# Testautomatisierung für das Internet der Dinge

Workshop „Sichere Plattformarchitekturen“

im Programm „Smart Service Welt“

Berlin, 15.02.2017

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

# Agenda

- IoT Testobjekte, -ziele und –konfigurationen
- Testware
  - Werkzeugkasten
  - TTCN-3
    - Konzept
    - Einsatz für IoT
  - Security Werkzeuge
    - Fuzzing
- IoT-T Testlab

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

# IoT

## Testobjekte und -ziele

- IoT **Devices**,
  - Mikrocontroller (**MCU**),
  - Gateways (Bosch XDK, IoT starterkits)

- IoT **Plattformen**
  - RIOT, relayr, Thread, mbed…
  - service layer (oneM2M)

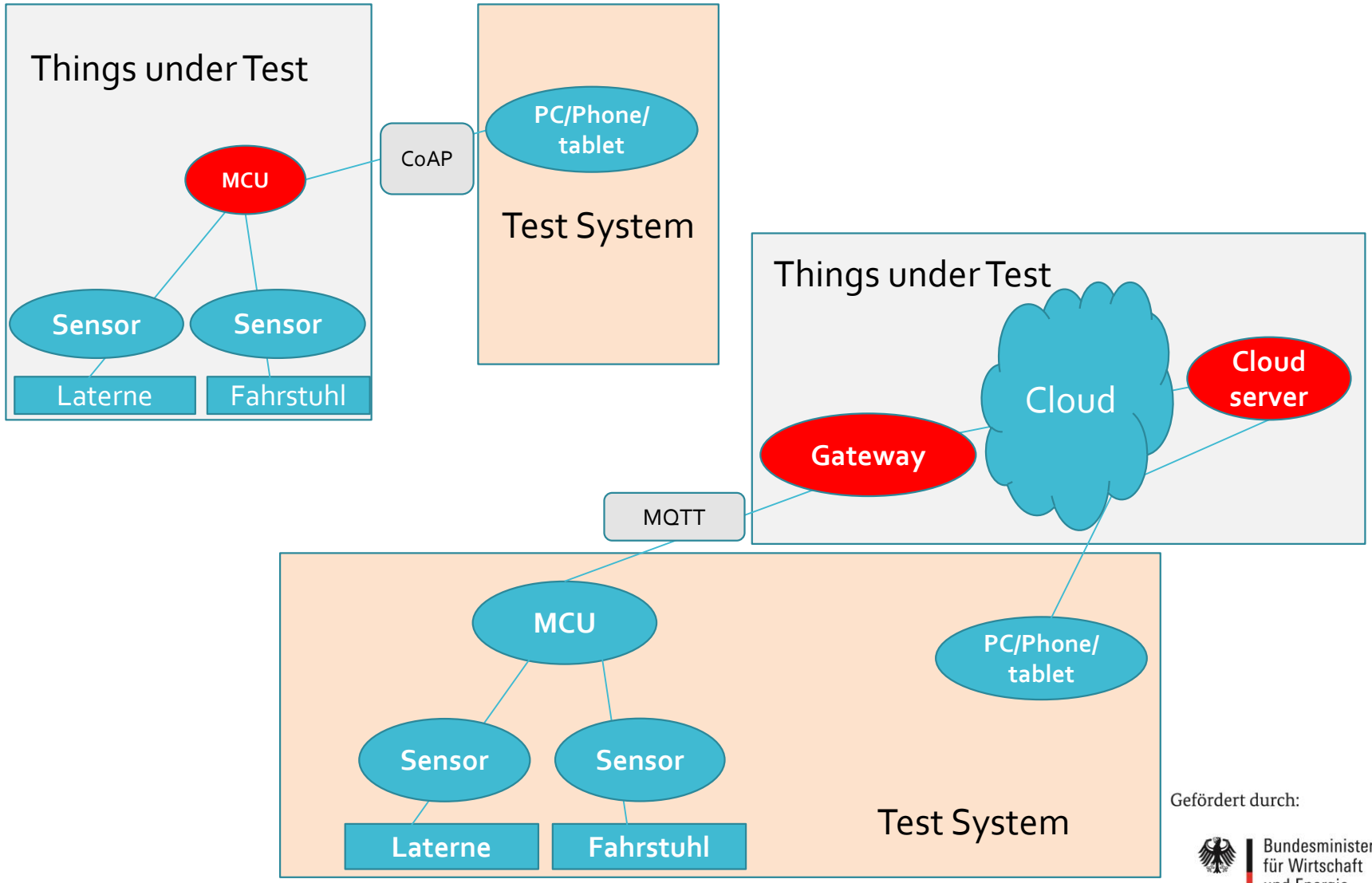
- IoT **Protokolle**
  - Constrained Application Protocol (**CoAP**)
  - MQ Telemetry Transport (**MQTT**)

| oneM2M | |
|---|---|
| HTTP, AMQP, MQTT | CoAP |
| TCP | UDP |
| IPv4, IPv6, 6LoWPAN | |
| MAC, IEEE 802.15.4 | **LPWAN** |
| PHY | **LoRa** |

- Black box mit **Vielzahl unterschiedlichster Schnittstellen**
- **Vielfache Konfigurationen**, verteiltes Testen,
- Funktionalität/**Konformität**, **Interoperabilität**, Robustheit/**Last**, **Sicherheit**

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

# Testkonfigura-tionen (Beispiele)




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

# Testware (Test Methoden und Werkzeuge)

- **Werkzeugkasten** *(vorhandene Mittel)*
  - Protokoll Tester/Monitor: z.B. Eclipse Titan, Wireshark, etc.
  - Devices (Hardware für physikalische Luft-Schittstellen): z.B. RFID kit, Bluetooth test device, …
  - GUI tester: z.B. Selenium
  - Web services Tester, z.B. soapUI
  - Testserver/clients (z.B. coap.me, lokal oder im Internet)
  - Weitere Test Umgebungen & Dienste: z.B. Firebase Test Lab für Android Apps
- Öffentliche **Testsuites** *(zu entwickeln)*
  - Unter Verwendung einer Standardisierten Notation
  - Abstrakt und plattform-unabhängig

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

# Testing and Test Control Notation (TTCN-3)

- Testbeschreibungen in international **standardisierter** Notation
  - European Telecommunication Standardisation Institute (ETSI)
  - International Telecommunication Union (ITU-T)
- Z.B. Mobilfunk (LTE) **Zertifizierung**, Automotive, e-Health

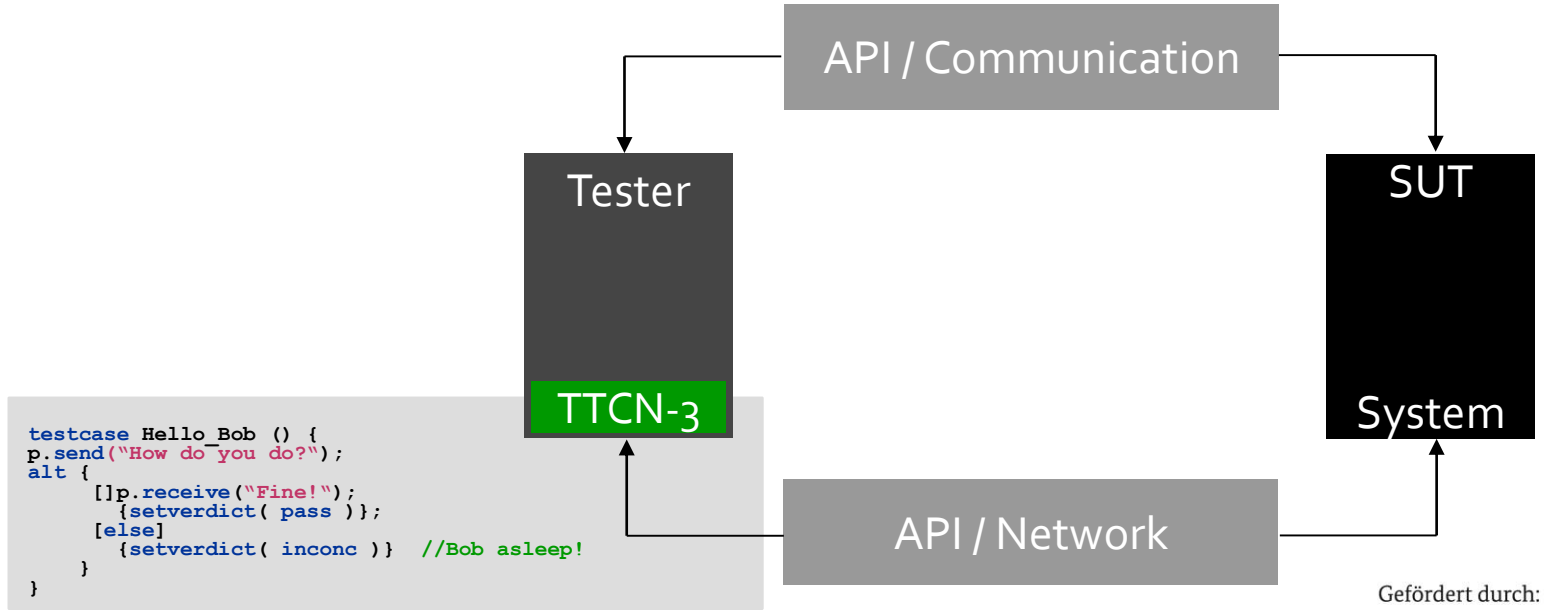
```
testcase Hello_Bob () {
p.send("How do you do?");
alt {
    []p.receive("Fine!");
          {setverdict( pass )};
    [else]
          {setverdict( inconc )}   //Bob asleep!
}
}
```

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

IoT

# Testing and Test Control Notation (TTCN-3)

- **Verteiltes Testen, plattformunabhängig**
- **Automatisierte** Ausführung (TTCN-3 -> Java/C++)
- Einbinden von Datentypen (ASN.1, IDL, XML, *JSON*)





Gefördert durch:

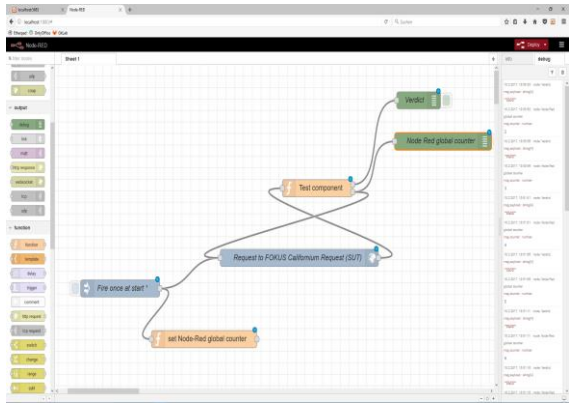
Bundesministerium für Wirtschaft und Energie

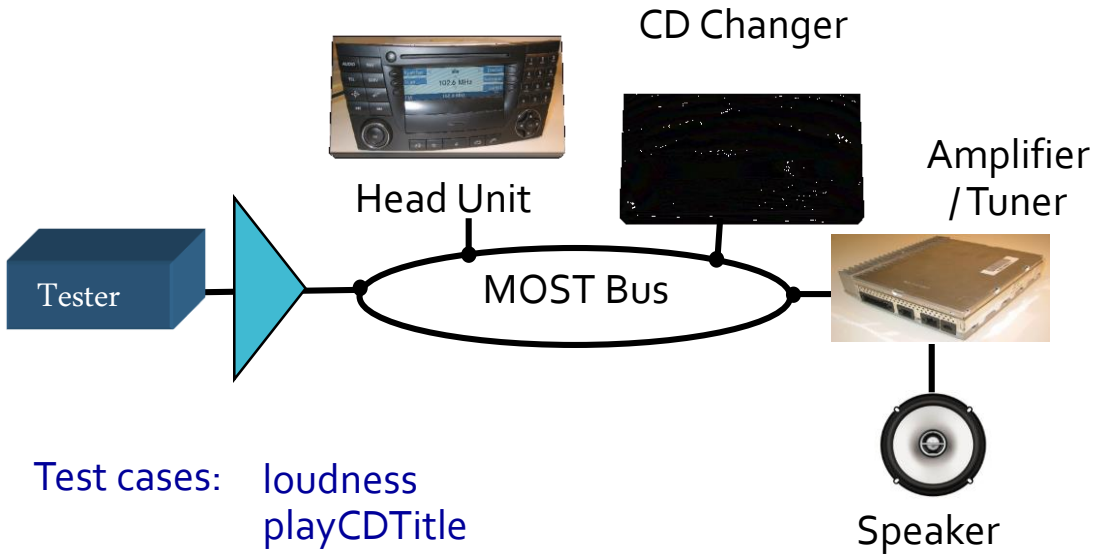
aufgrund eines Beschlusses des Deutschen Bundestages


DEKRA relayr bring things to life Fraunhofer IPK Fraunhofer FOKUS

# TTCN-3 für IoT

- Testwerkzeug/Plattform zur Einbindung **unterschiedlichster Protokolle** und **Schnittstellen**
- Steuerung von ***realen*** und ***virtuellen*** **Geräten** (spezielle Hardware-Interfaces, Simulatoren)
- *TTCN-3 „virtualized" (in Planung)*






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

# Testware: Security

- Vulnerability **Scanner** *[automatisiertes Aufdecken zur Erkennung von Schwachstellen]*:
  Insbesondere bei **Web-Anwendungen**, zero-day/**fuzzing**, Nutzung von **Datenbanken**, traffic/network **Analyse**, **Programm code** Scanner
- **Penetration** Tester *[Mittel und Methoden der Angreifer: Sichtung-Planung-Auswahl-Durchführung]*, z.B. "SQL injection"
- Intrusion **detection** tools (Angrifferkennung)
- **Last** test/Scalability
- *Weitere Hilfsmittel:*
  *Model-based testing (UML testing profile) und Risiko Modellierung*

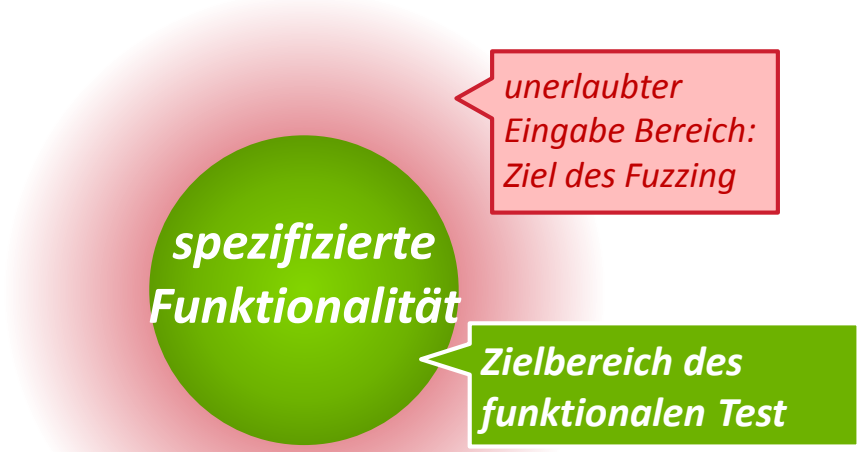
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IoT

# Testware: Security (Fuzzing)

- Fuzzing verwendet ungültiges bzw. unerwartetes Eingaben
  - *Zur Auslösung unerwartetes Verhalten*
  - *Zur Erkennung von Fehler und möglicher Schwachstellen*

- *Fuzzing ermöglicht das Auffinden von 0-Day Schwachstellen*
  - *Programm-Abbruch*
  - *Denial of Service*
  - *Sicherheitslücken*
  - *Leistungsverringerung*




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

DEKRA relayr bring things to life Fraunhofer IPK Fraunhofer FOKUS

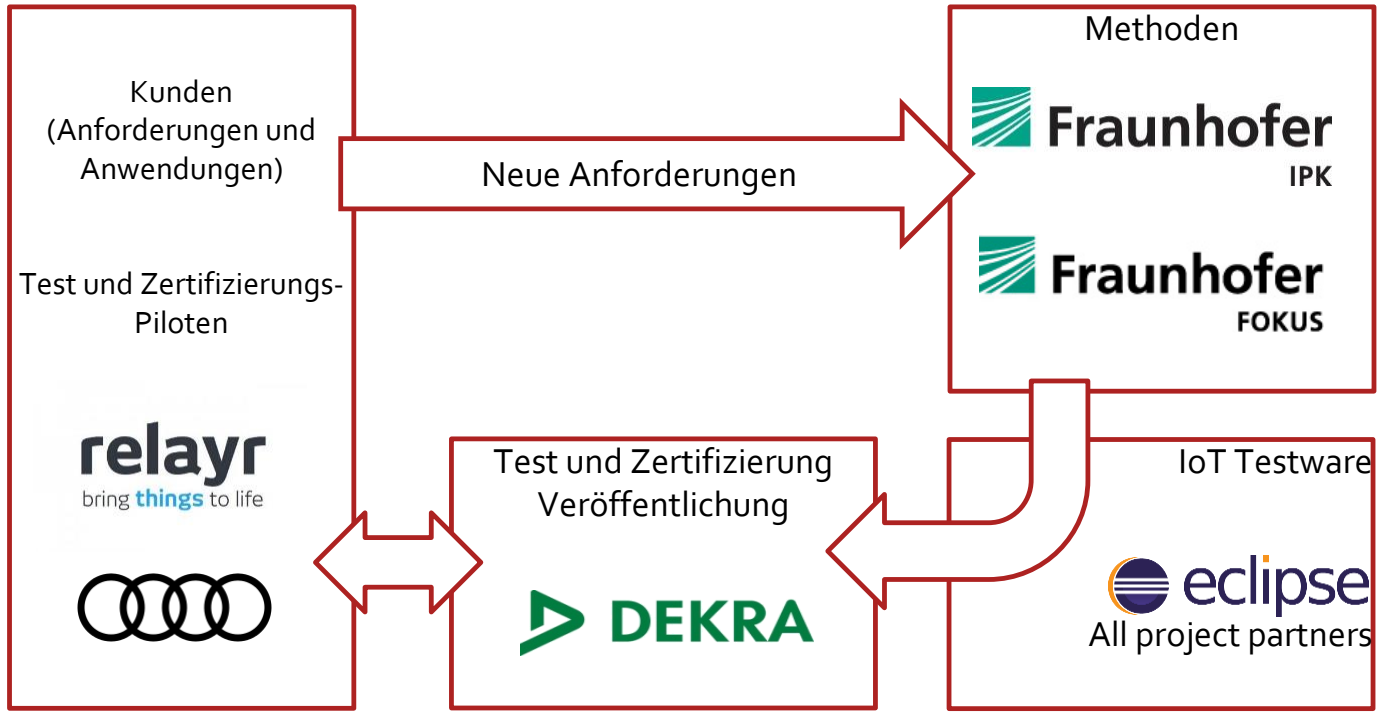
# Testlab (Testen und Zertifizieren)

- Fokus auf **Open source** Werkzeuge (Eclipse)
- Bereithaltung von zahlreichen **Endgerätetypen**
- Definition von **Testsuites** für IoT Protokolle **CoAP** und **MQTT**
- Unterstützung bei der Konfiguration
- „come in and test"
- Remote test service (online)

- Künftige **Zertifizierung**
  - „Leichtgewichtige" Auswahl von Kriterien
  - „Selbstzertifizierung" nach erfolgreichem Test
  - Ggf. Einbeziehung von Betriebssicherheit (Angrifferkennungssystem)

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

# Projekt www.IoT-T.de




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

Vielen Dank für die Aufmerk-samkeit

www.fokus.fraunhofer.de

(System Quality Center)

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages