netzwerk-Schicht |
| Applikations-Schicht (Analytics, Visualisierung und Steuerung) | - Mobile Applikationen  
- Webapplikationen |
| User | - Social Engineering |

Tabelle 1: Angriffsvektoren

Diese Angriffsvektoren sind im analytischen Quality Engineering entsprechend der Prioritäten aus der Risikoanalyse mit Testschwerpunkten zu versehen (Kap. -).

Übung zur IT-Sicherheit von IoT-Systemen

Die Kursteilnehmer bilden Gruppen zu je etwa 3-4 Mitgliedern und erarbeiten konkrete Qualitätsanforderungen (30 min). Der erreichte Stand wird im Plenum vorgestellt und diskutiert (15 min).
- Kompatibilität (10 Min)

IoT-QE LZ 12  (K2) Die Anforderungen an Interoperabilität für IoT Systeme erklären können [10]

**Kompatibilität** – die Möglichkeit, IoT-Systeme, -Produkte oder ihre Komponenten mit den Systemen, Produkten oder Komponenten anderer Hersteller zusammen oder aufeinander abgestimmt zu benutzen.

IoT Systeme, -Produkte oder -Komponenten müssen unter Umständen auf allen Ebenen der IoT Architektur mit Komponenten und Plattformen unterschiedlicher und wechselnder Hersteller koexistieren und ggfs. zusammenarbeiten. Zwei Unterkategorien der Kompatibilität spielen deshalb für IoT Systeme eine wesentliche Rolle:

- **Interoperabilität** – Sicherstellen der Kommunikation durch kompatible Datenformate und Protokolle und der Konnektivität zwischen Geräten unterschiedlicher Hersteller [ISTQB 16].
  
  Systeme/Komponenten können miteinander Informationen austauschen und nutzen. Dazu sind neben der Konnektivität der Komponenten kompatible Datenformate und Protokolle und eine einheitliche Interpretation der Daten erforderlich.

- **Koexistenz** – Systeme/Komponenten können gemeinsame Infrastrukturen nutzen, ohne sich gegenseitig in ihrer Funktionalität einzuschränken.

- Robustheit und Resilienz (10 Min)

IoT-QE LZ 13  (K1) Die für IoT Systeme wesentlichen Qualitätsmerkmale Robustheit und Resilienz kennen [10]


**Resilienz** ist die Fähigkeit zur Störungsbeseitigung sowie Benutzerunterstützung im Störungsfall – bei System- oder Dienstausfall oder Beeinträchtigungen muss ggf. geeignetes Personal oder Automatismen (Services) zur Verfügung stehen, um den Betrieb schnellstmöglich wiederherzustellen und/oder dem Nutzer Unterstützung zu gewähren.


Damit sind die Qualitätsmerkmale Robustheit und Resilienz für die Gesamtsysteme inklusive ihrer möglichen Anteile in der Cloud von großer Bedeutung.

- Wartbarkeit und Übertragbarkeit (15 Min)

IoT-QE LZ 14  (K2) Die Anforderungen an Wartbarkeit und Übertragbarkeit für IoT Systeme erklären können [15]

**Wartbarkeit** ist definiert als Diagnostizierbarkeit, Aktualisierbarkeit, Restartfähigkeit – auch aus der Ferne [ISTQB 16].

Auch im IoT stehen Hersteller von langlebigen IoT Geräten (z.B. Fahrzeuge, Produktionsmaschinen oder hochwertige Hausgeräte) vor der Herausforderung, dass er die Sicherheit, Interoperabilität und Wartung seiner IoT Geräte in Verbindung mit einer sich ändernden IoT Prozesskette über viele Jahre
hinweg unterstützen muss (z.B. Schließung von Sicherheitslücken, Unterstützung neuer Kommunikationsformate).

Typische Wartungsaufgaben sind dabei korrigierend, verbessernd, adaptiv und vorausschauend (predictive und preventive). Einerseits ermöglicht die Anbindung an das Internet erst eine automatisierte Wartung inklusive Vorhersagen und Prävention, andererseits sind viele IoT Geräte nicht dauerhaft mit dem Internet verbunden und nur eingeschränkt zugänglich.

Die ISO/IEC 25010 beleuchtet zum Thema Wartung vor allem die Aspekte der Software-Entwicklung:

- **Modularität** (Modularity) – Grad, zu dem ein System oder Computerprogramm aus einzelnen Komponenten besteht, sodass eine Änderung einer Komponente nur minimalen Einfluss auf andere Komponenten hat.

- **Wiederverwendbarkeit** (Reusability) – Grad an Aufwand und Wirksamkeit, zu dem ein Asset für mehr als ein System oder zur Entwicklung weiterer Assets genutzt werden kann.


- **Modifizierbarkeit** (Changeability) – Aufwand und Wirksamkeit, mit dem ein System verändert werden kann, ohne die Funktionalität zu beeinträchtigen oder Fehler zu injizieren.

- **Prüfbarkeit** (Testability) – Aufwand und die Wirksamkeit, mit dem Testkriterien fixiert werden können und der für die Durchführung von Tests erforderlich ist.

ISO/IEC 25010 gliedert das Qualitätsmerkmal **Übertragbarkeit** wie folgt auf:

- **Anpassbarkeit** – Grad, zu dem ein Produkt oder System effektiv und effizient auf andere oder entstehende Hardware-, Software- oder Nutzungsumgebungen angepasst werden kann (Individualisierbarkeit, falls die Anpassungen von einem Endnutzer vorgenommen werden).

- **Installierbarkeit** – Grad der Effektivität und Effizienz, mit der ein Produkt oder System in einer bestimmten Umgebung erfolgreich installiert und/oder deinstalliert werden kann.

- **Austauschbarkeit** – Grad, zu dem ein Produkt ein anderes bestimmtes Produkt mit demselben Zweck in derselben Umgebung ersetzen kann.

- **Performanz (10 Min)**

IoT-QE LZ 15 (K2) Die besonderen Herausforderungen an das Qualitätsmerkmal Performanz (Zeitverhalten und Verbrauchsverhalten) für IoT Systeme erklären können [10]

Gutes Laufzeitverhalten bei gleichzeitig niedrigem Ressourcenverbrauch stellt für viele IoT Produkte und -Komponenten eine große Herausforderung dar, da die Geräte oft sehr klein sind und günstig produziert werden müssen und keine externe Stromversorgung haben. Moderne Übertragungstechniken und -protokolle (z.B. LTE-M, LoRa, SigFox, etc.) sind auf kleine Datenraten und große Reichweiten bei kleinem Stromverbrauch optimiert, so dass Bandbreitengrenzen und ggfs. hohe Latenzzeiten im Design entscheidend berücksichtigt werden müssen.

Beim Qualitätsmerkmal Performanz unterscheidet ISO/IEC 25010 die folgenden für IoT Systeme, -Produkte und -Komponenten besonders relevanten Unterkategorien:

- **Laufzeitverhalten** (Time Behaviour) – Fähigkeit, Anforderungen hinsichtlich der Antwort- und Bearbeitungszeiten sowie die Durchsatzraten bei der Ausführung seiner Funktionen zu erfüllen.

- **Ressourcenverbrauch** (Resource utilization) – Art und Umfang der Verbräuche von Ressourcen (Strom, Speicherplatz, etc.), um die geforderten Funktionen zu erfüllen.

- **Kapazität** (Capacity) – Grad, zu dem die Höchstgrenzen eines Produkt- oder Systemparameters an die Anforderungen erfüllt sind.
- Ethische Aspekte bei IoT (10 Min)

IoT-QE LZ 16 (K2) Die Relevanz Ethischer Aspekte für IoT erklären können [10]


Dabei muss beachtet werden, dass ethische Entscheidungen aufgrund des unterschiedlichen moralischen und kulturellen Hintergrunds in den verschiedenen Regionen unterschiedlich ausfallen können. Wichtige Aspekte für die Bewertung von ethischen Fragestellungen sind u.a. Legalität, Gerechtigkeit, Respekt, Entscheidungsfreiheit, Umweltschutz und Nachhaltigkeit.

So können ethische Aspekte alle Qualitätsmerkmale eines IoT Systems beeinflussen.

Für IoT Projekte spielen ethische Aspekte eine zunehmend wichtige Rolle. Der Quality Engineer muss mögliche ethische Implikationen erkennen können, um diese bei der Konstruktion und Absicherung von IoT Systemen angemessen zu berücksichtigen. Dabei liegt die Verantwortung nicht beim Quality Engineer. Der Input zu ethischen Fragestellungen muss beim Qualitätsmanagement oder/und der Projektleitung eingefordert werden.

Beispiele:

1. Schutz der Privatsphäre: Welche gesellschaftlichen Normen (oder Gesetze) müssen beachtet werden, um das Selbstbestimmungsrecht des Menschen nicht zu verletzen (z.B. durch Möglichkeiten der Überwachung medizinischer Diagnosen)?
   Illegal wäre es, wenn medizinische Werte ohne das Wissen des Nutzers vom messenden Gerät nicht nur an die Applikation, sondern auch an die Krankenkasse des Nutzers übertragen werden.

2. Entscheidungsfreiheit: Welche Informationen dürfen einem Nutzer einer Software nicht vorenthalten werden, damit er immer noch frei entscheiden kann?
   Im Hinblick auf Sicherheit und Nachhaltigkeit ist es fragwürdig, wenn das Navigationssystem dem Nutzer nur schnelle Routen vorschlägt und keine Option auf langsameren oder risikoärmeren zulässt.

2.3 Qualitätsmerkmale und Ihre Spannungsfelder in IoT Systemen [60]

- Das Spannungsfeld von IT-Sicherheit und funktionaler Sicherheit (15 Min)

IoT-QE LZ 17 (K2) Das Spannungsfeld von IT-Sicherheit und funktionaler Sicherheit erklären können [15]

In IoT-Umfeld kommt es – stärker noch als im klassischen Umfeld – zu einem Spannungsfeld zwischen den Anforderungen an die IT-Sicherheit der Dinge und der vergleichsweise weit entwickelten IT-Sicherheit für klassische IT-Architekturen mit ihren oben erwähnten Schutzzielen. Klassisch erfordert funktionale Sicherheit stabile - meist zertifizierte - Softwareversionen, wohingegen IT-Sicherheit auch regelmäßige und kurzfristig notwendige Updates verlangt. Dabei gewinnen wegen der Datenbezogenheit bei IoT neben den primären auch die ergänzenden Schutzziele zunehmend an Bedeutung: Liegt der Fokus bei den – meist in Datenzentren – gut gesicherten IT-Systemen auf der Vertraulichkeit und Integrität, so liegt das Augenmerk bei den in aller Welt verstreuten Dingen auf Authentizität und Zurechenbarkeit. Dabei stellt die Verteilung funktionaler Sicherheit über IT und
Dinge hinweg automatisch Anforderungen an die Vernetzung und Interaktion bzgl. Verfügbarkeit, Vertraulichkeit und Verbindlichkeit.

- Das Spannungsfeld von Gebrauchstauglichkeit, Wartbarkeit und IT-Sicherheit (15 Min)

IoT-QE LZ 18  (K2) Das Spannungsfeld von Gebrauchstauglichkeit, Wartbarkeit und IT-Sicherheit erklären können [15]

Dinge und Services sollen möglichst einfach und sicher installiert, angepasst, in Stand gehalten und außer Betrieb genommen werden können (siehe auch Kapitel 6. Lifecycle):

- Einfach, d.h. möglichst automatisch und ohne aufwändige manuelle Eingriffe von Benutzern oder Servicebetreibern.
- Sicher, d.h. ohne Verletzung des Datenschutzes oder anderer zu schützender Werte.

Ein Benutzer möchte eine möglichst nahtlose Integration in seine installierte Umgebung mit seinen bereits genutzten Services und Dingen inklusive einer intuitiven Möglichkeit, diese auf seine individuellen Wünsche anzupassen. Demgegenüber muss ein Servicebetreiber einen vertragsgemäßen, sicheren Betrieb gewährleisten, der im Notfall auf manuelle Fernwartung zurückgreift und möglichst ohne den Einsatz eines Servicetechnikers vor Ort auskommt, was oftmals im Widerspruch zur einfachen Bedienbarkeit steht.

- Das Spannungsfeld von Resilienz, Robustheit und Performanz (15 Min)

IoT-QE LZ 19  (K2) Das Spannungsfeld von Resilienz, Robustheit und Performanz erklären können [15]

Die grundsätzliche Struktur von IoT Systemen als verteilte Systeme ist für die Resilienz von Vorteil, während sie aufgrund der Vielzahl an Schnittstellen eine Herausforderung für die Robustheit und Performanz darstellen kann. So kann z.B. die Störung / der Ausfall eines zentralen Gateways ein IoT System unverfügbar machen. Hier kann eine redundante Auslegung sowohl die Robustheit als auch Performanz verbessern, wobei mehr Systemressourcen benötigt werden.

- Das Spannungsfeld Konnektivität, Interoperabilität und IT-Sicherheit (15 Min)

IoT-QE LZ 20  (K2) Das Spannungsfeld von Konnektivität, Interoperabilität und IT-Sicherheit erklären können [15]


2.4 Zusammenhang zwischen Qualitätsmerkmalen und Anforderungen [60]

IoT-QE LZ 21  (K3) Die Qualitätsmerkmale eines Systems bewerten und daraus Anforderungen an das IoT System ableiten können [50]

Die Anforderungen an ein IoT. System sowie und deren Priorisierung ergeben sich direkt aus den relevanten Qualitätsmerkmalen.
Übung zur Herleitung von Anforderungen

Rollenspiel an Hand eines realistischen Beispiels/Szenarios eines IoT Produktes/Systems:

- Die Kursteilnehmer bilden Gruppen zu je etwa 3-4 Mitgliedern. Jede dieser Gruppen identifiziert und priorisiert die wichtigsten Qualitätsmerkmale.
- Aus diesen werden die zwei wichtigsten ausgewählt und für diese werden jeweils mehrere Anforderungen an das System aus Sicht des QE4IoT beschrieben. (25 min)
- Anschließend wird die Auswahl im Plenum vorgestellt und diskutiert. (25 min)

2.5 Beispiel „E-Health“ [10]

(Angelehnt an [oneM2M 16], chapter 7.3 Secure remote patient care and monitoring)


Anmerkung: In vielen Rechtssystemen – so auch in Deutschland – ist der Schutz von personenbezogenen Daten und insbesondere der von gesundheitsbezogenen Daten streng reguliert und Datenschutzverletzungen in diesem Umfeld werden stark bestraft.

E-Health-Systeme können private, zu schützende Daten auf ganz unterschiedlichen sensiblen Ebenen enthalten. Eine große Sorgfalt ist erforderlich, damit der Zugriff auf diese verschiedenen Daten nur für die jeweils autorisierte Nutzergruppe (Patient, Arzt, Pflegedienst, Familie) möglich ist.

Beteiligte Gruppen:

- Patienten, die Sensoren zur Messung ihrer medizinischen Werte benutzen.
- Betreiber von E-Health Anwendungen, die diese Sensoren bereitstellen und den Betrieb zur Überwachung der Messwerte durchführen und Dienste im Zusammenhang mit der Verarbeitung von Nachrichten an Pflegedienste, etc. erbringen.
- Medizinisches und pflegerisches Personal (Krankendienste, Pflegedienste, Ärzte, etc.) und andere administrative Dienstleister (Abrechnungsstellen, Versicherungen), die kontrollierten Zugriff auf ausgewählte Gesundheitsdaten erhalten müssen.
- Technische Dienstleister wie Netzprovider, Softwareanbieter, etc.

Auslöser für einen Datenzugriff:

- Neue Messdaten durch ein medizinisches IoT Gerät liegen vor.
- Eine Auswertung von empfangenen medizinischen Daten liegt vor und eine Reaktion (Alarm, Benachrichtigung, etc.) muss erfolgen.
- Eine Anfrage nach sensiblen medizinischen Daten zu einem Vorgang liegt von einem Berechtigten vor.
- Ein neuer Beteiligter (z.B. ein neuer Arzt) ist für ein medizinisches Szenario zuzulassen.
3 Konstruktives QE – IoT Architektur [165]

Begriffe

<table>
<thead>
<tr>
<th>Edge Computing</th>
<th>Dezentrale Datenverarbeitung mittels Teilauswertung von Sensorik Daten am Rand des Netzwerks, der sogenannten Edge, als Vorbereitung für den Upload in die Cloud.</th>
</tr>
</thead>
</table>

3.1 Was eine Architektur für IoT geeignet macht [15]

IoT-QE LZ 22 (K1) Wissen was eine Architektur für IoT geeignet macht [15]

Im Kontext IoT spielen Referenzarchitekturen eine herausragende Rolle, da typischerweise sehr komplexe Gesamtsysteme mit vielen Teilkomponenten betrachtet werden. Referenzarchitekturen müssen grundlegende Definitionen liefern und Gemeinsamkeiten für alle Systeme, die auf ihr beruhen, spezifizieren. Zudem müssen die besonderen Anforderungen im IoT Kontext berücksichtigt werden um zur Umsetzung von spezifischen IoT Projekten geeignet zu sein [Weyrich 16], [Heidrich 16]:

- Konnektivität: die Kommunikation zwischen verschiedenen Partnern (Geräten, Anwendungen, Diensten) muss durch die Referenzarchitektur sichergestellt werden.
- Interoperabilität: es kommen unterschiedliche Technologien zum Einsatz, gleichzeitig muss die Interoperabilität zwischen den einzelnen Komponenten des Gesamtsystems durch die Referenzarchitektur sichergestellt werden.
- Skalierbarkeit: Referenzarchitekturen müssen die Möglichkeit bieten, kleine IoT Lösungen als auch große IoT Lösungen, die ggf. eine Vielzahl von Geräten, Anwendungen und Diensten umfassen, abzubilden
- Datenerhebung und Datenanalyse: die Erhebung, Analyse und Weitergabe von Daten ist eine der grundlegenden Funktionen in IoT, die durch eine Referenzarchitektur ermöglicht werden müssen. IoT-Business ist Datenbusiness.
- IT-Sicherheit und Datenschutz: in allen Bereichen des IoT benötigt, muss durch eine Referenzarchitektur berücksichtigt werden. Hier gilt die Prämisse: - Security-by-Design
- Im Kontext industrielles IoT (IIoT) ggf. Echtzeitfähigkeit: d.h. verschiedene Klassen zeitlicher Anforderungen müssen durch die Referenzarchitektur abgebildet werden können

3.2 IoT Referenzarchitekturen [150]

Adäquate und auf die Domäne optimierte Architekturen sind die technische Basis für die Qualität eines Systems. Die Kenntnis der Spezifika von und Anforderungen an Architekturen im IoT Kontext sind daher ein wichtiger Bestandteil des Quality Engineering für IoT.

- Überblick über bestehende IoT Referenzarchitekturen (10 Min)

IoT-QE LZ 23 (K1) Ausgewählte IoT Referenzarchitekturen kennen [10]

beschreibt eine Referenzarchitektur die Interaktionen (Datenkommunikation, Synchronisation von Aktionen) unabhängig von der zugrundeliegenden Plattform. Sie bietet als generisches Modell Regeln und Leitlinien bei der Entwicklung einer spezifischen Architektur eines Systems und dient [ISO/IEC CD 30141]:

- der Beschreibung der Eigenschaften eines IoT Systems,
- der Definition der Domänen des IoT Systems,
- der Beschreibung des IoT Systems und seiner Elemente,
- der Beschreibung der Interoperabilität der Entitäten eines IoT Systems.

Eine übergreifende und umfassende Standardisierung von Referenzarchitekturen für IoT existiert derzeit nicht. Eine Vielzahl domänenunabhängiger und domänen spezifischer Referenzarchitekturen befindet sich derzeit in Entwicklung.

Die Referenzarchitektur AIOTI HLA (High Level Architecture) der "Alliance for Internet of Things Innovation" (AIOTI) [AIOTI 16] ist eine der - Stand 2017 - prominenten domänenunabhängigen IoT Referenzarchitekturen und dient in vorliegendem Lehrplan als Leitlinie für das IoT Architekturthema. Das Referenzmodell der Industrie 4.0 ist RAMI 4.0, eine in Deutschland prominente Initiative.

Das Referenzmodell OneM2M ist ein drittes prominentes Modell, welches darauf abzielt, eine Spezifikation für einheitliche M2M-ServiceSchicht zu etablieren umso den Austausch und das Teilen von Daten unter allen möglichen IoT-Interaktions zu ermöglichen.


- AIOTI HLA (60 Min)


Ein wesentlicher Aspekt ist der statische Blickwinkel auf die Elemente einer IoT Architektur. Das Domain Model der AIOTI Referenzarchitektur definiert die Elemente einer IoT Architektur wie folgt:

- User: Benutzer, menschlich oder anderweitig.
- Thing: physisches Objekt.
- IoT Service.
- Virtual Entity: virtuelle Instanz des physischen Objekts.
- IoT Device: Schnittstelle zu den physischen Möglichkeiten des physischen Objekts.

Ein User interagiert mit einem physischen Objekt (Thing), wobei ein IoT Service als Vermittler dieser Interaktion dient. Dieser IoT Service ist verbunden mit einer Virtual Entity (Virtuelle Instanz), die das physische Objekt virtuell abbildet und dessen Charakteristika in der virtuellen Welt repräsentiert. Die Interaktion des IoT Service mit dem physischen Objekt wird durch ein IoT Gerät (Device) ermöglicht, das auch die physischen Fähigkeiten des Dings erschließt.

IoT-QE LZ 25  (K2) Die Schichten von IoT Architekturen am Beispiel AIOTI erklären können [15]

Ein weiterer wesentlicher Aspekt ist der dynamische Blickwinkel, bei AIOTI abgebildet durch das AIOTI-Funktionsmodell. Es beschreibt Funktionen und Schnittstellen zwischen den Elementen eines IoT Systems und besteht aus drei Schichten:

- Die Applikationsschicht (Application Layer) beinhaltet Kommunikations- und Schnittstellenmethoden für die Kommunikation zwischen Prozessen.
- Die IoT Schicht (IoT Layer) enthält die spezifische IoT Funktionalität (z.B. Datenmanagement) und stellt diese über Application Programming Interfaces der Applikationsschicht zur Verfügung. Die IoT Schicht verwendet die Dienste der Netzwerkschicht.
Die Netzwerkschicht (Network layer) gruppiert Dienste auf Daten- und Kontrollebene. Die Netzwerkschicht stellt Transportmechanismen für Nutzerdaten (Kommunikation nah und fern sowie zwischen Entitäten der IoT-Schicht) und Steuerungsdienste zur Verfügung.

IoT-QE LZ 26  (K2) Die Funktionen der Schichten in IoT Architekturen am Beispiel AIOTI erklären können [15]

Die Funktionen innerhalb der Schichten werden durch Entitäten beschrieben:

- Die App-Entität realisiert die die IoT Applikationslogik dezentral in Geräten, Gateways oder Servern. Beispiele: Trackingsysteme für Fahrzeugflotten, Remote Blutzuckerüberwachung, etc.


- Die Netzwerke der Netzwerk-Schicht integrieren typischerweise heterogene Netzwerk-Technologien (PAN, LAN, WAN, etc.) und Netzwerk-Domänen, welche über das Internetprotokoll verbunden sind.

Je nach eingesetzten Kommunikationstechnologien kann die Netzwerkschicht unterschiedliche Dienstgüten (Quality of Service, QoS) anbieten. Letztlich werden die Anforderungen hieran von der Applikationsschicht bestimmt.

IoT-QE LZ 27  (K2) Den spezifischen Einfluss der Daten auf IoT Architekturen erklären können [15]

Das unter Umständen hohe Datenvolumen sowie die teilweise begrenzten Bandbreiten und Speichervolumen der Entitäten in der IoT Schicht, sowie deren nicht immer kontinuierlich gewährleistete Online-Verfügbarkeit machen Edge Computing zu einem wichtigen architekturen Ansatz. Edge Computing bezeichnet die dezentrale Datenverarbeitung am Rand des Netzwerks, der sogenannten Edge. Daten aus einem IoT System werden auf der Edge (z.B. im Gateway) aufbereitet, aggregiert und gespeichert und über die Netzwerk-Schicht den Applikationen direkt oder wiederum über eine Cloud zur Verfügung gestellt.


- RAMI 4.0 (25 Min)

IoT-QE LZ 28  (K1) RAMI als spezifische IoT Architektur kennen [10]

Das „Referenzarchitekturmmodell Industrie 4.0“, kurz RAMI 4.0, wurde im Jahr 2016 als DIN SPEC 91345:2016-04 veröffentlicht. Das Referenzarchitekturmmodell zielt darauf ab, mit den beteiligten Branchen (z.B. IKT, Automatisierung und Maschinenbau) ein einheitliches Verständnis für das Thema Industrie 4.0 herzustellen.

IoT-QE LZ 29  (K2) Die Schichten von IoT Architekturen am Beispiel RAMI 4.0 erklären können [15]

RAMI 4.0 beschreibt die wesentlichen Elemente eines Assets (aus der physischen Welt oder der Informationswelt) mittels eines dreidimensionalen Schichtenmodells. Auf diese Weise sollen komplexe Zusammenhänge aufgegliedert werden. Durch Kombination der drei Achsen des Schichtenmodells wird der jeweils relevante Aspekt zu jedem Zeitpunkt im Lebenslauf eines Assets dargestellbar. Die drei Achsen sind: [DIN SPEC 91345]:

- Architektur (Layers) beschreibt die Architektur mit ihren Funktionen und funktionspezifischen Daten in Form von 6 Schichten: Asset, Integration, Communication, Information, Functional, Business;

- Produktlebenszyklus (Life Cycle & Value Stream) stellt den Lebenslauf eines Assets dar (Entstehung bis Entsorgung) sowie den Wertschöpfungsprozess in Anlehnung an IEC 62890;
Hierarchie-Achse (Hierarchy) orientiert sich am Referenzarchitekturmodell für eine Fabrik in Anlehnung an die Normen DIN EN 62264-1 und DIN EN 61512-1, erweitert um Industrie 4.0 Aspekte.

Zu beachten ist, dass die Beschreibung im RAMI4.0 eine rein logische Beschreibung ist und sich eine reale Umsetzung davon unterscheiden kann. Security ist für RAMI4.0 ein elementarer Bestandteil und muss bei der Beschreibung jedes Abschnitts der drei Achsen immer mit betrachtet und beschrieben werden [DIN SPEC 91345].

- OneM2M (25 Min)

IoT-QE LZ 30 (K1) oneM2M als spezifische IoT Architektur kennen [10]


IoT-QE LZ 31 (K2) Die Schichten von IoT Architekturen am Beispiel OneM2M erklären können[15]

OneM2M nutzt ein 3 Schichten Modell, welches Applikationsschicht (Application Layer), eine Middleware-Schicht (Common Services Layer) und eine Netzwerkschicht umfasst. Die Funktionale Architektur von OneM2M definiert verschiedene Entitäten, basiert auf dem 3 Schichten Modell und umfasst die folgenden Funktionen [oneM2M 18]:

- **Application Entity (AE):** Entitäten in der Applikationsschicht, welche eine Applikationslogik implementieren.
- **Common Service Entity (CSE) repräsentiert die Instanzierung einer Sammlung von „Common Service Functions“, welche die üblichen IoT-Funktionen für die Applikationen bereitstellen (z.B. Daten- und Gerätemanagement, Lokalisierungsservices)
- **Network Service Entity (NSE) stellen die Services des darunterliegenden Netzwerkes für die CSEs bereit (z.B. Gerätemanagement, Lokalisierungsservices, oder Gerätetriggering).**

Hinweis: die darunterliegenden Netzerke stellen den reinen Datentransport-Service für die Entitäten in oneM2M bereit – diese Services sind nicht Bestandteil eines NSE.

- Abbildung von IoT Systemen auf Referenzmodelle (30 Min)

IoT-QE LZ 32 (K3) Eine IoT Referenzarchitektur auf eine spezifische IoT Systemarchitektur abbilden können [30]

Im Sinne des konstruktiven Quality Engineering sollte sich die spezifische Architektur eines IoT-Systems an einer geeigneten Referenzarchitektur orientieren.

Übung zu IoT-Referenzarchitekturen

Die Kursteilnehmer bilden Gruppen zu je etwa 3-4 Mitgliedern und lösen folgende Aufgabenstellungen:

- Die vorgestellten Referenzmodelle besitzen Gemeinsamkeiten. Welche sind dies? Können AIOTI HLA und oneM2M aufeinander abgebildet werden? Wenn ja, wie?
- Das Smart-Home Beispiel (siehe auch Kap. 1.3) soll mit Hilfe unterschiedlicher IoT Referenzarchitekturen dargestellt werden, AIOTI HLA und oneM2M.

Anschließend werden die Ergebnisse von den Gruppen vorgestellt und im Plenum diskutiert.
4 Konstruktives QE – Prozesse und Methoden

Begriffe

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Agile Softwareentwicklung</td>
<td>Agile Softwareentwicklung zielt darauf ab, den Entwicklungsprozess schlanker und flexibler zu halten. Selbstorganisierte Teams, enge Abstimmung mit dem Kunden sowie die Lieferung von Funktionalitäten in kurzen Abständen sind charakteristisch.</td>
</tr>
<tr>
<td>Update-Fähigkeit</td>
<td>Möglichkeit zur Erweiterung und/oder Verbesserung einer Version eines Softwareproduktes.</td>
</tr>
</tbody>
</table>

4.1 Prozesse und Best Practices für die IoT Entwicklung [10]

IoT-QE LZ 33 (K1) Best Practices in IoT kennen [10]

Das Ziel einer lernenden, sich selbst kontinuierlich verbessernden Organisation ist integraler Bestandteil von IoT Geschäftsmodellen. Datengetrieben werden Handlungsoptionen abgeleitet, die auch zu Änderungen in Geschäftsabläufen und Organisation führen können. Die Festlegung und Einhaltung von Prozessen nützt der Organisation durch:

- Schaffung von Transparenz (Fehlervermeidung durch Verstehen),
- Schaffung von Verantwortlichkeiten (Identifikation der Beteiligten mit ihrer Tätigkeit),
- bereichsübergreifende Kommunikation und Koordination,
- prozessorientiertes Denken und Handeln und
- Bildung einer Basis zur weiteren Optimierung und Automatisierung.

Best Practices bieten einen ähnlichen, wenn auch nicht vergleichbaren Nutzen, da sie unverbindlich und meist nur in Teilbereichen der Organisation angewendet werden. Im Unterschied zum Prozess und als Ergänzung dazu ist ein Best Practice:

- eine unverbindliche Empfehlung, wie in einem bestimmten Fall vorzugehen ist,
- flexibler als ein Standard und
- bei geänderten Anforderungen oder Bedingungen einfacher durch eine erfolgsversprechende Vorgehensweise ersetzbar.


- Das Team trägt gemeinsam die Gesamt-Verantwortung für die jeweilige Entwicklung und verfügt über entsprechende Handlungsmöglichkeiten (Kompetenzen).
- Key Performance Indicator werden im Team und über Teamgrenzen hinweg ausgehandelt.
Alle Umsetzungsschritte (Prototyp, Implementierung, Automatisierung etc.) orientieren sich am Nutzen (bzgl. Wertschöpfung).

4.2 Ansätze zur kontinuierlichen Entwicklung [35]

- Vorteile agiler Methoden (10 Min)

IoT-QE LZ 34 (K1) Die Vorteile agiler Methoden kennen [10]

Sequentielle Entwicklungsmodelle wie das V-Modell, die vorgelagerte Spezifikationen und nachgelagerte Verifikation & Validierung mit dem Kunden nutzen, geraten auch und insbesondere bei IoT-Systemen unter Druck durch:

- hohe Aufwände für die Spezifikationserstellung bei IoT-Produkten, die häufig sehr komplex sein können,
- zusätzliche technische Anforderungen, die noch während der Entwicklung entstehen,
- neue Anforderungen, die auf einer schnellen Anpassung an Kundenbedürfnisse beruhen.

Hier wirken agile Entwicklungsansätze durch ihre Prinzipien auf Effizienzsteigerungen hin. Sie basieren auf kontinuierlichen Verbesserungsprozessen, die in Iterationen beispielsweise nach dem Schema Plan-Do-Check-Act durchgeführt werden können:

- Plan – definiere Objekte und Prozesse zur Zielerreichung
- Do – setze den Plan um und sammle dabei Daten zur Beurteilung
- Check – überprüfe auf Abweichungen zu Plan und Zielerreichung, sowie Optimierungspotential
- Act (Adjust) – übernehme erfolgreiches und verbessere

- Vorteile automatisierter Methoden (10 Min)

IoT-QE LZ 35 (K1) Die Vorteile automatisierter Methoden kennen [10]


Zudem ist der Faktor Zeit für IoT Systeme oftmals besonders relevant, beispielsweise für das zeitnahe Ausrollen von Security Updates. Oft wird auch eine schnelle Reaktion auf Marktentwicklungen gefordert.


Zudem können verschiedene Infrastrukturen beispielsweise für die Entwicklung, den Vertrieb, den Betrieb, das Monitoring, die Wartung oder das Produkt- und Kundenmanagement genutzt werden.
Auch diese sollten möglichst weitgehend automatisiert nutzbar sein. Dabei sollten diese Automatisierungsansätze gleichermaßen dem konstruktiven und analytischen Quality Engineering unterliegen.

DevOps für IoT (15 Min)

IoT-QE LZ 36 (K2) DevOps für IoT erklären können [15]


In der Praxis bedeutet dies beispielsweise:

- für die Entwickler eine vermehrte Beschäftigung mit der Installation von virtuellen Maschinen und Aspekten der IT-Sicherheit oder mit der Planung und Durchführung von Auslieferungen.
- für die Administratoren die Beschäftigung mit Automatisierung in Kombination mit „Infrastructure as Code“, d.h. einer bestimmte IT-Infrastruktur, die Operations-Teams anstatt manueller Verfahren automatisch per Code verwalten und bereitstellen können, sowie der Umgang mit Versionsverwaltung und automatisierten Tests.
- für Entwickler und IT-Betrieb sich auf neue, bereichsübergreifende Key Performance Indicators (KPIs) und damit gemeinsame Anreiz-Metriken zu einigen und einzustellen.

Die an DevOps beteiligten Gruppen verfolgen auftragsgemäß Ziele, die teilweise in Konflikt zueinanderstehen:

- Entwickler möchten schnell Änderungen umsetzen,
- Tester möchten das Risiko von Abweichungen verringern und
- Administratoren möchten einen stabilen Betrieb gewährleisten.

Durch Etablierung einer zur Konsensbildung geeigneten DevOps-Kultur wird die Organisation in die Lage versetzt, schnell und effizient auf die Änderung von Rahmenbedingungen oder Geschäftszielen zu reagieren. Im Kontext von IoT bedeutet dies, das Silodenken aufzubrechen.

4.3 Weitergehende QE-Aktivitäten nach dem Rollout [30]

- Varianten in IoT Systemen (15 Min)

IoT-QE LZ 37 (K2) Die Bedeutung von Produkt- und Systemvarianten für IoT erklären können [15]


Ein IoT System besteht aus einer Vielzahl von Komponenten (Hardware und Software), die unterschiedlichen Lebenszyklen und Entwicklungsgeschwindigkeiten unterliegen (siehe auch Kapitel 6). Die IoT Komplexität wird durch den Einsatz von Varianten und Versionen zusätzlich vervielfacht. Aufgrund der kontinuierlichen Entwicklung von IoT Systemen kommt es u.a. zur:
- Betrieb von IoT Systemen (15 Min)

IoT-QE LZ 38  (K2) Die Bedeutung des Quality Engineering für die Betriebsphase bei IoT Systemen erklären können [15]


- die Pilotierung auf einem Teilsystem oder
- die betriebsspezifischen Regressionstests.

4.4 Beispiel “Ladevorgang eines Elektroautos” [10]

Abbildung 4: Ladevorgang eines Elektroautos (Icons made by Freepik, samshizone & Retinaicons from www.flaticon.com)

(Use Case „Plug-In Electrical Charging Vehicles and power feed in home scenario“ aus oneM2M Use Case Sammlung [oneM2M 16])

In diesem Anwendungsfall (siehe auch Abbildung) interagieren diverse Geräte und Systeme aus unterschiedlichen Industriedomänen miteinander und ihre Lebenszyklen sind typischerweise nicht synchronisiert.

Die Einhaltung der Qualitätsmerkmale im Echtbetrieb eines beteiligten Geräts oder Systems kann unmittelbar durch auftretende Qualitätsmängel eines anderen Systems beeinträchtigt werden. Diese Qualitätsmängel können beim Ersteinsatz aber auch erst nach längerer Nutzungszeit auftreten.

5 Analytisches QE (inkl. Test)[240]

Begriffe

| Fuzz Testing | Testtechnik, die mit Hilfe automatisch generierter und an ein Zielsystem versendeter anomaler ungültiger Nachrichtenfolgen, gebrochener Datenstrukturen oder ungültiger Daten Eingaben finden kann, die Störungen oder eine Verschlechterung von Dienstleistungen verursacht. ETSI TR 101 583 „Ein Testverfahren zur Entdeckung von Sicherheitsschwachstellen durch die massenhafte Eingabe von zufälligen Daten (Fuzz genannt) in die Komponente oder das System.“ [ISTQB 16] |
| Konformität | Die Fähigkeit eines Softwareprodukts, anwendungsspezifische Normen oder Vereinbarungen oder gesetzliche Bestimmungen und ähnliche Vorschriften zu erfüllen. [ISO 9126] |
| Things under Test | Erweiterung des Begriffs System under Test [ISTQB 17] auf ein SUT, welches cyphysische Komponenten integriert. |
| Datenqualität | Bewertung von Datenbeständen hinsichtlich ihrer Korrektheit, Relevanz und Verlässlichkeit, sowie ihrer Konsistenz und Verfügbarkeit auf verschiedenen Systemen. |

IoT-QE LZ 39  (K1) Die Notwendigkeit von Monitoring im Betrieb von IoT Systemen kennen [verteilt auf Kapitel]  
IoT-QE LZ 40  (K2) Die Herausforderungen verteilter Tests für IoT Systeme erklären können [verteilt auf Kapitel]

5.1 Einleitung [10]

IoT-QE LZ 41  (K2) Die besonderen Herausforderungen beim Testen von IoT Lösungen wie ihre Offenheit, Verteiltheit, Dynamik, Skalierung und Varianz erläutern können [10]  
IoT Lösungen zeichnen sich allgemein durch Offenheit, Verteiltheit, Dynamik, Skalierung und eine lange Betriebslaufzeit aus. Aus diesen Gründen werden daher neue Ansätze der analytischen Qualitätssicherung erforderlich.


Eine besondere Schwierigkeit ergibt sich aus der Fragestellung der Haftung bei Schadensfolgen nach Zweckentfremdung oder Sicherheitsvorfällen, insbesondere, wenn im Rahmen einer Zertifizierung zu einem bestimmten Zeitpunkt auf eine Selbsterklärung des Herstellers oder Betreibers zurückgegriffen wird.

5.2 Für IoT spezifische Testvorgehen und Teststufen [20]

IoT-QE LZ 42  (K2) Für IoT spezifische Testvorgehen und Teststufen erläutern können [20]  
Gerade für IoT Produkte ist effiziente und effektive Testbarkeit eine wichtige Voraussetzung für die Qualität des Produkts. Daher ist die Testanalyse und Testplanung in jeder Phase des Lebenszyklus (also auch die Wartungsphasen) durchzuführen. In den Wartungsphasen sind neben dem traditionellen Monitoring auch Predictive Maintenance Aspekte abzusichern. Eine frühzeitige Definition des

<table>
<thead>
<tr>
<th>Teststufe</th>
<th>Beispiel</th>
<th>Anmerkung</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Konformität zu unterstützten Protokollen</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Konformität zu standardisierten Abläufen</td>
<td></td>
</tr>
<tr>
<td>Integrationstest zur Einbettung des Testobjekts in seine (Test-) Umgebung</td>
<td>Kompatibilität</td>
<td>Kann stark von den spezifischen Einsatzzsenarien des Testobjekts abhängen.</td>
</tr>
<tr>
<td></td>
<td>Interoperabilität</td>
<td>Systemumgebung kann hohe evtl. auch nicht vollständig vorhersehbares Verhalten aufweisen (z.B. zukünftige neue Services). Umgebung kann durch Simulation erzeugt werden.</td>
</tr>
</tbody>
</table>

Tabelle 2: Teststufen

Der fundamentale Testprozess [ISTQB 17] wird im Kontext von IoT um die Phasen für die Laufzeit durch Monitoring & Watch Dogs erweitert, d.h. das System wächst zunehmend mit dem Testsystem zusammen:

- Planung und Steuerung: als Teil des Life Cycle Management
- Analyse und Entwurf: Risikoanalyse ergänzen
- Realisierung und Durchführung: Automatisierung und Laufzeit
- Bewertung und Bericht: fortlaufend
- Abschluss: erst mit Terminierung einer IoT Lösung
5.3 Testziele, Priorisierung und Risikoanalyse [75]

IoT-QE LZ 43 (K3) Testziele für IoT definieren und deren Priorisierung durchführen können [30]


Die Priorität von Testzielen orientiert sich an der Priorität der damit zu überprüfenden Qualitätsmerkmale. Testziele und deren Priorisierung sind kontinuierlich über den gesamten Lebenszyklus eines IoT Systems zu bewerten und gegebenenfalls anzupassen bzw. zu ergänzen.

Neben den Funktionalen Qualitätsmerkmalen gewinnen folgende Qualitätsmerkmale für IoT Systeme eine erhöhte Bedeutung für die Priorisierung der Testziele im Vergleich zu „klassischen“ Systemen:

<table>
<thead>
<tr>
<th>Grund</th>
<th>Qualitätsmerkmal</th>
</tr>
</thead>
<tbody>
<tr>
<td>spezifische (verteilte) Architekturen</td>
<td>Interoperabilität</td>
</tr>
<tr>
<td></td>
<td>Performanz und Leistungsfähigkeit</td>
</tr>
<tr>
<td></td>
<td>Anpassbarkeit</td>
</tr>
<tr>
<td></td>
<td>Robustheit und Resilienz</td>
</tr>
<tr>
<td>verknüpfte Lebenszyklen und Interdisziplinarität</td>
<td>Kompatibilität</td>
</tr>
<tr>
<td></td>
<td>Wartbarkeit</td>
</tr>
<tr>
<td></td>
<td>Übertragbarkeit</td>
</tr>
<tr>
<td>verknüpfte und umfassende Geschäftsprozesse, welche mit IoT-Systemen abgebildet werden</td>
<td>Funktionale Sicherheit (Safety)</td>
</tr>
<tr>
<td></td>
<td>IT-Sicherheit (Security)</td>
</tr>
<tr>
<td></td>
<td>Vertraulichkeit (Privacy)</td>
</tr>
<tr>
<td></td>
<td>Gebrauchstauglichkeit</td>
</tr>
<tr>
<td></td>
<td>Ethische Aspekte</td>
</tr>
</tbody>
</table>

Tabelle 3: Verstärkt zu testende Qualitätsmerkmale und ihre Motivation

Es ist hilfreich, die IoT Prüfanforderungen und Testziele in die Gruppen Prozess, System/Komponente und Kommunikationsprotokoll zu untergliedern.

IoT-QE LZ 44 (K3) Risikobasierte Priorisierung von Testzielen durchführen können [30]

Übung zu Testzielen für IoT-Systeme

Die Kursteilnehmer bilden Gruppen zu je etwa 3-4 Mitgliedern und lösen folgende Aufgabenstellungen an Hand eines konkreten Beispiels (z.B. Smart Home):

- Welche Testziele gibt es? Wie lassen sich diese gruppieren?
- Welche Prioritäten ergeben sich aus der Risikoanalyse?

Anschließend werden die Ergebnisse von den Gruppen vorgestellt und im Plenum diskutiert.

5.4 Testbarkeit und Testautomatisierung [15]

- Besonderheiten des IoT Testens (10 Min)

IoT-QE LZ 45 (K2) Die Besonderheiten beim IoT Testen benennen und Beispiele für IoT Tests auf verschiedenen Ebenen erläutern können [10]

Besonderheiten des IoT Testens in Ergänzung zu „klassischem“ Software- und Protokoll-Testen sind in der folgenden Tabelle aufgeführt [Schieferdecker 16].

<table>
<thead>
<tr>
<th>Perspektive</th>
<th>Besonderheiten</th>
<th>Testvarianten neben klassischem Software- und Protokoll-Testen</th>
</tr>
</thead>
</table>

Tabelle 4: Besonderheiten des IoT Testens
- Testautomatisierung (5 Min)

IoT-QE LZ 46 (K2) Die Notwendigkeit der Testautomatisierung für den IoT Test erläutern können [15]

Um einen effektiven Test zu gewährleisten ist ein hoher Grad an Testautomatisierung über alle Testphasen zu erlangen, da

- Sicherung der Qualität im Lebenszyklus mit einem hohen Grad an Testregression verbunden ist,
- der Faktor time to market eine wesentliche und kontinuierliche Bedeutung hat,
- die Komplexität und Dynamik des Systemkontexts für das IoT Produkt hoch ist,
- manuelle Vorgänge ein höheres Fehlerrisiko aufweisen als automatisierte Vorgänge.

5.5 Testprozess und Testarchitektur [15]

- IoT Testarchitekturen (15 Min)

IoT-QE LZ 47 (K2) IoT Testarchitekturen und typische IoT Testobjekte erläutern können [15]

Da IoT Systeme verteilte Systeme sind, kommen verteilte Testarchitekturen und entsprechende Prozessstrategien zum Einsatz, unter anderem Verbesserung der Effizienz durch Virtualisierung über das gesamte Testsystem. Für IoT Testsysteme sind folgende Testarchitekturen typisch (für Beispiele siehe z.B. [Jäkel 17]):

- Geräte basierte IoT Testarchitektur (z.B. für das Testen von Retroboxen oder Gateways), entsprechend der AIOTI IoT Schicht.
- Dienst basierte IoT Testarchitektur (z.B. für das Daten-orientierte Testen von Dashboards in der Cloud), entsprechend der AIOTI Applikationsschicht.
- Infrastruktur basierte IoT Testarchitektur, (z.B. für das Testen von oneM2M Funktionswerte), entsprechend der AIOTI Netzwerkschicht.

SUT und Testsystem können für verschiedene Testanforderungen ihre Rollen vertauschen. D.h. es kann sinnvoll sein, eine Komponente in einem Fall als SUT und im anderen Fall als Testsystem einzusetzen, welches das SUT stimuliert.

Es ist dafür zu sorgen, dass die Testumgebung lückenlos in die Prozess- und Toolumgebung integriert ist, typischerweise über den gesamten Lebenszyklus und in eine DevOps Prozessumgebung.

IoT-QE LZ 48 (K2) Wesentliche Aspekte der IoT Testarchitektur erläutern können [15]

Wesentliche Aspekte der Testautomatisierungsarchitektur sind [ISTQB 16]:

- Das Verständnis der Technologien des System under Test (SUT) sowie von dessen Integration in das Testautomatisierungssystem (TAS). Spezifisch für IoT:
  - IoT Testschnittstellen typischerweise auf Protokoll Level und Service Level.
  - für eine zukunftssichere Implementierung bedarf es eine sorgfältige Analyse der Testschnittstellen.
  - typische Interaktion zwischen SUT und TAS sind ereignisgetrieben und Peer-to-peer.
  - Systemgrenzen des SUT sind entscheidend für die Effizienz und Effektivität des TAS, diese können für verschiedene Testanforderungen variieren.
- Das Verständnis der Testumgebung. Spezifisch für IoT:
  - Simulation von Testumgebungen hat für IoT eine wesentlich größere Bedeutung als im „klassischen“ Test.
  - Mögliche variable Systemgrenzen zwischen SUT und TAS müssen in der Testarchitektur berücksichtigt werden.
o die Wartbarkeit der Testumgebung spielt eine wichtige Rolle.
o die reale Einsatzumgebung des IoT Produkts ist zu berücksichtigen.
o die Integration der Testumgebung in DevOps Tools ist zu berücksichtigen.

- Zeit, Aufwand und Komplexität der Implementierung (Planung und Controlling).
- Benutzerfreundlichkeit der Implementierung (Design ausgerichtet auf die Benutzerprofile der Tester als Anwender). Spezifisch für IoT:
  o da IoT Entwicklungsprojekte hochgradig interdisziplinär sind, müssen Anforderungen an die Benutzerfreundlichkeit aller beteiligten Rollen Beachtung finden.

5.6 Testmethoden [95]

- Wichtige IoT Testmethoden (20 Min)

IoT-QE LZ 49 (K2) Nutzbarkeit und Grenzen klassischer Testmethoden für IoT Systeme erläutern können [20]


Modellgetriebene Analysestrategien / Modellbasiertes Testen stellen optimale Analysemethoden (auch für die Definition der Systemgrenzen des SUT) zur Verfügung und sind eine wichtige Best Practice für Tests von IoT Systemen. Online MBT [ISTQB 17] ist eine Antwort auf den sich weiterentwickelnden Testentwurf entlang der Dynamik in IoT.


Während der Ausführung von Betriebs-/Laufzeittests kann es erforderlich sein, dass zu einem späteren Zeitpunkt die zugehörigen Testerwartungen (test purposes) verfeinert werden.

- Sicherheitstest (20 Min)

IoT-QE LZ 50 (K2) Die besonderen Anforderungen an das Testen von IoT Lösungen auf Sicherheit und die Anwendungen entsprechender Testmethoden auf unterschiedlichen Ebenen der IoT Architektur erläutern können [20]


Sicherheitstest notwendig. IOT Sicherheit ist nicht nur Geräte-Sicherheit! Die Absicherung einer einzelnen Teilkomponente ist nicht ausreichend zur Gewährleistung der Sicherheit des Gesamtsystems.

Im Folgenden werden die wichtigsten Testschwerpunkte aus verschiedenen Perspektiven dargestellt:

<table>
<thead>
<tr>
<th>Perspektive</th>
<th>Angriffsvektoren</th>
<th>Methoden</th>
</tr>
</thead>
</table>
| **Applikationen** (Analytics, Visualisierung und Steuerung) | - Mobile Applikationen  
- Webapplikationen  
- Daten- und Kontrollströme | - Test auf Webschwachstellen  
- Test auf sensitive Daten bei mobilen Geräten  
- Datenstromanalyse / Proxy / Man in the Middle-Angriffe  
- Denial of Service  
- Suche nach logischen Schwachstellen im Gesamtkonzept |
| **IoT-Schicht** (Plattformen und Schnittstellen, Computation, Aggregation- und Storage-Dienste) | - Cloud-Dienste  
- Webinterfaces (Konfigurationsinterfaces) der Geräte  
- Daten- und Kontrollströme  
- Zugriffs- und Rechtemanagement  
- Update Mechanismen (over the air updates)  
- Lokalisierungs Service | - Test auf Webschwachstellen  
- Datenstromanalyse / Proxy / Man in the Middle-Angriffe  
- Suche nach Protokollschwachstellen oder Fehlkonfigurationen, z.B. unverschlüsselte Kommunikationsverbindungen  
- Denial of Service  
- Suche nach logischen Schwachstellen im Gesamtkonzept  
- Spoofing von Endgeräten |
| **Physikalische Perspektive** (Geräte, Gerätekonnektivität) | - Backend APIs  
- Daten- und Kontrollströme  
- Verschlüsselung  
- Sonstige Kommunikation zwischen IoT-Schicht und Netzwerk-Schicht  
- Gerätespeicher und Speichererweiterung (z.B. SD-Karten)  
- Firmware der Geräte  
- Physikalische Geräteschnittstellen  
- Netzwerkschnittstellen der Geräte | - Datenstromanalyse / Proxy / Man in the Middle-Angriffe  
- Suche nach logischen Schwachstellen im Gesamtkonzept  
- Test auf Webschwachstellen  
- Ausnutzung von bekannten Protokollschwachstellen  
- Denial of Service  
- Suche nach sensitiven Daten (Passwörter, Schlüssel, …) und Manipulation von Daten  
- Firmwareanalyse  
- Seitenkanalangriffe |
Physikalische Manipulation oder Diebstahl der Geräte | Suche nach logischen Schwachstellen im Gesamtkonzept

<table>
<thead>
<tr>
<th>Testobjekt</th>
<th>Methoden</th>
<th>Was wird getestet?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technische Interoperabilität</td>
<td>Basis-Tests von Konnektivität und Kommunikationsprotokollen</td>
<td>Koppelung von Hardware/Software Komponenten um eine Basis-Kommunikation zu gewährleisten</td>
</tr>
<tr>
<td>Syntaktische Interoperabilität</td>
<td>Gezielte Überprüfung von Nachrichtenformaten bzw. der Syntax abstrakter Datenformate, Anwendung von Encoder/Decoder</td>
<td>Einhaltung der Syntax von z.B. HTML, XML oder ASN.1 Datenstrukturen</td>
</tr>
<tr>
<td>Semantische Interoperabilität</td>
<td>Durchführung von Fallbeispielen und Nutzerszenarien, ggf. unter Einbeziehung von standardisierten Use Case Katalogen</td>
<td>Es wird geprüft ob die Implementierungen der interoperierenden Komponenten/Systeme einer gemeinsamer Interpretation folgen</td>
</tr>
</tbody>
</table>

(Tabellized) Katalog von Testzielen, die in tabellarischer Form Angaben zu Konfiguration, sequenziellen Abläufen von Triggern und Beobachtungen der beteiligten Komponenten oder Systemen vorgeben

Standardisierte Testziele. Pluggtests

Tabelle 5: Testschwerpunkte für Sicherheitstests

- Interoperabilitätstest (15 Min)

IoT-QE LZ 51 (K2) Die besonderen Anforderungen an das Testen von IoT Lösungen auf Interoperabilität und die Anwendungen entsprechender Testmethoden auf unterschiedlichen Ebenen der IoT Architektur erläutern können [15]


Hinweis: In der Regel werden die Interoperabilitätstests nach erfolgreicherem Abschluss von Konformitätstests (z.B. durch TTCN-3 Technologie) durchgeführt.

Wichtige Methoden des Interoperabilitätstests sind:

Tabelle 6: Wichtige Methoden der Interoperabilitätstests

- Performanz Test (20 Min)

IoT-QE LZ 52 (K2) Die besonderen Anforderungen an das Testen von IoT Lösungen auf Performanz und die Anwendungen entsprechender Testmethoden auf unterschiedlichen Ebenen der IoT Architektur erläutern können [20]


Beispiele von Methoden und Werkzeuge für Performanz Tests [ISTQB 16]:

<table>
<thead>
<tr>
<th>Methoden</th>
<th>Werkzeug-Beispiele</th>
<th>Erläuterungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamische Analyse</td>
<td>Dynamische Analysewerkzeuge decken Fehlerzustände auf, wie sie lediglich zur Laufzeit eines Programms sichtbar werden, also z.B. Zeitabhängigkeiten und Speicherengpässe.</td>
<td>Diese werden typischerweise im Komponenten- und Komponentenintegrationstest sowie im Rahmen der Tests der Middleware verwendet.</td>
</tr>
<tr>
<td>Performanz Test / Lasttest / Stresstest</td>
<td>Performanztestwerkzeuge überwachen und protokollieren, wie sich ein System unter verschiedenen simulierten Benutzungsbedingungen verhält, hinsichtlich Anzahl konkurrierender Nutzer, Hochlauf-/Anlaufverhalten (ramp-up pattern) sowie Häufigkeit und relativem Anteil von Transaktionen. Die Last wird durch Erzeugen virtueller Nutzer simuliert, die einen ausgewählten Satz an Transaktionen durchführen, verteilt auf verschiedene Testmaschinen, allgemein bekannt als Lastgeneratoren.</td>
<td>Softwaretest, mit dem eine zu erwartende, auch extreme Last auf dem laufenden System erzeugt und das Verhalten desselbigen beobachtet und untersucht wird.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Testmonitore analysieren, verifizieren und zeichnen kontinuierlich die Verwendung von spezifischen Systemressourcen auf und geben Warnungen zu möglichen Problemen bei der Erbringung von Diensten aus.</td>
<td>z.B. zum Simulieren von Ereignisdaten</td>
</tr>
</tbody>
</table>

Tabelle 7: Methoden und Werkzeuge für Performanz Tests
- Produktzertifizierung (20 Min)

IoT-QE LZ 53 (K2) Die Herausforderungen bei der Prüfung auf Konformität und Zertifizierung erklären können [20]


Hauptfokus für IoT ist die Prüfung der IT-Sicherheit:

- funktionale Security-Anforderungen
- Stabilität
- Konformität und Fehleranfälligkeit einzelner IoT typischer Kommunikationsprotokolle

Deren Prinzipien unterscheiden sich nicht grundsätzlich von den IT-Sicherheitsprinzipien aus dem IT-Umfeld. Die Prüfkriterien sind jedoch auf das Umfeld und die speziellen Risiken abzustimmen. Insbesondere ist zu beachten, dass in der für IoT typischen langen Betriebsphase neue Sicherheitsvorfälle bekannt werden können und es zu zahlreichen Patches kommen kann, die die Frage nach der Gültigkeitsdauer eines Zertifikats aufwerfen und die Durchführung neuer bzw. eine Wiederholung von bestehenden Prüfungen erforderlich machen.

Auf diese generischen Standards kann zurückgegriffen werden [Wardaschka 17]:

- Protokollspezifische IoT Normen und -Standards
- Standards mit funktionalen Anforderungen
- Standards mit nicht-funktionalen Anforderungen (Performanz, Verfügbarkeit, Zuverlässigkeit, Dokumentation, (Arbeits-)Prozesse)
- Zu entwicklende IoT spezifische Standards

5.7 Zusammenfassung [10 Min]
6 Lifecycle [45]

Begriffe

<table>
<thead>
<tr>
<th>IIoT</th>
<th>Industrielles Internet der Dinge bedeutet die Anwendung des IoT auf die verarbeitende Industrie (Industrielles Internet oder Industrie 4.0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrie 4.0</td>
<td>Industrie 4.0&quot; steht für ein &quot;Zukunftsprojekt&quot; der deutschen Bundesregierung und bezeichnet die „vierte industrielle Revolution“. Wesentliche Merkmale der vierten industriellen Revolution sind Individualisierung bzw. Hybridisierung der Produkte und die Integration von interdisziplinären Stakeholdern und Geschäftsprozessen.</td>
</tr>
</tbody>
</table>


6.1 Im IoT-Kontext verknüpfte Lebenszyklen mit ihren Phasen und ihre Bedeutung aus QE-Sicht [15]

IoT-QE LZ 54 (K2) Die Bedeutung der im IoT Kontext verknüpften Lebenszyklen für das QE verstehen [15]


<table>
<thead>
<tr>
<th>Phase</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate</td>
<td>Die Entwicklung oder die Einbindung einer im IoT Kontext einzusetzenden Entität (z.B. Gerät, Service, Infrastruktur, Daten) wird angestoßen.</td>
</tr>
<tr>
<td>Build</td>
<td>Die Entität wird konzipiert und notwendige Voraussetzungen wie IoT Infrastruktur und Organisationsstrukturen werden geschaffen.</td>
</tr>
<tr>
<td>Develop</td>
<td>Die Entität wird entwickelt und in die IoT Zielumgebung ausgerollt.</td>
</tr>
<tr>
<td>Operate</td>
<td>Die Entität wird in ihrer IoT Zielumgebung betrieben und unterstützende Kundendienstleistungen erbracht.</td>
</tr>
<tr>
<td>Update</td>
<td>Die Entität wird gewartet wobei Korrekturen aber auch funktionale wie nicht-funktionale Verbesserungen ausgerollt werden.</td>
</tr>
<tr>
<td>Decommission</td>
<td>Die Entität hat das Ende ihres Lebenszyklusses erreicht und wird außer Betrieb genommen.</td>
</tr>
</tbody>
</table>

Tabelle 8: Phasen im IoT Produkt Lebenszyklus nach ISO/IEC CD 30141

6.2 Die besondere Bedeutung der Interdisziplinarität für den IoT-Lebenszyklus verstehen [30]

- Die interdisziplinäre Natur des IoT-Lebenszyklus (15 Min)

Die unterschiedlichen Perspektiven im IoT-Lebenszyklus beziehen sich auf die jeweils zu betrachtende Phase und welche Daten und Services in dieser Phase Wem zur Verfügung gestellt werden. Generell werden die gesammelten Daten an einen cloudbasierten Service gesendet, dort mit anderen Daten aggregiert (Daten/Informationen werden aus unterschiedlichen Quellen zusammengefasst) und in Interaktion mit dem Endbenutzer genutzt.

Was daran interdisziplinär ist, zeigt sich in der enormen Vielfalt der Möglichkeiten in Bezug auf:

- Daten sammeln, aggregieren, sicher übertragen,
- die Auswahl an Lösungen für Gateways,
- genutzte Software und Tools für IoT Applikationen,
- verschiedenste Services sowie
- diverse IoT Plattformen und -Frameworks.

Diese Vielfalt an technischer Infrastruktur wird durch die am Lebenszyklus beteiligten unterschiedlichen Branchen samt der diversen Experten ergänzt und erhöht damit die interdisziplinäre Natur des IoT-Lebenszyklus.

Hinzu kommt die interdisziplinäre Abstimmung bezüglich Produkt und Prozessen auf technischer, organisatorischer und Management Ebene (Geschäftsebene) in jeder Phase.

- Drittbeiligte im IoT-Lebenszyklus und ihre Bedeutung (15 Min)


Weniger abstrakt gibt es im IoT Life Cycle maßgebliche Drittbeiligte, die direkten Einfluss auf QE Maßnahmen haben. Sie initiieren Anforderungen und Vorschriften, die wiederum über den gesamten
IoT-Lebenszyklus bei Planung, Durchführung, Kontrolle und Optimierung von Quality Engineering Maßnahmen zur berücksichtigen sind. Zu diesen Drittbeteiligten gehören:

- Gesetzgeber
- Normierungsgremien
- Prüfstellen/Zertifizierungsstellen
- Betriebsräte/Personalräte
- Verbände/Vereinigungen

### Anhang A  Begriffe / Glossar

<table>
<thead>
<tr>
<th>Begriff</th>
<th>Seite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet of Things, Internet der Dinge (IoT)</td>
<td>8</td>
</tr>
<tr>
<td>Digital Twin</td>
<td>8</td>
</tr>
<tr>
<td>Konstruktives Quality Engineering</td>
<td>8</td>
</tr>
<tr>
<td>Qualitätsmerkmal</td>
<td>13</td>
</tr>
<tr>
<td>Funktionale Sicherheit (Safety)</td>
<td>13</td>
</tr>
<tr>
<td>IT-Sicherheit (Security)</td>
<td>13</td>
</tr>
<tr>
<td>Robustheit</td>
<td>13</td>
</tr>
<tr>
<td>Resilienz</td>
<td>13</td>
</tr>
<tr>
<td>Performanz</td>
<td>13</td>
</tr>
<tr>
<td>Interoperabilität</td>
<td>13</td>
</tr>
<tr>
<td>Gebrauchstauglichkeit (engl. Usability)</td>
<td>13</td>
</tr>
<tr>
<td>Wartbarkeit</td>
<td>13</td>
</tr>
<tr>
<td>Produkt-Zertifikat</td>
<td>13</td>
</tr>
<tr>
<td>Edge Computing</td>
<td>24</td>
</tr>
<tr>
<td>Fog Computing</td>
<td>24</td>
</tr>
<tr>
<td>Referenzmodell</td>
<td>24</td>
</tr>
<tr>
<td>DevOps</td>
<td>29</td>
</tr>
<tr>
<td>Agile Softwareentwicklung</td>
<td>29</td>
</tr>
<tr>
<td>Update-Fähigkeit</td>
<td>29</td>
</tr>
<tr>
<td>Fuzz Testing</td>
<td>34</td>
</tr>
<tr>
<td>Konformität</td>
<td>34</td>
</tr>
<tr>
<td>Things under Test</td>
<td>34</td>
</tr>
<tr>
<td>Datenqualität</td>
<td>34</td>
</tr>
<tr>
<td>IIoT 4</td>
<td>44</td>
</tr>
<tr>
<td>Industrie 4.0</td>
<td>44</td>
</tr>
</tbody>
</table>
Anhang B Referenzen

\url{https://aioti.eu/wp-content/uploads/2018/06/AIOTI-HLA-R4.0.7.1-Final.pdf}
[DIN SPEC 91345] DIN SPEC 91345, Referenzarchitekturmodell Industrie 4.0 (RAMI4.0), April 2016
\url{http://www.etsi.org/deliver/etsi_eg/203200_203299/203251/01.01.01_60/eg_203251v010101p.pdf}
[Heidrich 16] Mike Heidrich und Jijun Luo, Industrial Internet of Things, Referenzarchitektur für die Kommunikation,
\url{https://www.esk.fraunhofer.de/content/dam/esk/dokumente/Whitepaper_IoT_dt_April16.pdf}
\url{https://www.vde-verlag.de/iec-normen/preview-pdf/info_iec61508-1%7Bed2.0%7Db.pdf}
\url{https://standards.ieee.org/findstds/standard/1028-2008.html}
\url{https://www.iso.org/standard/35733.html}
\url{http://www.iso27001security.com/html/27034.html}
\url{https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf}
\url{https://www.iso.org/standard/50508.html}
https://www.iso.org/standard/22749.html


[ISTQB 16] ISTQB® Certified Tester Advanced Level Syllabus “Test Automation Engineer” (2016)


http://www.onem2m.org/component/rsfiles/download-file/files?path=Release_2_Draft_TS%255CTS%5C001-Functional_Architecture-V2_19_0.docx&Itemid=238

[oneM2M drafts] oneM2M published drafts, http://www.onem2m.org/technical/published-drafts

[RAMI 4.0 15] Das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0), Martin Hankel und Bosch Rexroth (2015)

[Riedel 16] Oliver Riedel et al, Modellbasierte modulare Shopfloor IT - Integration in die Werkzeuge der Digitalen Fabrik (2016)
http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-3162488.pdf


[Weyrich 16] Michael Weyrich et al, Referenzarchitekturen für das IoT: Überblick zum Stand der Technik und wesentliche Trends,
Anhang C  Lernziel / Kognitive Ebenen des Lernens

Auszug aus [ISTQB 11]:

Taxonomiestufe 1: **Kennen (K1)**
Der Lernende ruft im Gedächtnis gespeicherte Informationen (z.B. Begriffe, isolierte Fakten, Abfolgen, Prinzipien, Mittel und Wege) ab. Typische beobachtbare Leistungen sind erkennen, nennen, bezeichnen.

**Schlüsselworte:** sich erinnern, erkennen, wiedergeben, kennen

Taxonomiestufe 2: **Verstehen (K2)**
Der Lernende begründet oder erläutert Aussagen zum Thema. Typische beobachtbare Leistungen sind beschreiben, zusammenfassen, vergleichen, klassifizieren, begründen, erklären, Beispiele für Testkonzepte nennen.

**Schlüsselworte:** zusammenfassen, verallgemeinern, abstrahieren, klassifizieren, vergleichen, auf etwas übertragen, etwas gegenüberstellen, erläutern, interpretieren, übersetzen, darstellen, rückschließen, folgern, kategorisieren, Modelle konstruieren, erklären, Beispiele geben, begründen, verstehen

Taxonomiestufe 3: **Anwenden (K3)**
Der Lernende überträgt erworbenes Wissen auf gegebene neue Situationen oder wendet sie zur Problemlösung an. Typische beobachtbare Leistungen sind ausführen, anwenden, beurteilen, ermitteln, entwerfen, analysieren.

**Schlüsselworte:** anwenden, einsetzen, ausführen, nutzen, Verfahren verstehen, Verfahren anwenden