R4.1: Stand IoT Labore / Auswahl viel versprechender Protokolle

Abgleich Wissensstand im Projekt

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Version 0.1, Datum: 01.06.2017

Autoren:

André Wardaschka (Ed) - DEKRA
Axel Rennoch (Ed) - Fraunhofer FOKUS
Michael Wagner - Fraunhofer FOKUS
Rutten, Stefan - DEKRA
Frank-Walter Jäkel - Fraunhofer IPK
Stefan Stoelzle - AUDI AG
Paul Hopton - Relayr
Yuliya Brynzak - Relayr

Inhalt

1. Einleitung

Das Labor (vom lateinischen *laborare* = „arbeiten“, „leiden“, „sich abmühen“) bezeichnet im Allgemeinen einen Arbeitsplatz zur Durchführung verschiedener Experimente, Prozess- und Qualitätskontrollen, Prüfungen und Messungen [6].

Da das angestrebte Ziel der Zertifizierung von IoT Teil-Systemen neben Prüflaboratorium auch eine Inspektions- und Zertifizierungsstelle benötigt, wird im Anschluss zunächst auf die Erläuterung dieser Begriffe eingegangen. Des Weiteren wird die Bedeutung einer Zertifizierungsstelle erläutert. Dabei ist es wichtig, die Bedeutung und Notwendigkeit der Akkreditierung zu verstehen, weshalb diesem Thema ein eigenes Kapitel gewidmet ist.

Grundlagen der Zertifizierung bilden hierbei Leit-, Richtlinien, Normen und Standards. Daher wird im Folgenden kurz der gegenwärtige Stand grundlegender Standards und Normen für den IoT Bereich aufgezeigt. Hierbei wird auch erläutert, warum die existierenden Standards und Normen nicht ohne weiteres auf den IoT-Bereich anwendbar sind, sondern neue IoT-spezifische Standards benötigen.

Den Abschluss bilden eine Übersicht gegenwärtiger Prüflabore, sowie ein Ausblick anstehender Standardisierungsarbeiten zur Realisierung eines IoT-Labors.

2. Begrifflichkeiten

Zertifikate werden grundsätzlich nur von Zertifizierungsstellen ausgestellt. Dabei entscheidet die Zertifizierungsstelle, welche Bereiche zu prüfen sind. Die Prüfaufträge werden im Anschluss vom Zertifizierer bei Bedarf an qualifizierte, unabhängige Prüflabore vergeben und die Ergebnisse von der Zertifizierungsstelle bewertet. Daher ist es durchaus möglich, dass verschiedene Prüflabore von unterschiedlichen Anbietern in unterschiedlichen Bereichen mit Prüfungen beauftragt werden.

Die Inspektions- und Prüfergebnisse werden von der Zertifizierungsstelle evaluiert und hiernach bei positivem Ergebnis gegebenenfalls ein Zertifikat ausgestellt.

2.1. Prüflaboratorium

ISO/IEC 17025 („Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien“) hat sich seit seiner ersten Veröffentlichung im Jahre 1999 zu *dem* Hauptstandard für Prüf- und Kalibrierlaboratorien entwickelt. Er regelt die Kompetenz, Unparteilichkeit und konsistente Arbeitsweise von Laboratorien. Zu den Anwendern dieser Norm gehören nicht nur Laboratorien und deren Kunden, sondern auch Akkreditierungs- und Zertifizierungsstellen, die mit Hilfe dieser Norm die Kompetenz von Laboratorien nachvollziehen beziehungsweise nachweisen können.

Die zwei Hauptabschnitte des ISO/IEC 17025 Standards beschreiben die

Anforderungen an das Management zu den Themen

- Organisation, Managementsystem
- Lenkung der Dokumente
- Prüfung von Anfragen
- Angeboten und Verträgen, Vergabe von Prüfungen und Kalibrierungen im Unterauftrag
- Beschaffung von Dienstleistungen und Ausrüstungen
- Dienstleistungen für den Kunden

- Beschwerden
- Lenkung bei fehlerhaften Prüf- und Kalibrierungsarbeiten
- Verbesserung
- Korrekturmaßnahmenvorbeugende Maßnahmen
- Lenkung von Aufzeichnungen
- Interne Audits
- Managementbewertungen

und

Technische Anforderungen an

- Personal
- Räumlichkeiten und Umgebungsbedingungen
- Prüfverfahren und deren Validierung
- Einrichtungen
- Messtechnische Rückführung
- Probenahme
- Handhabung von Prüfgegenständen
- Sicherung der Qualität
- Ergebnisberichte

Dabei dienen die Management-Anforderungen dem Betrieb und der Effektivität eines Qualitäts-Managementsystems des Labors. Die technischen Anforderungen hingegen beinhalten die Faktoren, welche die Richtigkeit und Zuverlässigkeit von Laborergebnissen beeinflussen können. Die Einhaltung der Vorgaben an Management und Technik ermöglicht zusammen das Erreichen von gleichbleibend gültigen Ergebnissen.

Angelehnt an ISO 9001 ist die Erfüllung der Anforderungen durch entsprechende Dokumentation zu belegen.

2.2. Inspektionsstelle

Unter Inspektion versteht man die „Untersuchung der Entwicklungs- und Konstruktionsunterlagen eines Produktes, eines Produktes selbst, eines Prozesses oder einer Anlage und Ermittlung seiner/ihrer Konformität mit spezifischen Anforderungen oder, auf der Grundlage einer sachverständigen Beurteilung, mit allgemeinen Anforderungen“ (DIN EN ISO/IEC 17000:2005, 4.3)/[7].

Die Aufgabe einer Inspektionsstelle besteht darin, die Konformität inspizierter Gegenstände oder Prozesse mit Vorschriften, Normen, Spezifikationen, Inspektionsprogrammen oder Verträgen zu *bewerten*. Der Inspektionsauftrag kann im Allgemeinen von Privatkunden, Gesellschaften oder Behörden kommen. Bei einer angestrebten Zertifizierung kommt der Auftrag jedoch direkt von der Zertifizierungsstelle.

Eine Inspektionsstelle bewertet daher nicht nur die Prüfergebnisse von Laboratorien, sondern auch die Erfüllung nicht-funktionaler Anforderungen.

Die Prüfdienstleistung kann hierbei durch einen oder mehrere Unterauftragnehmer (Prüflaboratorien) oder durch die Inspektionsstelle selbst erfolgen. Eine personelle Trennung ist bei Prüfungen durch die Inspektionsstelle nicht gefordert [7].

Neben allgemeinen Anforderungen zu Unparteilichkeit, Unabhängigkeit und Vertraulichkeit regelt ISO/IEC 17020 die Anforderungen an

- Verwaltung, Organisation und Management einer Inspektionsstelle,
- Ressourcen (Personal, Einrichtung, Geräte)
- Prozesse (z.B. zu Verfahren, Dokumentation, Beschwerden und Einsprüche)
- das Managementsystem (insbesondere Dokumentation und deren Lenkung und Ergebnisbewertungen)

Ein wichtiger Unterschied der Inspektion zu Prüfungen und Zertifizierungen besteht darin, dass bei vielen Typen von Inspektionen ein sachverständiges Urteil zur Ermittlung der Akzeptanz nach „allgemeinen Kriterien“ mit einbezogen wird. Daher wird ein besonderes Augenmerk auf die Kompetenz der Inspektoren gelegt.

2.3. Zertifizierungsstelle

Die Zertifizierung von Produkten, Prozessen oder Dienstleistungen ist ein Mittel, um sicherzustellen, dass sie den Normen und anderen normativen Dokumenten festgelegten Anforderungen entsprechen [DIN EN ISO/IEC 17065:2013-01].

Die Norm ISO/IEC 17065 enthält Grundsätze und Anforderungen an die Kompetenz und Unparteilichkeit der Zertifizierung von Produkten, Dienstleistungen und Prozessen sowie der Stellen, die diese Tätigkeiten anbieten. Dabei wird auf die Unparteilichkeit der Zertifizierungsstelle besonders Wert gelegt, um die Akzeptanz zertifizierter Produkte, Prozesse und Dienstleistungen zu fördern.

Eine Zertifizierungsstelle ist hierbei das hauptsächlich rechtlich haftbare Glied in dem Prozess einer Konformitätsbewertung. Sie ist in diesem Prozess das Organ, welches Zertifizierungsanträge entgegen nimmt, typischerweise die Prüf- und Inspektionsaufträge vergibt und nach abschließender Evaluierung von Prüf-, Inspektions- und Auditergebnissen gegebenenfalls ein Zertifikat ausstellt. Die Zertifizierungen sind hierbei oftmals zeitlich begrenzt.

3. Notwendigkeit der Akkreditierung

Prinzipiell darf jedes Unternehmen prüfen, testen und sogar Zertifikate ausstellen. Doch selbst die Prüfung gleicher Anforderungen durch unterschiedliche Laboratorien garantiert nicht gleiche Ergebnisse, da sich qualitative Unterschiede auch im Ergebnis niederschlagen. Das Vertrauen in Zertifikate, Inspektionen, Prüfungen oder Kalibrierungen steht und fällt jedoch mit dem Vertrauen in die Kompetenz desjenigen, der die Bewertungsleistung erbringt.

Aus diesem Grund werden Prüf-, Inspektions- und Zertifizierungsstellen formal „akkreditiert“ (lat. „Glauben schenken“). In diesem Verfahren weisen sie gegenüber einer unabhängigen Akkreditierungsstelle nach, dass sie ihre Tätigkeiten fachlich kompetent, unter Beachtung gesetzlicher sowie normativer Anforderungen und auf international vergleichbarem Niveau erbringen. Die Akkreditierungsstelle (in Deutschland die „Deutsche Akkreditierungsstelle“ (DAkkS)) begutachtet und überwacht dabei das Managementsystem und die Kompetenz des eingesetzten Personals. Die Akkreditierung belegt daher die Qualität der Arbeit einer Konformitätsbewertungsstelle. Akkreditierungen tragen somit entscheidend dazu bei, die Vergleichbarkeit von

Konformitätsbewertungsergebnissen zu gewährleisten und Vertrauen in die Qualität und Sicherheit von Produkten und Dienstleistungen zu erzeugen.

Die Anforderungen an Akkreditierungsstellen, die Konformitätsbewertungsstellen wie Laboratorien, Inspektions- und Zertifizierungsstellen akkreditieren, sind in der Norm DIN EN ISO/IEC 17011 festgelegt. Diese Norm definiert Akkreditierung als

> „Bestätigung durch eine dritte Seite, die formal darlegt, dass eine Konformitätsbewertungsstelle die Kompetenz besitzt, bestimmte Konformitätsbewertungsaufgaben durchzuführen“ [9]

Die der Akkreditierung zugrunde liegenden Normen sind international harmonisiert. Hierdurch wird gewährleistet, dass die Akkreditierung weltweit nach gleichen Maßstäben erfolgt. Dank harmonisierter Normen und internationaler Abkommen werden die Bewertungsleistungen der in Deutschland akkreditierten Stellen in vielen anderen Ländern anerkannt.

Hierdurch ergeben sich die folgenden Vorteile der Konformitätsbewertung durch akkreditierte Stellen:

Für Prüflabore, Inspektions- und Zertifizierungsstellen:

- Objektiver Nachweis für Qualität und Kompetenz
- Unterscheidungsmerkmal und somit Wettbewerbsvorteil

Für Unternehmen:

- Internationale Vergleichbarkeit von Zertifikaten, Prüfungen und Inspektionen
- Vermeidung mehrfacher Bewertungen und hierdurch verursachte Mehrfach-Kosten durch internationale Anerkennung
- Erleichterte Auswahl von Prüf-, Inspektions- und Zertifizierungsstellen
- Unterscheidungsmerkmal und somit Wettbewerbsvorteil

Für Verbraucher:

- Vergleichbarkeit von Bewertungsaussagen (national und international)
- Erhöhte Transparenz bei Qualitätsaussagen
- Höheres Vertrauen in Produktqualität
- Verbesserte Produkte durch weniger Produktfehler

4. Grundlegende Standards und Normen im IoT-Bereich

Der Begriff „Standard“ wird im deutschen Sprachgebrauch als Oberbegriff für Industrie-Standards und Normen verwendet. Eine Norm bezeichnet hierbei die Formulierung und Publikation von Anforderungen, Methoden und Regeln durch eine anerkannte Organisation oder Normungs-Gremium[1]. Aus einer Norm alleine leitet sich noch keine Rechtsbindung ab, sondern erst durch die Anwendung einer Norm zur Erfüllung einer (rechtlich bindenden) Richtlinie.

[1] Im englischen Sprachgebrauch gibt es diese Unterscheidung nicht, was im deutschen Sprachgebrauch teilweise zu Verwirrungen führt

Im Gegensatz dazu beinhalten Industrie-Standards (so genannte „De-facto“-Standards) Anforderungen, Methoden und Regeln, welche sich über die Zeit eine breite Akzeptanz verschafft haben und sich hierdurch in eher stillschweigender Übereinkunft etabliert haben. Hierzu zählen oftmals Übertragungsprotokoll-Spezifikationen.

Als Grundlage einer Zertifizierung und Akkreditierung können sowohl Normen als auch Standards dienen, weshalb in Bezug auf das IoT-(Prüf-)Labor im Folgenden sowohl Normen als auch (Industrie-)Standards betrachtet werden.

Gegenwärtig gibt es jedoch keinen „IoT-Standard“, sondern allenfalls eine Ansammlung von übergeordneten Normen, welche jedoch zu allgemein sind, um daraus für den IoT-Anwendungsbereich Prüfmethoden und Bewertungskriterien ableiten zu können. Eine IoT-spezifische Norm oder Standard ist jedoch eine zwingende Voraussetzung für ein IoT-Labor. Dabei kann es sich sowohl um einen proprietären (z.B. Dekra-)Standard als auch Norm handeln. Dabei könnte ein IoT-Labor auf Basis eines proprietären Standards als Übergangslösung und Echo-System bis zur Verabschiedung einer Norm dienen.

Hauptfokus des IoT-Labors wird die Prüfung von Security (Informations-Sicherheit) sein. Neben funktionalen Security-Anforderungen wird hierbei die Stabilität geprüft und die Konformität und Fehleranfälligkeit einzelner IoT-typischer Kommunikations-Protokolle untersucht. Da die gegenwärtigen Internet- und Funk-Protokolle auch im IoT-Kontext Verwendung finden, wird man sich im Rahmen dieses Projektes auf die Prüfung der wichtigsten IoT-Protokolle der Anwendungsschicht des TCP/IP Modells beschränken. Konformitätsprüfungen von IoT-Funkprotokollen werden hierbei gänzlich ausgeschlossen, um durch die hiermit verbundenen Kosten die Marktakzeptanz einer Prüfung und Zertifizierung nicht schon im Vorfeld zu minimieren.

Im Bereich IoT Security existieren zurzeit allenfalls Whitepaper oder Leitlinien, wie zum Beispiel die *Strategic Principles for Securing the Internet of Things* [10] des amerikanischen Departments of Homeland Security. Diese haben jedoch keinen bindenden Charakter und sind vielmehr als Hilfestellung für die Entwicklung gedacht und weniger als trennscharf formulierte Grundlage für Prüfinstitutionen.

Da sich die Prinzipien der Informations-Sicherheit für IoT-Geräte jedoch nicht von den Security-Prinzipien aus dem IT und Automatisierungs-Umfeld unterscheiden, kann bei der Erstellung eines neuen Standards auf eine Fülle bestehender Anforderungen zurückgegriffen werden. Die Herausforderung besteht hierbei darin, aus der Fülle von Empfehlungen und Standards die für den IoT Anwendungsfall minimalen Anforderungen zu formulieren. Dabei ist es von entscheidender Bedeutung, dass die Anforderungen prüfbar sind und dazugehörige Prüfmethoden und Prüfkriterien formuliert werden.

Als wesentliche Grundlage dienen hierbei die Standards, die in den folgenden Kapiteln kurz vorgestellt werden. Hinzu kommen Publikationen und Empfehlungen, die für einzelne Teilbereiche herangezogen werden, wie beispielsweise

- NIST SP 800-82 Rev. 2 *Guide to Industrial Control Systems* [11]
- NIST SP 800-183 *Network of ‚Things‘* [12]
- NIST SP 800-12 Rev. 1 *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* [13]
- NIST SP 800-12 Rev. 1 *An Introduction to Information Security* [14]

- OWASP *Best Practices* [15]
- OWASP *Top 10* [16]
- BSI TR-02102 *Kryptographische Verfahren: Empfehlungen und Schlüssellängen* [23]
- NIST SP 800-57 *Recommendation for Key Management* [24][25]

4.1. Protokollspezifische IoT Normen und Standards

Das Internet der Dinge kann mit altbekannten Technologien aus dem Bereich der Web-Anwendungen aufgebaut werden. So können IoT-Sub-Systeme mittels bekannter Protokolle, wie HTTP(S), JSON, WebSockets oder XMPP miteinander verbunden werden, was in der Praxis auch der Fall ist. Da diese Protokolle jedoch nicht IoT spezifisch sind, werden diese im Rahmen des IoT-T-Projektes bei der Konformitätsprüfung nicht speziell betrachtet.

Trotz der existierenden Web-Protokolle haben sich weitere Standards etabliert. Dies ist dem Umstand geschuldet, dass IoT-Systeme teilweise spezielle Anforderungen zu erfüllen haben. So wurden neue Protokolle geschaffen, um z.B. einem niedrigen Verbrauch an Energie und Bandbreite zu genügen oder trotz großer Latenz noch zu funktionieren. Die unterschiedlichen Anforderungen erklären daher, warum sich mehrere Standards parallel etabliert haben und es nicht nur ein einziges IoT Protokoll der Anwenderschicht zu betrachten gilt.

Speziell für den IoT-Einsatz haben sich hierbei die folgenden Protokolle etabliert:

- ISO/IEC PRF 02922 MQTT (Message Queue Telemetry Transport Protocol)
- RFC 7228 CoAP (Constrained Application Protocol)
- IEC 62541 OPC-UA (Open Platform Architecture - Unified Architecture)

4.2. Standards mit funktionalen Anforderungen

4.2.1. Common Criteria

Mit den Common Criteria (ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation, kurz CC) [1] wurde ein Standard zur Bewertung und Prüfung von Sicherheitsfunktionalitäten von IT Produkten nach gestaffelten Vertrauenswürdigkeitsstufen geschaffen.

Die Common Criteria bieten Mittel zur Spezifikation der Sicherheitsanforderungen und eine einheitliche Methodik zur Evaluierung und Bewertung der umgesetzten Sicherheitsfunktionalitäten. Im Rahmen spezieller Abkommen ist ein Common Criteria IT-Sicherheitszertifikat international anerkannt und ermöglicht die Gegenüberstellung der Sicherheitseigenschaften zertifizierter Produkte. Ein CC Zertifikat liefert klare Aussagen bezüglich der behaupteten Sicherheitseigenschaften: Korrektheit der Sicherheitsfunktionalität, Wirksamkeit der Sicherheitsfunktionalität gegen Angriffe, Analyse der potentiellen Schwachstellen sowie entsprechende Prüftiefe. Ausgehend von den Sicherheitsvorgaben (Security Target, ST), die dem Zertifikat zugrunde liegen, hat der Abnehmer des zertifizierten Produkts die Möglichkeit, die entsprechende Sicherheitsfunktionalität zu erfassen und zu entscheiden, inwieweit dieses Produkt für den geplanten Einsatzzweck und die vorgesehene Einsatzumgebung aus sicherheitstechnischer Sicht geeignet ist.

In den jeweiligen Ländern sind staatliche oder staatlich anerkannte Institutionen für die Zertifizierung nach CC verantwortlich. Die entsprechenden Prozesse und nationalen Charakteristika werden durch

die nationalen Zertifizierungsschemata festgelegt. In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Zertifizierung von Produkten nach Common Criteria verantwortlich. Das BSI begleitet deren Evaluierung, so dass die Vergleichbarkeit der Bewertung sowie ein hohes Vertrauen in die Ergebnisse gewährleistet sind. Die rechtliche Grundlage zur Durchführung von Zertifizierungsverfahren bilden die Zertifizierungsverordnung und das Gesetz zur Stärkung der Sicherheit der Informationstechnik des Bundes.

Für den Nutzer bzw. Kunden ist es essenziell zu wissen, in welchem Maße er Zusicherungen über die Sicherheit eines Produktes tatsächlich vertrauen kann. Die Common Criteria verfolgen daher das Ziel, dem Nutzer je nach EAL-Stufe eine dem Sicherheitsbedarf angepasste Menge von Belegen für die Vertrauenswürdigkeit des Produkts an die Hand zu geben. Diese Belege zeigen, welche Maßnahmen bei Entwicklung und Realisierung des Produkts getroffen wurden, um das Produkt sicher zu machen. Die so belegte Vertrauenswürdigkeit ist natürlich an verschiedene Bedingungen gebunden. Beispielsweise muss der Nutzer stets in der Lage sein, zu identifizieren, ob er tatsächlich das zertifizierte Produkt (in der zertifizierten Version) in der Hand hat. Auch Handbücher, Datenblätter und andere „Guidance-Dokumente“ werden im Rahmen der Common Criteria evaluiert. Dadurch wird sichergestellt, dass dem Nutzer alle nötigen Informationen zur Verfügung stehen, um das Produkt sachgemäß und vor allem ohne (sonst evtl. selbst verursachte) Sicherheitsbeeinträchtigungen einsetzen zu können.

Die CC berücksichtigen auch die zukünftige Weiterentwicklung zertifizierter Produkte sowie die parallel stattfindende Evolution von Bedrohungen und Angriffstechniken. Wenn im Rahmen einer Produktweiterentwicklung sicherheitsrelevante Änderungen vorgenommen wurden, wird eine Re-Zertifizierung erforderlich. Bei wesentlichen Änderungen der Bedrohungslage wird analog ein Re-Assessment durchgeführt. Hersteller sind weiterhin verpflichtet, der Zertifizierungsstelle neu bekannt gewordene Angriffe auf zertifizierte Produkte mitzuteilen. Darüber hinaus ist generell der Gültigkeitszeitraum eines CC-Zertifikats stets zeitlich beschränkt.

4.2.2. System und Komponentenanforderungen gemäß IEC 62443

Bei der IEC 62443 Normenreihe handelt es sich um ein Regelwerk zur Informations-Sicherheit industrieller Kommunikationsnetze. Dabei liegt der ursprünglich gedachte Anwenderkreis auf dem Gebiet der industriellen Automatisierungstechnik. Die Standardserie richtet sich neben Betreibern, Produkt-Integratoren, -Lieferanten, Dienstleistern und Behörden auch an Genehmigungsstellen. Da es keine vergleichbare Standardserie im Security-Bereich gibt, die sowohl funktionale, als auch nicht-funktionale Anforderungen in diesem Umfang stellt, scheint sich diese Norm-Reihe nunmehr weit über die ursprünglich angedachte Anwendung der Automatisierungstechnik hinaus zu etablieren. So wird diese Normreihe mittlerweile auch von anderen Gebieten, wie dem der Funktionalen Sicherheit [22], referenziert und findet damit indirekt Anwendung in Bereichen wie Automotive, Maschinen Sicherheit oder Medizintechnik.

Des Weiteren führt der Standard in Anlehnung an *Safety Integrity Level* bei der Funktionalen Sicherheit das Konzept der *Security Level* bei den funktionalen Anforderungen ein. Hierdurch findet der Standard prinzipiell Anwendung in Bereichen unterschiedlichster Risikotoleranz. So sind die Anforderungen so allgemein gehalten, dass sie sowohl bei kritischen Industrieanlagen als auch Konsumenten-Endgeräte als Grundgerüst herangezogen werden können. Direkt auf IoT anwendbar ist die IEC 62443-Serie jedoch nicht, da die Anforderungen, Testmethoden und Bewertungskriterien dem neuen Kontext angepasst werden müssen.

4.3. Standards mit nicht-funktionalen Anforderungen

Das IoT Prüflabor wird größtenteils funktionale Anforderungen prüfen. Dennoch soll an dieser Stelle auf nicht-funktionale Anforderungen eingegangen werden, da diese teilweise Voraussetzung für eine sinnvolle Prüfung sind.

Nicht-funktionale Anforderungen beziehen sich typischerweise auf ein Qualitätsmerkmal wie

- Performanz
- Verfügbarkeit
- Zuverlässigkeit
- Dokumentation
- (Arbeits-)Prozesse

So beschreibt zum Beispiel IEC 62443-2 (s. **Fehler! Verweisquelle konnte nicht gefunden werden.**) die notwendigen Prozeduren eines Informations-Sicherheits- Management-Systems von Betreibern. Die Anforderungen entsprechen hier dem Grundschutz nach ISO 27001 und werden für das IoT-Prüflabor nicht weiter betrachtet.

Security relevante Anforderungen an Verfügbarkeit und Zuverlässigkeit werden hingegen durch IEC 62443-3-3 und 62443-4-2 mit abgedeckt und sind Teil der Tests.

Die zur Prüfung notwendige Dokumentation kann durch Anforderungen an einen gut funktionierenden Entwicklungsprozess gemäß IEC 62443-4-1 abgeleitet werden.

5. Zu entwickelnde IoT spezifische Standards

In Deutschland erfolgt die Mitarbeit an der internationalen Standardisierungsarbeit der ISO zum Thema Internet of Things im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), Arbeitsausschuss Internet of Things [2]. Zu den aktuellen Projekten zählen neben einem Standard zu Definitionen und Vokabular, die Referenzarchitektur zu IoT (IoT RA), IoT use cases und ein Framework zur Interoperabilität von IoT Systemen.

Ein weiterer DIN NIA Arbeitskreis „IT-Sicherheitsmaßnahmen für IoT Devices“ befindet sich derzeit noch in der Gründungsphase. Sein Ziel ist die Betrachtung der Herausforderungen an die IT-Sicherheit durch die zunehmende Zahl vernetzter Geräte, vom Unternehmen bis in den Endkonsumentenmarkt hinein. Alleine durch die hohe Anzahl an Geräten wird die Wahrscheinlichkeit des Auftretens ausnutzbarer Schwachstellen, wie auch die Auswirkung bei Ausnutzung dieser Schwachstellen, enorm erhöht. Um diesen Bedrohungen entgegenzuwirken soll nun, von der Koordinierungsstelle IT-Sicherheit initiiert, eine DIN Spezifikation erstellt werden, welche einen Satz an Maßnahmen zur Sicherstellung eines Mindestmaßes an IT-Sicherheit dieser Geräte enthält. Diese Spezifikation soll dabei helfen, einen Mindeststandard in Bezug auf IT-Sicherheit zu definieren und zu etablieren, indem sie beispielsweise als Referenz bei der Auswahl von Zulieferern herangezogen werden und somit unter anderem als Vertragsgrundlage dienen kann. [3]

Bei der Analyse zur den Herausforderungen an die IT-Sicherheit der Vielzahl von vernetzten Geräten fordert eine Studie von Industrieunternehmen und der Europäischen Agentur ENISA [4] von der EU die Erstellung von Europäischen Basisanforderungen, eine Evaluation und Zertifizierung durch unabhängige Einrichtungen sowie die Einführung eines sog. EU Trust Label. In diesem Zusammenhang

wird empfohlen auf Standards aufzubauen, die die Unterstützung der europäischen Industrie bzw. Regierungseinrichtungen haben.

6. Gegenwärtiger Stand IoT relevanter Prüflaboratorien

Derzeit gibt es kein einziges IoT Prüflabor, wohl aber Labore, die sich mit angrenzenden Themen befassen. Zu nennen sind hier Labore

1. zur Feststellung von Protokoll-Konformität eines Produkts, wie zum Beispiel die von der *OPC Foundation* beauftragten Testlabore in Europa und Amerika zur Überprüfung einer OPC-UA Konformität [17]
2. vom Bundesamt für Sicherheit (BSI) autorisierte Prüflabore
    - zur Prüfung von informationstechnischen Produkten wie Smart Cards, Smart Meters, Betriebssysteme, Datenbanken und Firewalls gemäß Common Criteria [19]
    - zur Prüfung von technischen Richtlinien [18]
    - zur Durchführung von Penetrationstests [20]
3. zu Forschungszwecken, wie zum Beispiel das Stanford Computer Security Lab [21]
4. von allgemein als vertrauenswürdig geltenden Organisationen autorisierte Labore. So ist es zum Beispiel seit Anfang 2017 möglich, oneM2M Produkte bei der *Telecommunications Technology Association* (TTA) in Südkorea zertifizieren zu lassen. Durch die enge Zusammenarbeit von TTA mit der oneM2M Organisation, die auch durch ETSI unterstützt wird, kann die Zertifizierung als Vorbild durchaus als Vorbild für europäische Zertifizierungsverfahren dienen. Insbesondere sind die für die Testprozedur zugrunde gelegten, ausführlichen Definitionen von Testkonfigurationen und systematischen Testfällen erwähnenswert.

Daneben gibt es eine Vielzahl von Dienstleistern, die Penetrationstests gemäß eigener Prüfverfahren und Maßstäbe durchführen.

Als kritisch zu bewerten ist bei den oben aufgeführten Laboren, dass eine gleichbleibende Qualität und Unabhängigkeit nicht gewährleistet ist. So lässt selbst das Bundesamt für Sicherheit zu, dass die vom BSI autorisierten Prüflabore gleichzeitig Beratungstätigkeiten ausüben, was eine Objektivität der Prüfung von vorne herein ausschließt. Des Weiteren wird weder von den Laboren eine Akkreditierung verlangt noch eine benannte Stelle zur Ausgabe eines (DAkkS-) Zertifikates gefordert. Eine gleichbleibende Qualität der Labore und „Zertifizierungsstelle“ ist daher rein subjektiv und nicht durch eine objektive Institution wie der Deutschen Akkreditierungsstelle (DAkkS) oder vergleichbaren internationalen Institutionen gesichert.

7. Zusammenfassung und Ausblick

Die Vision des zukünftigen IoT-Prüflabors beinhaltet die folgenden Grundbausteine und Nebenbedingungen:

- ein (oder mehrere) verabschiedete, international anerkannte IoT spezifische Standards
- allgemein anerkannte Prüfmethoden und Bewertungskriterien für IoT Security-Anforderungen
- validierte Prüf-Software, um alle funktionalen Anforderungen automatisiert zu testen
- eine benannte, vertrauenswürdige Zertifizierungsstelle (wie beispielsweise die DEKRA)
- ein akkreditiertes IoT Prüflabor

Da sich das Förderprojekt auf die Dauer von zwei Jahren beschränkt, ist es absehbar, dass in diesem Zeitraum nicht alle Punkte umsetzbar sind.

8. Referenzen

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. https://www.commoncriteriaportal.org/cc/

[2] DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), NA 043-01-41 AA Arbeitsausschuss Internet of Things. http://www.din.de/de/wdc-grem:din21:193522726

[3] DIN NA 043-01-41 AA N 884: Einladung zur Gründungssitzung GAK „IT-Sicherheitsmaßnahmen für IoT Devices“, Juli 2017.

[4] Infineon – NXP – STMicroelectronics – ENISA: Common Position On Cybersecurity, Dez. 2016. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

[5] ETSI Industry Specification Groups. http://www.etsi.org/about/how-we-work/how-we-organize-our-work/industry-specification-groups-isgs

[6] https://de.wikipedia.org/wiki/Labor

[7] DAkkS: Festlegungen für die Anwendung der DIN EN ISO/IEC 17020:2012, http://www.dakks.de/sites/default/files/71_sd_0_012_anwendung_17020-2012_20131028_v1.1.pdf

[8] DIN EN ISO/IEC 17065:2013-01: Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren (ISO/IEC 17065:2012)

[9] http://www.dakks.de/content/was-ist-akkreditierung

[10] Homeland security – Securing the Internet of Things https://www.dhs.gov/securingtheIoT

[11] NIST SP 800-82 Rev. 2 *Guide to Industrial Control Systems (ICS) Security* http://dx.doi.org/10.6028/NIST.SP.800-82r2

[12] NIST SP 800-183 *Network of ‚Things‘* http://dx.doi.org/10.6028/NIST.SP.800-183

[13] NIST SP 800-52 Rev. 1 *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* http://dx.doi.org/10.6028/NIST.SP.800-52r1

[14] NIST SP 800-12 Rev. 1 *An Introduction to Information Security* http://dx.doi.org/10.6028/NIST.SP.800-12r1

[15] OWASP Best Practices https://www.owasp.org/index.php/Category:OWASP_Best_Practices

[16] OWASP Top 10 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[17] OPC Foundation Test Labs https://opcfoundation.org/certification/how-to-certify/

[18] BSI Liste der Prüfstellen von Technischen Richtlinien https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/TR-Liste/TR_Pruefstellen.html

[19] BSI Liste der CC / ITSEC Prüfstellen https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/CC_Liste/cc_itsec_pruefstellen.html

[20] BSI Liste zertifizierter IT-Sicherheitsdienstleister https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/IS_REV_PEN/IS_REV_Dienstleister/stellen_zertifizierung_pentester-is-revisoren.html

[21] Stanford Computer Security Laboratory https://seclab.stanford.edu/

[22] Generic Standard for Functional Safety IEC 61508-1:2010

[23]BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
[24]NIST SP 800-57 Part 1 Rev. 4 Recommendation for Key Management, Part 1: General http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4
[25]NIST SP 800-57 Part 2 Recommendation for Key Management, Part 2: Best Practices for Key Management Organization http://dx.doi.org/10.6028/NIST.SP.800-57p2