Agenda: Testautomatisierung für IoT-Plattformen und Anwendungen

Am 10. Oktober 2018 im Veranstaltungszentrum von Fraunhofer FOKUS

Kaiserin-Augusta-Allee 31, 10589 Berlin

Uhrzeit	Thema	
10:00 - 10:05	**Dr. Stefan Afting** *BMWi*	Begrüßung
10:05 - 10:30	**Dr. Steffen Everst** BOSCH SI	Keynote: The Rise of Open Source in the Manufacturing Industry
10:30 - 11:00	**Axel Rennoch, Michael Wagner** *Fraunhofer FOKUS* **Dr. Inessa Seifert** *iit*	Vorstellung des Projekts IoT-T: thematische Einführung in den Workshop, Umfrageergebnisse ca. 10‘ Diskussion

Schlanke, leistungsfähige und energieeffiziente Kommunikationsprotokolle bilden die erforderliche Basis für das Internet of Things. Aus der ursprünglichen Vielfalt an herstellerspezifischen Kommunikationsprotokollen haben sich in den letzten Jahren drei wesentliche IoT-Protokolle auf dem Markt als de-facto Standards etabliert: MQTT – MQ Telemetry Transport, CoAP - Constrained Application Protocol und OPC UA - Open Platform Communications – eine umfangreiche Kommunikationsarchitektur für IoT-Anwendungen im produzierendem Gewerbe. Trotz der inzwischen vereinheitlichen Spezifikation dieser Protokolle existieren zahlreiche Implementierungen, die oft miteinander inkompatibel sind. Darüber hinaus werden neben den rein funktionalen Anforderungen an die verschiedenen IoT-Anwendungen - sei es SmartHome, SmartBuilding oder SmartCities – auch Anforderungen an IT-Sicherheit sowie Performance der cloudbasierten IoT-Plattformen immer wichtiger. Um die Vision einer reibungslosen und sicheren Integration von verschiedenen Implementierungen der Protokolle und Kommunikationsschnittstellen zu ermöglichen, setzten die Partner des IoT-T Konsortiums folgende Anwendungsbeispiele und Testwerkzeuge um:
Die Anwendersicht wird im ersten Use Case „Testing Industrial IoT“ von Audi repräsentiert. Der Use Case adressiert die sichere Integration der Komponenten der Zulieferer in die laufende Produktion via Plug & Produce. Der zweite Use-Case „Cloudbasierte IoT-Plattform und Cyber Security“ adressiert eine sichere Integration von IoT-Anwendungen in cloudbasierte Infrastrukturen des IKT-Dienstleisters relayr.
DEKRA baute ein Testlabor auf, in welchem die Zertifizierung der Mindestanforderungen an IoT-Anwendungen möglich wird. Im Testlabor können nun die Kommunikationsprotokolle auf die Konformität mit Spezifikationen sowie auf IT-Sicherheit nach den Security by Design-Prinzipien zertifiziert werden. Für DEKRA steht die Standardisierung der Prüfziele nach dem zentralen IT-Sicherheitsstandard IEC 62443 im Vordergrund, um branchenübergreifende und international anerkannte Zertifizierung der IoT-Anwendungen zu erreichen.
Die Forschungs- und Entwicklungspartner Fraunhofer IPK und Fraunhofer FOKUS waren gemeinsam mit dem Anwendungspartner relayr an der Entwicklung der Testsuites für MQTT, CoAP und OPC UA beteiligt, um die verschiedenen Implementierungen einerseits auf die Konformität mit der Spezifikation und anderseits auf die IT-Sicherheit automatisiert prüfen zu können.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

11:00 - 11:30	**Jens Stomber** *Digitale Prozessplanung Ingolstadt* *AUDI AG*	Industrial IoT-Anwendungen am Beispiel Automotive ca. 10‘ Diskussion

Insbesondere in der Produktion ist die Digitalisierung für Automobilhersteller kein Neuland. Dennoch halten aktuell unter dem Stichwort „Industrie 4.0“ und „Industrial Internet“ Technologien Einzug in die Fabriken, die einerseits neue Anwendungsfelder begründen und andererseits die Architektur etablierter Lösungen neu definieren. Das Rückgrat der Industrie 4.0 bildet dabei das Industrielle Internet der Dinge (Industrial IoT oder IIoT).
Unter diesem Schlagwort sollen in den kommenden Jahren internetzentrische Kommunikationsprotokolle traditionelle Feldbusse ablösen. Doch wie wird sichergestellt, dass die neuen Geräte und Services auch die Anforderungen einer Fabrik der Zukunft erfüllen? Bedeutet die technologische Konvergenz und grenzenlose Konnektivität nicht auch eine größere Angriffsfläche für Cyberbedrohungen?
Standardisierte Testverfahren geben Anwendern aus der Industrie die Möglichkeit, Implementierungen objektiv zu beurteilen, um im Ergebnis ein hohes Qualitäts- und Sicherheitsniveau zu erreichen.

11:30 - 11:40	Kaffeepause	
11:40 - 12:10	**Frank-Walter Jäkel** *Fraunhofer IPK*	Testing APIs *Anforderungen und Lösungen zur Überprüfung von digitalen Schnittstellen in der Fertigung* ca. 10‘ Diskussion

Durch die digitale Transformation ist der Bedarf an einer herstellerübergreifenden Interoperabilität von Schnittstellen und Protokollen gestiegen. Der Vortrag wird sich auf Prüfwerkzeuge konzentrieren, welche die Kompatibilität neuer Maschinen in Bezug auf vorhandene oder geplante IT-Infrastrukturen der Fertigung beziehen. Anwendungen wie die Betriebsdatenerfassung (BDE) erwarten spezifische IT-Schnittstellen von Anlagen, Geräten und Sensoren. Der Lösungsansatz basiert auf OPC-UA als zentrale Kommunikationsinfrastruktur für Industrie 4.0 und demonstriert typische Einsatzfälle für die Testwerkzeuge.

12:10 - 12:40	**Jackson Bond** *relayr*	Cloudbasierte IoT-Plattform und Cyber Security ca. 10‘ Diskussion

Studien (z.B. Gartner) prognostizieren, dass bis 2020 über 60% der Unternehmen IoT-Anwendungen einsetzten werden. Dies bedeutet jedoch auch, dass die Angriffsfläche für Industriespionage, Erpressung und völlig neue Formen von Cyber-Bedrohungen enorm zunehmen wird.
Solche Bedrohungsszenarien wecken in der Industrie massive Bedenken gegenüber der Digitalisierung und bremsen das Innovationspotential aus.
Der Erfolg von IoT-Anwendungen auf dem Markt hängt daher maßgeblich von der Sicherheit und der nahtlosen Integrations- und Kommunikationsfähigkeit der IoT-Geräte und –Anwendungen ab. Dazu bedarf es innovativer cloudbasierter Lösungen für die Verwaltung und Steuerung der IoT-Geräte. Ebenso werden komfortable Werkzeuge zum Testen der Absicherung gegen Cyberangriffe sowie zum Erreichen einer transparenten Qualitätsbewertung der IoT-Softwarekomponenten verschiedener Hersteller benötigt.
Um dies zu veranschaulichen, wird der Vortrag zunächst die aktuelle Marktlage und die Herausforderungen durch das IoT beleuchten. Darauf aufbauend wird der Kundenbedarf und die resultierende Notwendigkeit für die Absicherung der Bedrohungsszenarien aus der Sicht von IoT-Anbietern skizziert.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

12:40 - 13:40	**Mittagspause**	
13:40 - 14:10	**André Wardaschka** *DEKRA*	Testlabor für IoT Security – die Standard-Challenge ca. 10‘ Diskussion

Standards bilden die Grundlage für Konformitätsbewertungen. Im Bereich IoT-Security sind die Standardisierungsaktivitäten jedoch weder auf nationaler noch auf internationaler Ebene abgeschlossen. Der Vortrag beleuchtet daher die derzeitige Standardisierungslandschaft und erläutert die Wahl, Anwendung und Grenzen der verwendeten Standardserie IEC 62443 als Grundlage für Security-Prüfungen von IoT-Produkten. Dabei werden neben den technischen Aspekten auch die Bedeutung von nicht-funktionalen Anforderungen wie beispielsweise die Performance und Skalierbarkeit bei der Produktentwicklung erläutert.

14:10 - 14:40	**Axel Rennoch, Sascha Hackel** *Fraunhofer FOKUS*	Verlobung von Standardisierung und Open-Source-Software mit IoT-Testware ca. 10‘ Diskussion

Am Beispiel der Standardisierungsvorhaben in der von uns gegründeten Working Group MTS TST beim European Telecommunications Standards Institute (ETSI) stellen wir vor, wie wichtig die Standardisierung von Tests für IoT ist und wie dies mit Open-Source-Software vereinbar ist. Des Weiteren werden Veränderungen im aktuellen Ökosystem durch Standardisierung von Testzielen für die Testkataloge bei ETSI aufgezeigt und wir wagen einen Blick in die Zukunft.
Dabei leiten uns folgende Fragen:
An welchen Schnittstellen gibt es Optimierungspotentiale? Welche neuen Verfahren und Technologien fehlen noch?

14:40 - 15:00	Kaffeepause	
15:00 - 16:00	**Dr. Inessa Seifert** **Petra Weiler** **Tilman Liebchen** *iit*	Open-World-Café

Eine Auswahl an Themen wird von den Moderatorinnen und Moderatoren der Begleitforschung in kleinen Gruppen diskutiert.

16:00 - 16:30	**Dr. Inessa Seifert** **Petra Weiler** **Tilman Liebchen** *iit*	Vorstellung der Ergebnisse der Open-World-Café
16:30	Ende der Veranstaltung	

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages