TESTAUTOMATISIERUNG FÜR INTEROPERABILITÄT UND IT-SICHERHEIT VON IOT-PLATTFORMEN UND -ANWENDUNGEN

Smart Service Welt

Impressum

Herausgeber
Begleitforschung Smart Service Welt I
Institut für Innovation und Technik (iit)
in der VDI/VDE Innovation + Technik GmbH

Dr. Inessa Seifert
Steinplatz 1
10623 Berlin
seifert@iit-berlin.de

Texte und Redaktion
Begleitforschung Smart Service Welt I

Gestaltung
Loesch*Hund*Liepold Kommunikation GmbH

Bilder
Fotohaus Zacharias (S. 4), André Wardaschka (S. 6), FotoStudio Elif (S. 8), Fraunhofer IPK/Katharina Strohmeier (S. 10), Nicole Hackel (S. 11)

Stand
Mai 2019

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

EDITORIAL

Reibungslose Kommunikation immer und überall, durchgehende Interoperabilität und hohe Erwartungen an Datenschutz und IT-Sicherheit – die Anforderungen an Serviceplattformen für das Internet der Dinge (Internet of Things, IoT) steigen.

Durch das industrielle IoT löst sich die klassische Automatisierungspyramide der industriellen Fertigung auf: In der digitalen Produktion kann jedes Gerät oder jede Anlage potenziell mit jedem oder jeder anderen kommunizieren. Das Erfassen, Verarbeiten und Analysieren von Sensor- und Prozessdaten findet dabei immer häufiger auf IoT-Plattformen in der Cloud statt. Der IT-Sicherheit und Interoperabilität von Kommunikationsschnittstellen und -protokollen kommt dabei eine besondere Bedeutung zu: Zum einen müssen die IoT-Kommunikationsprotokolle Cyberattacken standhalten, zum anderen bei der wachsenden Anzahl der vernetzten Sensoren, Aktoren und Geräte stets die gleiche Kommunikationssprache sprechen. Sie müssen also mit den standardisierten Spezifikationen übereinstimmen. Hier helfen automatisierte Tests, die den Betreibern von IoT-Plattformen und -Anwendungen das Management und die Nutzung von zahlreichen Kommunikationsschnittstellen und -protokollen erleichtern.

Die Begleitforschung zum Technologieprogramm Smart Service Welt hat gemeinsam mit dem Smart-Service-Welt-Projekt „IoT Testing – Testautomatisierung für IoT-Plattformen und -Anwendungen“[1] (IoT-T) den gleichnamigen Workshop am Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS organisiert, um sich mit den Projekten der BMWi-Technologieprogramme Smart Service Welt I und II sowie PAiCE über Ergebnisse und Erkenntnisse auszutauschen. Im Rahmen des Workshops widmeten sich die Teilnehmenden den aktuellen Herausforderungen bei der Bewertung der Interoperabilität und IT-Sicherheit von Kommunikationsprotokollen für das industrielle IoT. Besonderes Augenmerk lag auf dem neuen Ansatz der Standardisierung der Prüfziele für automatisierte Tests in Kombination mit Open-Source-Lösungen. Diese ermöglichen sowohl den IoT-Anwendungsentwicklern und IT-Sicherheitsprüfern als auch den Endanwendern die erforderliche Transparenz bei der IT-Sicherheit.

Um technologische Trends und offene Forschungsfragen im Bereich der Testautomatisierung für IoT-Plattformen und -Anwendungen einem größeren Kreis als den Workshop-Teilnehmenden zugänglich zu machen, wird die Expertise der Workshop-Referenten in dieser Interviewsammlung vorgestellt. Damit werden Einblicke in führende Industrieunternehmen, cloudbasierte IoT-Plattformbetreiber, Prüfunternehmen und Forschungseinrichtungen gewährt. Bei den Beiträgen handelt es sich um die individuellen Meinungen der Interviewten. Die Experten Jens Stomber (AUDI AG), Alexander Kaiser (relayr), André Wardaschka (DEKRA), Frank-Walter Jäkel (Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik IPK) und Sascha Hackel (Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS) standen Rede und Antwort zu unter anderem folgenden Fragen:

- Wie werden Produktionsprozesse durch die modernen Kommunikationstechnologien verändert?
- Inwieweit wird Open-Source-Software in Deutschlands Schlüsselbranche, der Automobilindustrie, eingesetzt?
- Wie verändert das Internet der Dinge das Geschäft der Cloudcomputing-Anbieter und Plattformbetreiber?
- Wie rüsten sich die traditionellen Prüferunternehmen im Hinblick auf die Herausforderungen im für sie neuen Geschäftsfeld der IT-Sicherheit für das Internet der Dinge?

Insgesamt lässt sich beobachten, dass die Welt der Open-Source-Software (OSS) und der Standardisierungsaktivitäten auf der europäischen Ebene zusammenwachsen. Auch der zunehmende wirtschaftliche Einfluss der Open-Source-Organisationen wie eclipse, Linux und Apache auf den Softwaremarkt und insbesondere auf die produzierenden Unternehmen nimmt zu. IT-Riesen wie Microsoft, Google, Amazon und IBM haben schon lange die Vorteile von OSS entdeckt, mit der die Kosten für die Softwareentwicklung gesenkt werden können. Nun steigen auch die traditionellen deutschen Konzerne wie Audi in die Welt der Open-Source-Foundations-Ökonomie ein.

Wir danken dem Konsortium des IoT-T-Projekts herzlichst für die Bereitschaft zu den hier abgedruckten Gesprächen und dafür, die Expertise auch einer breiteren Öffentlichkeit zugänglich zu machen.

1 Siehe http://www.iot-t.de, zuletzt geprüft am 5.12.2018.

„AN OPEN SOURCE KOMMEN WIR IN DER AUTOMOBILBRANCHE NICHT VORBEI.“

Jens Stomber
Digitale Prozessplanung, AUDI AG
Tel.: 0841-89 57 14 14
jens.stomber@audi.de

Herr Stomber, wie ist Ihre Sicht auf die modernen Kommunikationstechnologien für die Produktion?

Die Herausforderung für uns ist es, die Technologien in die relativ langen Produktlebenszyklen der Automobilindustrie einzubinden, die aktuell bei rund sieben Jahren liegen. Stellen Sie sich ein bereits bewohntes Haus vor, in welchem Sie die einzelnen Geräte und die Haustechnik neu vernetzen wollen: Für die Netzwerkverbindungen müssen die Wände aufgerissen und überall Kabel mit hohem Zeit- und Kostenaufwand neu verlegt werden. Ähnliches gilt für die Produktionsprozesse bei einem Fahrzeughersteller wie VW oder Audi, die dem Fließbandprinzip folgen. Das Produkt und der Fertigungsablauf werden über einen Zeitraum von circa zwei Jahren ausgeplant und optimiert. Anschließend erfolgt die Projektierung und Umsetzung der Fertigungslinien „in Stahl und Eisen“. Bei Automatisierungstechnik und Kommunikationstechnologien kommen dabei bewährte Konzernstandards zum Einsatz, damit die Technologien im rauen Produktionsumfeld beherrschbar bleiben und die anschließende Instandhaltung gewährleistet ist. Kommunikationstechnologien im Nachhinein zu ändern, erscheint nicht zielführend, weil Anlagentechnik und Fertigungsabläufe bereits festgelegt sind. Die Leistungskenngrößen wie Stückzahlen, Varianten oder Durchlaufzeiten lassen sich kaum durch Aufrüsten mit neuen Technologien verbessern.

Wo können neue Kommunikationstechnologien in der Produktion zum Einsatz kommen?

Moderne Kommunikationstechnologien stiften erst dann einen Nutzen, wenn durch sie neue Fertigungskonzepte möglich werden, die einen Produktivitätszuwachs versprechen.

An welchen Stellen profitieren Sie in bestehenden Fertigungsprozessen von – auch nachgerüsteten – Kommunikationstechnologien?

Lösungen zur Werkerführung kommen in Fertigungsbereichen mit niedrigerem Automatisierungsgrad zum Einsatz, beispielsweise in der Fahrzeugendmontage oder im Prüf- und Finish-Bereich. In einigen bestehenden Anlagen gibt es Komponenten mit einer zusätzlichen Kommunikationsschnittstelle, zum Beispiel in Form eines OPC UA[2] Embedded Controllers. Diese Komponenten können wir nachträglich in der laufenden Produktion in Gebrauch nehmen, um Daten von Prozessendgeräten in eine eigens dafür ausgelegte Infrastruktur zu schreiben – in einen sogenannten Data Lake der Produktion.

Welche Perspektiven für den Einsatz von Kommunikationstechnologien gibt es bei der Planung von neuen Standorten?

Neue Projekte wie die E-Motorenfertigung am Standort Győr bieten beispielsweise die Möglichkeit, modulare Montage auf der Basis von fahrerlosen Transportsystemen zu pilotieren.

In welche Richtung wird sich der Fertigungsprozess vor dem Hintergrund der Digitalisierung und der Kommunikationstechnologien Ihrer Meinung nach grundsätzlich entwickeln?

Ich bin überzeugt davon, dass grundsätzlich die größten Potenziale in kürzeren Produktlebenszyklen und kleineren Losgrößen liegen, die aber deutlich mehr Flexibilität erfordern. Doch nicht nur die Fertigungseinrichtungen innerhalb einer Produktionshalle müssen sich vernetzen, um das Potenzial voll zu nutzen. Der Produktionsprozess muss unternehmensübergreifend gesehen werden: Gerade die kleineren Zuliefererunternehmen können sich dann zu einem Produktionsnetzwerk zusammenschließen und als Konsortium auftreten. Denkbar ist auch ein horizontales Kapazitätsmanagement, bei dem ein Unternehmen einem anderen Unternehmen seinen Maschinenpark auftragsbezogen zur Verfügung stellt.

Sind funkbasierte Kommunikationstechnologien eine bessere Lösung?

Funkbasierte Kommunikationsprotokolle wie WirelessHART, ISA100.11a oder ZigBee sind zwar bereits seit

2 OPC Unified Architecture (The Industrial Interoperability Standard): https://opcfoundation.org

Jahren verfügbar, entsprechen jedoch nicht den hohen Echtzeitanforderungen und der geforderten Ausfallsicherheit hochautomatisierter Lösungen: Beispielsweise können im Anlagenprozess beim Karosseriebau temporäre Funkschatten durch große Metallflächen wie Frontklappen oder Seitenwandrahmen entstehen, die die Kommunikation unterbrechen. Eine Notausfunktion oder andere zeitkritische Signale können daher aktuell nur mit kabelbasierten Feldbussen prozesssicher realisiert werden. Die Anwendung des neuen Mobilfunkstandards 5G in Verbindung mit TSN, dem Time-Sensitive Networking, wird zurzeit untersucht, ist produktiv aber noch nicht im Einsatz.

Welche Rolle spielt dabei Open-Source-Software?

OSS ist in der Produktion noch vergleichsweise wenig verbreitet und dies aus verschiedenen Gründen. Erstens betragen die Kosten für auf uns zugeschnittene, kommerzielle Softwareentwicklung nur einen Bruchteil der Gesamtkosten für die Beschaffung von Fertigungseinrichtungen. Beim Bau einer neuen Fabrik liegt der Anteil an Kosten für die IT beispielsweise zwischen zwei und vier Prozent der Gesamtkosten. Außerdem scheuen viele Unternehmen die Risiken von Lizenzverletzungen. Und schließlich möchten Großunternehmen die Software auf Maschinensteuerungen nicht unbedingt selbst weiterentwickeln. Dies ist von Maschinenherstellern nicht vorgesehen.

OSS hat sich aber bereits aus den Bereichen Internethosting und Rechenzentrum in den Office-Bereich hinein entwickelt. Meine Prognose ist, dass künftig auch die Fabriken von Open Source erobert werden: Open Source begeistert aktuell mehr Entwickler, insbesondere aus Forschung und Start-ups. Wer innovativ sein und nicht den Anschluss verlieren will, muss sich zu Open Source bekennen. Hinzu kommt, dass nur OSS die Transparenz bietet, die das Vertrauen der Anwender gewinnt. Wer die Transparenz in den Softwareentwicklungsprozessen benötigt und IT-Sicherheit gewährleisten muss, kommt an Open Source nicht vorbei. Bei Audi haben wir daher einen Open-Source-Diagnostics-Service eingerichtet. Dieser dient dazu, Lizenzbestimmungen für OSS zu überprüfen und verringert damit das Risiko von Lizenzverletzungen.

Bleiben wir beim Stichwort Sicherheit. Welche Prüfmethoden und Verfahren für IT-Sicherheit haben Sie etabliert?

Wir verfügen über ein etabliertes Prüfregime. In jedem IT-Projekt wird in der Konzeptphase neben der IT-Architekturfreigabe auch eine Freigabe des IT Sicherheitskonzeptes bei der Abteilung IT-Sicherheit eingeholt. Bei der Auslieferung der finalen Software wird durch einen Penetrationstest und ein Code-Review sichergestellt, dass die IT-Sicherheitsvorgaben auch umgesetzt wurden.

Software, die Teil einer Produktionsanlage ist bzw. nicht im Rechenzentrum, sondern im Shopfloor eingerüstet wird, gilt nicht als IT-Umfang bzw. als IT-Projekt und unterliegt daher nicht dem genannten Prüfregime. Insbesondere decken die Standardwerkzeuge für Penetrationstests wie zum Beispiel NESSUS oder OpenVAS nicht die in der Produktion verwendeten Kommunikationsprotokolle wie OPC UA ab. Mit der IEC 62443 existiert zunächst ein international anerkannter Standard für IT-Sicherheit in der Produktion, der jedoch nicht im Speziellen auf einzelne Kommunikationsprotokolle eingeht. Entsprechende Testfälle und Testverfahren müssen für Industrienetze durch die Macher der Protokolle bereitgestellt werden. Für Protokolle, die nicht von Industriekonsortien und Fabrikausrüstern betreut werden, sondern in der Open Source entwickelt werden, etabliert sich aktuell die MTS TST Arbeitsgruppe der ETSI – dem Europäischen Institut für Telekommunikationsnormen[3] – als Standardisierungsinstanz für Testfälle und Testwerkzeuge. Im nächsten Schritt müssen die bei ETSI entwickelten Testverfahren ihren Weg in die Lastenhefte und Inbetriebnahmeprozesse der Automobilindustrie finden. Bis dahin wird IT-Sicherheit in diesem Metier vor allem durch Trennung von Netzwerken und Zonierung erreicht.

An welchen Schnittstellen gibt es Optimierungspotenziale durch neue Testverfahren und Kommunikationstechnologien?

Zunächst existieren zwischen IT (Informationstechnologie) und OT (Operational Technology, das heißt Betreiber und Instandhalter in der Produktion) kulturelle und methodische Unterschiede beim Umgang mit IT-Sicherheit. Da Industrie 4.0 jedoch eine Datendurchgängigkeit vom Shopfloor über die MES- (Manufacturing Execution System) bis in die ERP- (Enterprise-Ressource-Planning) und Office-Ebene bedeutet, müssen IT und OT bei diesem wichtigen Thema künftig enger zusammenarbeiten. IT-Sicherheitsrichtlinien haben unternehmensweit Gültigkeit, auch in der Produktion. Das Repertoire der IT-Security-Governance wie Sicherheitsrichtlinien, Business-Impact-Analyse und Risikoanalyse wird aktuell Schritt für Schritt auch in der Produktion aufgebaut, denn ohne IT-Sicherheit ist Industrie 4.0 nicht denkbar.

3 Methods for Testing & Specification Testing Working Group: https://portal.etsi.org/tb.aspx?tbid=97&SubTB=97

„UNSER ZIEL IST ES, KRITERIEN UND PRÜFMETHODEN VERGLEICHBAR ZU MACHEN.“

André Wardaschka
DEKRA Testing and Certification GmbH
Tel: 0234-36 96-118
andre.wardaschka@dekra.com

Herr Wardaschka, was bedeutet das Internet der Dinge für Sie als Prüfer und Gutachter?

Immer mehr Geräte im Haushalt oder in einer Fabrik sind mit dem Internet verbunden – dadurch hat sich der Markt für Prüfer dramatisch vergrößert.

Ein Knackpunkt im Internet der Dinge ist die IT-Sicherheit. Wo liegen aus Ihrer Sicht die größten Herausforderungen?

Oberstes Ziel ist es, Menschen zu schützen, also Personenschaden zu minimieren und wenn irgend möglich zu vermeiden, beispielsweise beim Einsatz von Maschinen oder beim Schutz vor Explosionen. Hierbei handelt es sich um Safety-Aspekte. Man unterscheidet zwischen Safety (im Sinne von Vermeidung und Minimierung von Personenschäden) und Security (im Sinne von Angriffsprävention auf IT-Systeme). Im industriellen Kontext sind Safety-Aspekte im besonderen Maße wichtig. Heutzutage funktioniert Safety nicht ohne Security, denn das Internet ist ein Einfallstor und kann Safety-Maßnahmen zunichtemachen.

Wie unterstützen Sie Lösungen für IT-Sicherheit im Internet der Dinge?

Die Hersteller-Unternehmen kommen oftmals nicht aus der IT-Branche und haben dadurch große Anlaufschwierigkeiten im Bereich Security. Wir haben sehr gute, etablierte Beziehungen zu den produzierenden Unternehmen. Diesen bietet DEKRA neben Prüfungen auch Schulungen an. Darin zeigen wir, was bei der Entwicklung der neuen internetfähigen Geräte beachtet werden muss.

Gibt es bereits etablierte IT-Sicherheitsanforderungen im Internet der Dinge?

Welche Security-Mindestanforderungen ein internetfähiges Gerät erfüllen soll, bevor es auf den Markt kommt, ist momentan im Allgemeinen nicht geregelt. Die verfügbaren Empfehlungen – sogenannte Guidelines – beschreiben, welche Anforderungen prinzipiell erfüllt werden sollten. Die Empfehlungen reichen jedoch nicht. Sie zeigen verschiedene Lösungsmöglichkeiten auf, sie sind aber rechtlich nicht bindend. Eine Ausnahme bildet dabei das Gebiet der kritischen Infrastruktur, da es hier eine staatliche Regulierung gibt. Im Bereich Smart Metering gibt es zum Beispiel ein hohes staatliches Interesse, die IT-Sicherheit zu regeln. Für IoT-Bereiche, die nicht in staatliches Hoheitsgebiet fallen, gibt es derzeit noch keine Security-Regulierung. So beinhalten Guidelines keine Liste an Anforderungen oder Prüfkriterien, die es im Bereich nicht-kritischer Infrastrukturen einzuhalten gilt. Im Projekt IoT-T wurde aber durch die Einrichtung der ETSI-Arbeitsgruppe MTS TST ein Grundstein für die Prüfbarkeit gelegt. Hier haben wir begonnen, eine Anzahl solcher Anforderungen und Prüfkriterien zu definieren, sodass die Prüfer klar feststellen können, wann IT-Sicherheitsanforderungen erfüllt sind und wann nicht. Der Prüfer benötigt eine solche sogenannte rote Linie, mit deren Definition in den Standardisierungsaktivitäten bei ETSI angefangen wurde. Die Prüfkriterien stellen eine Entscheidungshilfe dar, um zu beurteilen, ob ein Gerät den Test bestanden hat oder nicht. Die Arbeit an dem neuen ETSI-Standard mit Prüfkriterien für Mindestanforderungen an IoT-Security hat aber gerade erst begonnen. Es ist zu erwarten, dass auch weitere Stakeholder ihr Interesse bekunden und dem Arbeitskreis beitreten werden. Unser Ziel ist es, die Kriterien genau festzuhalten, um die Prüfmethoden und -verfahren vergleichbar zu gestalten.

An welchen Standards und Normen sollten sich IoT-Entwickler orientieren?

Inzwischen hat sich im Bereich Security die IEC-62443-Normenreihe horizontal über verschiedene Domänen hinweg etabliert. Dieser Standard wurde zwar ursprünglich eigens für die Automatisierung entwickelt. Aufgrund seiner generischen Natur ist er auch auf andere Bereiche übertragbar. Der Einsatz in anderen Bereichen ist möglich, da die Anwendung durch spezifische Profile für Domänen angepasst werden kann. Im Rahmen von relevanten Safety-Normen wird die IEC 62443 daher mittlerweile auch referenziert. Der Standard lässt aber offen, wie er angewendet werden soll. Für die Hersteller ist oftmals unklar, wie die Test- und Bewertungskriterien für ihre Systeme aussehen sollten. Zusätzlich müssen die Hersteller der IoT-fähigen Produkte Security-Entwicklungsprozesse etablieren, um so zum

Beispiel auf mögliche Softwarefehler adäquat zu reagieren. Das sind häufig die Haupthürden, mit welchen die Hersteller ohne Security-Vorkenntnisse zu kämpfen haben.

Reichen die bestehenden Standards und Normen aus?

Keineswegs – denn für spezifische Bereiche werden oftmals spezifische Anforderungen benötigt. Es reicht auch nicht aus, die Standards auf nationaler Ebene zu definieren. Da Konzerne international agieren, wäre dies kontraproduktiv für alle Beteiligten. Idealerweise werden die Standards auf europäischer Ebene oder sogar weltweit definiert. Das Rahmenwerk wird hierbei teilweise von der europäischen ENISA (European Union Agency for Network and Information Security) und von nationalen Behörden wie dem BSI (Bundesamt für Sicherheit in der Informationstechnik) vorgegeben. Allerdings steht die ENISA mit wenigen Mitarbeiterinnen und Mitarbeitern den viel größeren nationalen Behörden wie dem BSI oder der französischen ANSSI (Agence nationale de la sécurité des systèmes d'information) verhältnismäßig unterrepräsentiert gegenüber. Dieses Ungleichgewicht kann dazu führen, dass die starken europäischen Industrienationen ihre De-facto-Standards durchsetzen, beziehungsweise Standards aus anderen Ländern nicht akzeptieren. Ein Beispiel dafür ist die französische Gesundheitskarte, die in Frankreich schon lange eingesetzt wird. Deutschland wird diese Lösungen nicht übernehmen und voraussichtlich seinen eigenen Weg gehen. Ein ähnliches Vorgehen wäre für den Bereich IoT-Security fatal.

Welche Chancen und Risiken bestehen beim Einsatz von Open-Source-Software in den Prüflaboren?

Open-Source-Software-Tools sind eine große Chance und haben einen sehr hohen Nutzen für die Prüflabore und Hersteller – unter der Voraussetzung, dass diese Software von der OSS-Community gepflegt wird. Viele OSS-Tools werden von Hochschulen und Forschungseinrichtungen initiiert, für die die Entwicklung und vor allem die langfristige Fortführung schwierig sind. Eine weitere wichtige Eigenschaft von OSS ist die Transparenz: Die Prüfer müssen wissen, was in dem Softwarecode enthalten ist und vor allem, was fehlt oder fehlerhaft ist. Allerdings schaffen nur etablierte Tools Vertrauen. Das führt zu einem Henne-Ei-Problem. Wird ein Fehler in einem IT-Security-Tool entdeckt, sollte eine Korrektur von der OSS-Community zeitnah und vor allem zuverlässig erfolgen. Die Fehlerkorrekturen müssen hierbei nachvollziehbar sein. Die OSS-Tools sind dabei eine Chance für alle Beteiligten, weil sie auch für das sogenannte Self-Assessment von Produzenten genutzt werden können, das keine Beteiligung von einer externen Prüferorganisation erfordert. Allerdings müssen bei OSS-Tools auch fortschreitende Versionen nachvollziehbar sein. Jede Prüfung muss dabei wiederholbar sein und immer gleiche Ergebnisse liefern. Bei Rückfragen der Auftraggeber müssen die gefundenen Probleme zudem nachvollziehbar präsentiert werden können.

Welche technologischen Herausforderungen und welchen Forschungsbedarf müssen Prüfer und Gutachter künftig adressieren?

Es läuft eher anders herum: Die Prüfer und Gutachter müssen sich stets auf den neuesten Stand bringen und mit der Forschung zusammenarbeiten. Die Forschung beschäftigt sich in der Regel intensiver mit den neuen Gefahren und Problemen und spiegelt die Ergebnisse in Richtung Prüfung. So erweitern wir stetig unseren Horizont. Neue Themen und Forschungsgebiete werden dabei entdeckt und erschlossen. Die aktuelle Forschung beschäftigt sich in der Regel viel intensiver mit der Herausforderung, neue Sicherheitslücken – sogenannte „zero day exploits" – ans Licht zu bringen. Der Hauptfokus der Prüfer liegt jedoch auf Sicherheitslücken, die schon bekannt sind und die oftmals in einem neuen Kontext wiederkehren. Daher sind auch die Impulse, die aus der IT-Sicherheitsforschung kommen, in der Regel viel stärker. Der Erfahrungsaustausch zwischen den Prüfern und Forschern erfolgt zum Beispiel über die Teilnahme an Fachkonferenzen. Die Prüfung profitiert hierbei von der Entwicklung der IT-Sicherheitsforschung. Wenn eine Lücke entdeckt wird, spiegelt sich das typischerweise auch in den Werkzeugen wider. Die Prüfer entwickeln hierbei in der Regel keine IT-Sicherheitstools. Es sind die Security-Forscher, die Probleme finden und öffentlich machen. Die Hersteller der Security-Tools greifen die Security-Probleme und Nachweismöglichkeiten auf. Die Prüfer und Gutachter finden sich meistens am Ende dieser Kette. Von der Wechselwirkung profitiert aber die ganze IT-Sicherheitscommunity.

Ein prominentes Beispiel für die Wechselwirkung war der Heartbleed-Implementierungsfehler in der Verschlüsselungsbibliothek OpenSSL. Bruce Schneier, eine weltberühmte Koryphäe der IT-Sicherheitsforschung, vertrat die Einschätzung, dass im Falle der Bewertung der Schadenshöhe auf einer Skala von 1 bis 10, Heartbleed 11 Punkte erhielte. Es ist davon auszugehen, dass die Lücke zumindest einzelnen Geheimdiensten bekannt war, bevor sie von Sicherheitsforschern entdeckt und publiziert wurde. Die Lücke wurde vom OpenSSL-Team geschlossen. Der Test auf diese Lücke ist heutzutage Standard in einer Reihe von kommerziellen und OSS-Werkzeugen.

Jede Veränderung von Softwareentwicklungen – egal ob kommerziell oder Open Source – schafft natürlich neue Angriffspunkte. Dabei agiert die öffentliche IT-Sicherheitscommunity als ein Gegenspieler zu Kriminellen und Geheimdiensten, die solche Lücken ausnutzen.

„ES ERÖFFNEN SICH NEUE GESCHÄFTSMODELLE FÜR ANWENDER UND BETREIBER.“

Alexander Kaiser
relayr GmbH
Tel.: 0176-63 17 04 41
E-Mail: alexander.kaiser@relayr.de

Herr Kaiser, wie verändern cloudbasierte Plattformen das produzierende Gewerbe?

In der Produktion fördern cloudbasierte Industrial-IoT-Plattformen (I-IoT-Plattformen) den Wandel zur datengetriebenen Ökonomie und verändern nachhaltig die Geschäftsmodelle in der Fertigungsindustrie.

Welche Prozesse sind dank cloudbasierten Plattformen leichter geworden?

Den größten Mehrwert stellt die Transparenz der Produktionsprozesse dar, welche durch die Vernetzung des I-IoT in Echtzeit überwacht und ausgewertet werden können. Das bietet die Möglichkeiten, Defekte oder auch potenzielle Flaschenhälse in der Produktion schneller und einfacher aufzudecken und Prozesse zu optimieren, indem man sie verbessert.

Gibt es auch Vorgänge, die komplizierter werden, wenn cloudbasierte Plattformen eingesetzt werden?

Insbesondere im Kontext einer schlanken Produktion – der sogenannten Lean Production – ist eine große Menge an qualitativ hochwertigen Daten notwendig. Durch den Einsatz von cloudbasierten Plattformen können solche Produktionsprozesse deutlich effizienter und mit höherer Automatisierung umgesetzt werden, weil Daten aus verschiedenen verteilten Sensorquellen auf der Plattform zentral gebündelt, effizient überwacht und analysiert werden. Zudem eröffnen die erfassten Daten sowohl den Anwendern als auch dem Betreiber der cloudbasierten Plattform neue Geschäftsmöglichkeiten. Allerdings ist es noch eine offene Herausforderung, das Potenzial der Daten effektiv zu nutzen.

Worin genau liegt aus Ihrer Sicht diese Herausforderung?

Zum einen ist die Menge der erhobenen Daten – Stichwort Big Data – enorm, zum anderen erfordert die Interpretation der Daten sowie deren Verwertung eine besondere Expertise und neues, zusätzliches Know-how. Die Produktionsausfälle werden oft mit menschlichen Fehlern zusammengebracht. Daher müssen die Datenschutzaspekte bei den anfallenden Daten so berücksichtig werden, dass die Privatsphäre der Mitarbeiterinnen und Mitarbeiter nicht verletzt wird. Der Umgang mit den Datenmengen in der Produktion ist komplexer geworden und muss erst verstanden und erlernt werden.

Was wird durch den Einsatz von automatisierten Tests für IKT-Dienstleister und Anwender leichter? Welche Prozesse verändern sich?

Automatisierte Tests sind im IKT-Bereich seit Jahren fester Bestandteil der Entwicklungsprozesse und spielen eine entscheidende Rolle bei Continuous Integration und Continuous Development (CI und CD). Dadurch wird eine gleichbleibende oder sogar steigende Qualität gewährleistet. Die Tests lassen sich zwar automatisieren, allerdings muss sichergestellt werden, was die durchgeführten Tests wirklich bedeuten. Die Ausführung der Tests ist also leichter geworden. Der Fokus soll aber insbesondere auf die Qualität der Tests gelegt werden. Die Verantwortung für die Qualitätssicherung darf keineswegs der Maschine übertragen werden. Die Interpretation der Testergebnisse ist für die Entwickler schwieriger geworden, da die Testprotokolle manuell überprüft und ausgewertet werden müssen.

Welche technologischen Herausforderungen und welchen Forschungsbedarf müssen Sie als IKT-Dienstleister künftig adressieren?

In der Zukunft wird nicht nur die Anzahl der einzelnen smarten Dinge und Geräte wie Sensoren oder Aktuatoren steigen, sondern auch die Anzahl der smarten Fabriken und Zulieferer. Dies bedeutet, dass die Vernetzung auf einer höheren Organisationsebene immer stärker in den Vordergrund treten wird. Hier entstehen Herausforderungen, die mit kundenspezifischen Individuallösungen nicht bewältigt werden können.

Außerdem wird der effiziente Datenaustausch über die gesamte Fertigungskette, beispielsweise zwischen einem

Zulieferer und einem OEM, an Bedeutung gewinnen. Hierzu müssen die Daten sowohl syntaktisch als auch semantisch interoperabel sein, um solche Vernetzungen generisch und kosteneffizient realisieren zu können. Die Themenkomplexe der semantischen und betrieblichen Interoperabilität werden erst noch an Bedeutung gewinnen. Eine kosteneffiziente technologische Umsetzung stellt eine große Herausforderung dar und muss von IKT-Dienstleistern im Forschungsumfeld oder in Ökosystemen gelöst werden. Solche Szenarien stellen die Dienstleister auch vor Herausforderungen bezüglich der Datensicherheit und Datenhoheit.

Was ist Ihr Ansatz, um die nötige Interoperabilität zu gewährleisten?

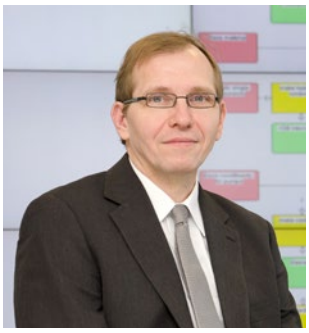
Ein gemeinsames Framework zum Austausch von Daten über Unternehmens- und auch Branchengrenzen hinweg wird aktuell im Rahmen der oneM2M-Initiative[4] standardisiert. Die Idee von oneM2M ist ein Betriebssystem nach dem Marketplace-Prinzip von Android, mit dem Ziel, das Internet der Dinge konzeptionell zu beschreiben. Auf der konzeptionellen und standardisierten Basis wären Anwendungen wie beispielsweise die Steuerung eines Industrieroboters nach dem App-Prinzip in das gesamte Produktionssystem integrierbar. Das oneM2M-Framework versucht, möglichst viele Anwendungsfälle abzudecken und diese auf einer relativ hohen Abstraktionsebene zu beschreiben. Dadurch wird es sehr komplex und insbesondere für kleine und mittlere Unternehmen schwer zugänglich. Es ist zu erwarten, dass sich oneM2M, genauso wie OPC UA[5], langsam durchsetzt. Weitere vergleichbare Ansätze wie Web-of-Things-Ontologien von W3C[6] sind ebenfalls sehr komplex und erfordern einen hohen Einarbeitungsaufwand.

Welche Rahmenbedingungen müssen sich aus Ihrer Sicht am dringendsten verändern?

Das Interesse der Unternehmen liegt momentan nicht auf komplexen Frameworks, sondern auf der Nutzung von Daten. Wer letztendlich über die Daten bestimmt, ist eine offene Frage. Sowohl Zulieferer als auch Hersteller wollen über die Sensor- oder Maschinendaten bestimmen. Rechtlich gesehen, agieren die Unternehmen in einer Grauzone, welche die Nutzung der Daten und somit auch datengetriebene Geschäftsmodelle hemmt. Dienstleistungen wie Analyse und Optimierung würden aber einen erheblichen Mehrwert für produzierende Unternehmen bieten. Die fehlende Regelung über die Bestimmung der Daten erzeugt Unsicherheit aufseiten der Kunden.

4 oneM2M: http://www.onem2m.org.
5 OPC Foundation: http://www.opcfoundation.org.
6 World Wide Web Consortium: http://www.w3.org.

„FÜR BETREIBER VON SMARTEN FABRIKEN IST INTEROPERABILITÄT ENTSCHEIDEND.“



Frank-Walter Jäkel
Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik IPK
Tel.: 030-390 06-174
E-Mail: Frank-Walter.Jaekel@ipk.fraunhofer.de

Herr Jäkel, Sie arbeiten an der Testautomatisierung für Plattformen und Anwendungen im Internet der Dinge. Welche technologischen und wissenschaftlichen Herausforderungen bergen automatisierte Tests?

Die Herausforderungen in der Entwicklung automatisierter Tests ist, dass die Testwerkzeuge sicher einsetzbar und leicht zugänglich sein und sich zugleich einer hohen Akzeptanz erfreuen müssen. Ein Knackpunkt ist auch, dass die Tests vergleichbar sein müssen, um breit genutzt werden zu können. Dabei spielen die Standardisierung der Testziele und der Testprozesse eine wesentliche Rolle. Außerdem müssen die Tests nachvollziehbar sein. Dies gilt vor allem dann, wenn verschiedene Testmethoden unterschiedliche Ergebnisse liefern.

Welche Forschungsfelder sollen in Zukunft im Bereich Testware für das Internet of Things adressiert werden? Welche gibt es insbesondere im industriellen Bereich?

Eine offene wissenschaftliche Fragestellung ist die flexiblere und schnellere Anpassbarkeit der Testwerkzeuge an unterschiedliche Entwicklungen. Weitere Herausforderungen liegen bei der Vernetzung von Planungssystemen und Industrieanlagen in unternehmensübergreifendem Wertschöpfungssystem. Dabei geht es nicht darum, Komponenten reibungslos rein technisch zu integrieren, sondern auch Verträge zwischen den einzelnen Partnern automatisch zu überprüfen. In zunehmend autonomen und teilautonomen Fertigungsnetzen werden die Businessaspekte zu einem wesentlichen Bestandteil der Kommunikation.

Wo liegen die konkreten Vorteile?

Automatisierte Interoperabilitätstests für das Vertragsmanagement zwischen verschiedenen Kooperationspartnern werden die Geschäftsprozesse weiter optimieren. So kann beispielsweise auf einen Wechsel der Partner in einem Wertschöpfungsnetz schneller reagiert werden.

Wird dieses Optimierungspotenzial schon hinreichend gehoben?

Komponentenhersteller und Anbieter der Fertigungsanlagen zeigen momentan noch wenig Interesse an Forschung zur Interoperabilität der Kommunikationsschnittstellen. Sie versprechen sich so einen gewissen Schutz gegenüber der Konkurrenz und eine stärkere Bindung der eigenen Kunden. Für die Betreiber der smarten Fabriken ist die Interoperabilität zwischen Geräten, Anlagen und Kommunikationsprotokollen aber entscheidend.

Welche weiteren künftigen Forschungsthemen neben der Interoperabilität werden Ihrer Meinung nach an Relevanz gewinnen?

In Zukunft werden Transparenz, Monitoring und Fehlerdiagnose als Forschungsthemen eine große Rolle spielen.

„WIR BRAUCHEN NEUE TESTWERKZEUGE FÜR NEUE TECHNOLOGIEN.“

Sascha Hackel
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Tel.: 030-34 63 72 55
E-Mail: sascha.hackel@fokus.fraunhofer.de

Herr Hackel, Sie beschäftigen sich mit Testtechnologien für das Internet der Dinge. Darunter sind solche, die automatisiert prüfen, ob IoT-Kommunikationsprotokolle mit den standardisierten Spezifikationen übereinstimmen. Außerdem schreiben Sie Tests, um IT-Sicherheitslücken in den Implementierungen der IoT-Protokolle zu finden. Was sind für Sie aktuell die größten technologischen und wissenschaftlichen Herausforderungen bei automatisierten Tests?

Die Herausforderungen bei der Automatisierung von Tests für das IoT haben sich dahingehend entwickelt, dass die Tests an sich ständig verändernde, neue Tools angepasst werden müssen. Beispielsweise müssen Testwerkzeuge für neue Technologien wie Prozessorenspeicher oder komplexe Multi-Cloud-Infrastrukturen für Neuentwicklungen geschaffen werden.

Was bedeutet dies konkret?

Momentan ist der manuelle Aufwand sehr hoch, wenn wir auf Basis von Dokumenten, die die Teststandards für die Kommunikationsprotokolle beschreiben, den eigentlichen Quellcode für die automatisierten Tests schreiben. Neue Ansätze zielen also darauf ab, aus vorliegenden Dokumenten heraus die gewünschten Tests möglichst (semi-) automatisiert zu generieren.

Wie ausgereift ist dieses Verfahren bereits?

Mit dem heutigen Stand der Technik ist es äußerst schwierig, aus einem Text mit Standards formale Regeln abzuleiten, die zum gewünschten Ergebnis führen. Die Text-Dokumente sind in natürlicher Sprache gehalten und Sprache ist üblicherweise mehrdeutig. Außerdem sind an einem Standardisierungsprozess verschiedene Stakeholder beteiligt, die oftmals gegensätzliche Interessen vertreten. Ein Standard ist also stets ein Kompromiss, der zwischen verschiedenen Parteien geschlossen wird. Um mehr Spielraum für eigene Entwicklungen zu ermöglichen, werden manche Punkte zum Teil absichtlich vage und nicht eindeutig formuliert. Momentan müssen die Standards dementsprechend intensiv von Testentwicklerinnen und -entwicklern studiert werden, um die Zusammenhänge richtig zu verstehen und anschließend die Testspezifikationen zu erstellen. Diese manuelle Tätigkeit ist sehr fehleranfällig.

Ist die Fehleranfälligkeit der Testspezifikationen unvermeidbar?

Das europäische Institut zur Entwicklung von Standards ETSI[7] stellt meistens auch die Implementierungen der Testspezifikationen bereit, die gemeinsam mit verschiedenen Stakeholdern aus Forschung und Industrie diskutiert werden. So verläuft die Entwicklung der Spezifikationen Hand in Hand mit der Entwicklung der Standards. Es gibt formale Testspezifikationen der IoT-Protokolle MQTT[8] und CoAP[9], die in der ETSI-Arbeitsgruppe MTS TST entwickelt wurden, außerdem wurden Referenzimplementierungen in der Testsprache TTCN-3[10] bei der Eclipse Foundation bereitgestellt. So werden die Standards kontinuierlich auf ihre praktische Relevanz hin überprüft, angepasst und somit Fehleranfälligkeit vorgebeugt.

Welche Forschungsfelder sollen in Zukunft im Bereich Testware für das Internet der Dinge adressiert werden? Welche gibt es insbesondere im industriellen Bereich?

Ich fände es interessant, einen technischen Prozess für neue Kommunikationsprotokolle zu etablieren, die aus formalen Testbeschreibungen heraus automatisiert auf die IT-Sicherheit überprüft werden können. Momentan ist dies nicht möglich, weil heutige Standards keine eindeutige und formalisierbare Beschreibung beinhalten.

Der größte Forschungsbedarf liegt aber beim Management der komplexen Cloud-Anwendungen und insbesondere auf der IoT-Kommunikationsebene: Neue Konzepte für flexible und skalierbare Kommunikationsinfrastrukturen wie Edge- und Fog-Computing bringen neue Herausforderungen mit

7 https://portal.etsi.org/tb.aspx?tbid=97&SubTB=97.
8 Machine-to-machine (M2M)/Internet of Things (MQTT): http://www.mqtt.org.
9 Constrained Application Protocol (CoAP): http://www.coap.technology.
10 Testing and Test Control Notation Version 3 (TTSN-3): http://www.ttcn-3.org.

sich, auch für die Entwickler der automatisierten Tests. Auf der unteren IoT-Kommunikationsebene muss beispielsweise die semantische Interoperabilität beim Austausch der Sensordaten und Geräte automatisch geprüft werden.

Im Internet der Dinge müssen generell neue Konzepte für die Update-Mechanismen sowie für die Nutzung der IoT-Geräte erforscht werden. Besonders wenn ein IoT-Gerät den Hersteller verlässt, müssen sowohl die IT-Sicherheit als auch die Safety der Hardware durch Robustheitstests gewährleistet sein. Daher wird Testware für Software in Verbindung mit Hardware zunehmend wichtiger. So müssen beispielsweise Cyberattacken auf Geräte verhindert werden, die durch das Versenden von Signalen die Batterien angreifen und leerlaufen lassen. Zu dieser Schnittstelle gibt es noch viel Forschungsbedarf.