**kM216 – Notizen und Zusammenfassung**

Inhaltsverzeichnis

[1. IoE 2](#_Toc118883196)

[2. IIoT 3](#_Toc118883197)

[3. Industrie 4.0 3](#_Toc118883198)

[4. Cloud- und Edge Computing 4](#_Toc118883199)

[5. Sensoren und Aktoren 4](#_Toc118883200)

[6. I2C – Inter-Integrated Circuit 5](#_Toc118883201)

[7. MQTT 5](#_Toc118883202)

[8. Funktechnologien 5](#_Toc118883203)

[8.1 Bluetooth 6](#_Toc118883204)

[8.2 Zigbee 6](#_Toc118883205)

[8.3 Z-Wave 6](#_Toc118883206)

[8.4 Wlan 7](#_Toc118883207)

[8.5 Sigfox 7](#_Toc118883208)

[8.6 Narrowband-IoT 8](#_Toc118883209)

[8.7 LoRa – LoRaWAN 8](#_Toc118883210)

[9. Security 8](#_Toc118883211)

[9.1 Firmware 9](#_Toc118883212)

[10. Testing 9](#_Toc118883213)

# IoE

Ein **Ding** muss folgende drei Sachen beinhalten:

* eine zentrale Verarbeitungseinheit (CPU)
* Speicher (RAM)
* Ein- und Ausgabeeinheit(en) (eng. **I**nput/**O**utput, I/O)

**Daten** kann man in eine **Information** umwandeln und davon **Wissen** ableiten.

**IoT:** Daten werde häufig lokal und auch in Echtzeit gespeichert und verarbeitet. Daher ist das Geschehen mit den Daten von durch die Grenzen des Netzwerks und durch die Fähigkeiten der integrierten Geräte begrenzt.

**Big Data:** unendliche Fülle von Informationen welche im Internet durch die wachsende Anzahl verbundener Geräte generiert werden.

Haupteigenschaften von Big Data: **Volumen**, **Vielfalt** und **Geschwindigkeit**.

Volumen: bezeichnet die Menge der transportierten und gespeicherten Daten.

Vielfalt: welchen Typ (Audio, Video, etc.) die Daten haben und wie stark sie sich gleichen.

Geschwindigkeit: wie schnell Daten produziert, empfangen und (vielleicht) verarbeitet werden

**Das Internet of Everything (IoE)**

IoE die **Verbindungen zwischen Menschen, Prozessen, Daten und Dingen herstellt.** Diese **vier Säulen** werden zusammengebracht, um Synergien zu nutzen, wodurch jede Säule die Wirkung und Fähigkeiten der anderen verstärkt. Das wahre Potential des IoE kann nur realisiert werden, wenn alle Teile reibungslos zusammenarbeiten.

Dinge und Menschen sammeln Daten, stellen diese den vernetzten Säulen über die Infrastruktur des IoE zur Verfügung und bereiten sie mittels optimierter Prozesse auf, um fundierte Entscheidungen zu treffen und umzusetzen, welche innerhalb eines Wirtschafts- oder Sozialsystems einen (Mehr-)Wert generieren.

**Das Internet of Things (IoT)**

**Das IoT besteht aus physischen Objekten, die selbst über das Internet kommunizieren und dort Daten über ihren eigenen Zustand oder Umgebungsparameter austauschen, um Erkenntnisse zu gewinnen und Abläufe zu steuern.**

**Die 4 Säulen des IoE: Kernkomponenten IoT:**

* Physische Objekte
* People
* Process
* Data
* Things
* Konnektivität
* Sensorik
* Infrastruktur

# IIoT

**Industrielle Internet der Dinge (IIoT)**

IIoT-Technologien nur in industriellen Umgebungen von Spezialisten in einem industriellen Bereich eingesetzt. Entsprechend geringer fällt die Marktorientierung aus. Zu den IIoT-Haupteinsatzbereichen zählen Kraftwerke, Öl- und Gasraffinerien sowie Produktionsanlagen.

Es ist eine Unterkategorie des IoT. IoT und IIoT verfolgen unterschiedliche Ziele.

Bei IoT-Geräten handelt es sich üblicherweise um Geräte des täglichen Lebens.

Bei IIoT-Geräten handelt es sich um die Daten von Maschinen.

**IoT-Geräte** und -Technologie ausfallen, bringt dies aufgrund ihrer Verwendung in kleinem Umfang ein relativ geringes Risiko mit sich.

Ausfall von **IIoT-Geräten** und -Technologie gefährlicher sein, da IIoT-Technologie via Netzwerk verbunden ist und beim Ausfall schwerer Maschinen lebensbedrohliche Situationen erzeugen kann.

In der Regel müssen **IoT-Geräte** nicht mit Altsystemen kompatibel sein. Im Gegensatz dazu müssen **IIoT-Geräte** tendenziell Kompatibilität mit verschiedenen Altsystem-Geräten und -Maschinen im Industrieanlagenumfeld aufweisen.

**IoT-Geräte** in alltäglichen Umgebungen und werden entsprechend gestaltet, um normalen Temperaturen und anderen Umweltbelastungen zu widerstehen. Daher gestalten **IIoT-Gerät**-Hersteller ihre Geräte üblicherweise in einer Weise, die Feuchtigkeit, Funkstörungen und extremen Temperaturen standhalten kann, um die Übermittlung einheitlicher Ergebnisse zu gewährleisten.

**Ziel vom IoT:**

Beim **IoT** (Internet of Things) werden Gegenstände intelligent gemacht.

**Ziel vom IoE:**

Beim **IoE** (Internet of Everything) werden die intelligenten **Dinge** mit **Prozessen**, **Daten** und **Menschen** verknüpft.

# Industrie 4.0

**Industrie 4.0:**

1.Industrielle Revolution:

* Kohlebergbau
* Dampfmaschine 1769 erfunden von James Watt
* War Motor für den Antrieb von Maschinen

2. Industrielle Revolution:

* Ende des 19. Jahrhunderts
* Verwendung von Öl und Elektrizität
* Produktionsmittel wurden dadurch modernisiert
* Automobil- und Chemieindustrie hat davon stark profitiert
* Produktionsmaschinen wurden elektrisch
* Fliessbandarbeit, wodurch selbst ungelernte Arbeiter produktiv und effizient arbeiten
* **Massenproduktion identischer Produkte.**

3. Industrielle Revolution:

* Mitte des 20. Jahrhunderts
* Aufkommen von **Elektronik, Telekommunikation und Computern**
* **Implementierung wichtiger Automatisierungen**, die den Arbeitern die komplexesten Aufgaben abnehmen konnten.
* **Mobilität**
* **Beginn der Robotik, der Flexibilität der Produktionswerkzeuge und der Massenproduktion**.

4. Industrielle Revolution:

* Produktanpassung
* Verbraucher will ein **vollständig personalisiertes Produkt**
* Industrie 4.0 hat sich verpflichtet, diese Nachfrage nach einzigartigen und personalisierten Produkten bei gleich bleibenden Kosten zu befriedigen, trotz des damit verbundenen geringen Produktionsvolumen.

# Cloud- und Edge Computing

**Cloud Computing**: Die Datenverarbeitung findet in einer Cloud statt. Cloud Computing ist ideal, um große Datenmengen zu speichern und zu verarbeiten, etwa um KI-Modelle zu trainieren.

**Edge Computing:** Wenn die Felddaten nicht direkt in die Cloud übertragen werden, sondern wenn sogenannten Edge Devices – Rechner, welche nur die relevanten Ergebnisse an die Cloud übermitteln. Der Ansatz spart teure Datenübertragung zur Cloud, ermöglicht Echtzeitdienste und führt zu mehr Datensicherheit und Zuverlässigkeit.

# Sensoren und Aktoren

**Sensoren:** ist ein technisches Bauteil, das bestimmte physikalische oder chemische Eigenschaften (Wärmemenge, Temperatur, Feuchtigkeit, Druck, pH-Wert, Ionenstärke, elektrochemisches Potential) **erfassen kann.**

**Aktoren:** Aktoren sind **Antriebselemente,** die elektrische Signale und Strom in **mechanische Bewegung** oder Licht transformieren. Sie stellen das Gegenteil zu Sensoren dar, die auf mechanische Bewegung mit elektrischen Impulsen reagieren. Da diese Antriebe heute praktisch in fast allen Bereichen zur Anwendung kommen, sind sie ein fester Bestandteil der modernen Technik. Der Klassiker ist der Elektromotor, ein Servo im Modellbau oder die höherwertigen Schrittmotoren. Aktoren benötigen meist noch eine Steuereinheit, welche die Ströme und Kräfte gezielt ansteuern kann.

# I2C – Inter-Integrated Circuit

Der I²C-Bus ist als Zweidrahtverbindung zwischen einem Master (Controller) und an ihn angeschlossene Sensoren oder IC-Bausteine (Slaves) für kurze Distanzen konzipiert worden. An einer Kommunikation können auch mehrere Master und bis zu 128 Slaves beteiligt sein. Die beiden dazu notwendigen Datenleitungen, neben den Versorgungsspannungsleitungen, bezeichnen wir mit SDA (Datenleitung) und SCL (Taktleitung); SDA und SCL bilden den Datenbus. Sensoren verwenden das I2C-Protokoll.

SDA (**S**erial **DA**ta Line: serielle Datenleitung) und SCL (**S**erial **Clock** Line: serielle Taktleitung)

# MQTT

MQTT (**M**essage **Q**ueue **T**elemetry **T**ransport) ist ein schlankes Protokoll für die Kommunikation zwischen verschiedenen Geräten (M2M – machine-to-machine). legt der Struktur keinerlei Beschränkungen beim Code oder einem Datenbankschema auf. Die einzige Bedingung ist dass jedes Datenpaket eine Information zur Identifikation beinhalten muss. Diese Identifikationsinformation heisst Topic Name. Das MQTT Protokoll benötigt einen Datenbroker. Dieses ist die zentrale Idee dieser Technologie. Die zentrale Stelle des Protokolls ist der MQTT-Server oder Broker der Zugriff auf die Clients, die entweder als publisher (sendet Daten) und den subscriber (abonniert Daten) besitzt. Alle Geräte senden ihre Daten nur zu diesem Broker und erhalten ihre Informationen auch nur von ihm. sendet der Broker es zu allen Geräten in dem Netzwerk, die es abonniert haben. Wenn ein Gerät etwas von dem Broker möchte, muss er das entsprechende Topic abonnieren. Nach dem Abonnement eines Topics braucht man nichts mehr zu tun.

Ports: 8883, 1883 🡪endet meistens mit 83

Netzwerkprotokoll: TCP

# Funktechnologien

Durch die Nutzung von Funktechnologien entfällt bei den IoT-Sensoren der Kosten- und Zeitaufwand für die Verkabelung und die IoT-Sensoren können an Standorten ohne Zugang zum Stromnetz verbaut und über eine Batterie mit Strom versorgt werden. Ausserdem muss die zur Datenübertragung genutzte Funktechnologie einen geringen Energieverbrauch aufweisen, damit die batteriebetriebenen IoT-Sensoren eine möglichst lange Batterielaufzeit haben. Anforderungen: hohe Reichweite, gute Netzabdeckung und starke Durchdringung von Objekten. Bei IoT-Lösungen im Consumer-Bereich werden meistens Funktechnologien, wie z.B. WLAN, Bluetooth oder ZigBee eingesetzt. **L**ow **P**ower **W**ide **A**rea **N**etwork (LPWAN) stammen. LPWAN-Funktechnologien zeichnen sich durch geringe Anschaffungs- und Betriebskosten aus, haben einen geringen Energieverbrauch, eine gute Durchdringung von Objekten und können Datenpakete mit einer geringen Datenraten über mehrere Kilometer übertragen, sollte aber allerdings nicht für zeitkritische Anwendungen genutzt werden. Die bekanntesten LPWAN-Funktechnologien sind [LoRaWAN](file:////tag-2/funktechnologien-und-deren-einsatzgebiet/lora-lorawan), Sigfox und [NB-IoT](file:////tag-2/funktechnologien-und-deren-einsatzgebiet/narrowband-iot).

## Bluetooth

Bluetooth ist ein Funkstandard, um auf kurze Distanzen Daten, Musik, Videos oder Bilder zu übertragen. Somit können zwei gekoppelte Geräte miteinander kommunizieren, ohne dass zwischen ihnen eine Kabelverbindung besteht. Für die Funkverbindung nutzt Bluetooth das **ISM-Band** (Industrial, Scientific and Medical). Frequenbereich 2.4 GHz wie Wlan. Bluetooth führt ein Frequenz-Hopping durch. Das bedeutet, dass der Sender und der Empfänger nur für den Bruchteil einer Sekunde auf einen Kanal Daten austauschen und dann gemeinsam auf einen anderen Kanal wechseln. Funkreichweite: 10 – 20 Meter theoretisch bis zu 100 Meter möglic

## Zigbee

ZigBee ist ein bei der Heimautomation verbreitetes Kommunikationsprotokoll. Es vernetzt LEDs und viele weitere Produkte im Smart Home herstellerübergreifend. Das ZigBee-Protokoll regelt, wie Geräte im vernetzten Heim miteinander kommunizieren und Signale übertragen. Funkreichweite: 10 – 20 Meter theoretisch bis zu 100 Meter möglich. Die maximal erzielbare Datenübertragungsrate liegt bei 250 Kilobit pro Sekunde (kBit/s). Sie können ZigBee für alle Arten von Wohnräumen, Häusern und Gewerberäumen verwenden. ZigBee ist ein vielseitiges, energieeffizientes Heimvernetzungs-Funkprotokoll, das für smarte Gebäude, Smart-Home-Lösungen, Embedded-Geräte und das Internet der Dinge (IoT) ausgelegt ist. Übertragung von geringen Datenmengen und im Hinblick auf einen minimalen Energieverbrauch. Hat eine leichte Installation

## Z-Wave

Drahtloser Funkstandart, welcher für die Heimautomatisierung und angrenzende Aussenanlagen entwickelt und für Smart-Home-Anwendungen weltweit lizenziert wurde. Diese Funkkommunikation ist auf geringen Energieverbrauch und hohe Kommunikationssicherheit optimiert. Z-Wave-Geräte können auch zusammen funktionieren wenn sie nicht vom gleichen Hersteller sind. Somit ist es möglich, Geräte unterschiedlicher Hersteller und Anwendungsbereiche in einem gemeinsamen Funknetz zu betreiben. Z-Wave-Geräte können durch Batterien oder Netzspannung versorgt werden. Innerhalb von Gebäuden können einzelne Geräte über eine Entfernung von bis zu 25 Metern miteinander kommunizieren, im Freien sind bis zu 100 Meter möglich. Ein Vorteil dabei sind die 868 MHz (868,40 MHz, 868,42 MHz, 869,85 MHz) Funkwellen, da sie Wände besonders gut durchdringen können.

**Funkreichweite:** innerhalb eines Gebäudes bis zu 25 Meter und im Freien bis zu 100 Meter. F

Die Funkwellen können Wände besonders gut durchdringen.

Z-Wave Plus ist eine Erweiterung Je nach Produkt geht es dabei z. B. um längere Batterielebensdauer, schnelleren Betrieb, grössere Abdeckung der Reichweite und/oder einfacherer Geräteinstallation. Z-Wave Plus-Geräte sind kompatibel mit den Geräten der klassischen Z-Wave-Generation.

## Wlan

Wireless Local Area Network (kurz Wireless LAN oder W-LAN, meist WLAN oder drahtloses lokales Netzwerk) bezeichnet ein lokales Funknetz, wobei meist ein Standard der IEEE-802.11 gemeint ist. WLAN bezeichnet das Funknetzwerk, Wi-Fi hingegen die Zertifizierung durch die Wi-Fi Alliance anhand des IEEE-802.11-Standards. Da WLAN auf der Sicherungsschicht (Schicht 2 im OSI-Modell) dieselbe Adressierung wie Ethernet verwendet, kann über einen Wireless Access Point mit Ethernet-Anschluss leicht eine Verbindung zu kabelgebundenen Netzen hergestellt werden.

Je höher die Frequenz eines drahtlosen Signals ist, desto kürzer seine Reichweite. So decken 2,4 GHz Netzwerke eine wesentlich grössere Reichweite ab als 5 GHz Wireless-Netzwerke. Insbesondere durchdringen die höheren Signale von 5 GHz-Netzwerken, feste Gegenstände nicht so gut, wie 2,4-GHz-Signale.

Im **Ad-hoc-Modus** ist keine Station besonders ausgezeichnet, sondern alle sind gleichwertig. Ad-hoc-Netze lassen sich schnell und ohne grossen Aufwand aufbauen.

## Sigfox

gleichnamiges, proprietäres Funknetzwerk, das Anwender gegen eine Gebühr nutzen können, um kleine Datenpakete zu übertragen. Durch die verwendete Modulationstechnik kann Sigfox Daten über eine grosse Reichweite (bis 40 km in ländlichen Gebieten) senden und hat eine gute Gebäudedurchdringung. Dabei verbraucht Sigfox nur wenig Energie, was in einer lange Batterielaufzeit der Endgeräte resultiert. Sigfox pro Tag maximal 140 Datenpakete übertragen werden und ein Datenpaket kann maximal 12 Byte gross sein. Durch diese Einschränkungen eignet sich Sigfox für Anwendungen, die in grossen Zeitintervallen (grösser 10 Minuten) Datenpakete senden und nur kleine Datenpakete übertragen müssen. Die Endgeräte können bidirektonal kommunizieren. Die Datenpakete werden von der Basisstation an die Sigfox Cloud gesendet. In der Sigfox Cloud werden die Authentizität und Integrität der Datenübertragung sichergestellt. Ausserdem werden die empfangenen Daten in ein lesbares Format umgewandelt und in einer Datenbank in der Sigfox Cloud gespeichert. Es werden Schnittstellen (z.B. MQTT, HTTP) bereitgestellt, um die Daten weiterzuleiten. Ein Endgerät besitzt einen einzigartigen Schlüssel, mit dem es sich gegenüber der Sigfox Cloud authentifizieren kann und die Integrität des gesendeten Datenpakets gewährleistet wird. Die Datenpakete werden mit Sigfox standardmässig nicht-verschlüsselt übertragen.

## Narrowband-IoT

**N**arrow**b**and-**IoT** (**NB-IoT**) ist eine Erweiterung zum LTE-Mobilfunkstandard und wird von Telekommunikationsanbietern bereitgestellt. Die Anwender können NB-IoT durch die Zahlung einer Gebühr nutzen, um Datenpakete zu übertragen. Mit den niedrigen Frequenzbändern B8 und B20 wird eine gute Gebäudedurchdringung und hohe Reichweite durch die langwelligen Funksignale erreicht. können beliebig oft Datenpakete übertragen werden und bei Funkstörungen können Datenpakete wiederholt gesendet werden. 🡪keine Beschränkung der Sendezeit. n Endgerät ist mit einer SIM-Karte von einem Telekommunikationsanbieter ausgestattet. NB-IoT verfügt über umfangreiche Sicherheitsmechanismen. gesendeten Datenpakete verschlüsselt, um ein nicht-autorisiertes Auslesen und Manipulieren der Daten zu verhindern (Integrität). Allerdings ist der Energieverbrauch des Endgeräts durch das Verschlüsseln der Daten höher und die Batterielaufzeit dadurch geringer.

## LoRa – LoRaWAN

**L**ong **R**ange **W**ide **A**rea **N**etwork (LoRaWAN) ist ein Low-Power-Wireless-Netzprotokoll auf der Ebene der Vermittlungsschicht. Sie sind frei verfügbar und Software-Grundmodule sind als Open-Source-Software verfügbar. LoRaWAN nutzt das proprietäre, patentierte, leitungslose „LoRa“-Übertragungsverfahren auf der Bitübertragungsschicht. Damit sich die Kommunikationspartner in umfangreichen LoRaWAN-Netzwerken nicht gegenseitig stören, werden die Datenpakete pseudozufällig auf unterschiedlichen Kanälen gesendet. Mit LoRaWAN können private Netzwerke aufgebaut werden. Hierbei liegt die Verantwortung für den Aufbau und Betrieb der Gateways beim Anwender. Dadurch besteht keine Abhängigkeit von kommerziellen Anbietern. Der Netzwerkserver und Anwendungsserver können vom Anwender betrieben werden oder es können die Dienst von Anbietern wie The Thing Network oder Loriot genutzt werden.

# Security

Netzwerk muss geschützt werden. Angriffe finden über das Netzwerk statt. Sicherheit 🡪In dem man Netzwerke voneinander trennt. Die IoT Device sollen in einem eigenen WLAN operieren und keinen Zugriff auf andere Netzwerke haben. VLANs (**V**irtual **L**ocal **A**rea **N**etworks) unterteilen ein bestehendes einzelnes physisches Netzwerk in mehrere logische Netzwerke. Eine Kommunikation zwischen zwei unterschiedlichen VLANs ist nur über einen Router möglich, der an beide VLANs angeschlossen ist. Die Firewall ist so das Herzstück eines Netzwerkes. Überwachung von den Aktivitäten der angeschlossen Geräten am Netzwerk.

**Personendaten**

* alle Angaben die sich auf eine bestimmte oder bestimmbare Person beziehen

**Besonders schützenswete Personendaten**

* Religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten
* Gesundheit, Intimsphäre oder Rassenzugehörigkeit
* Massnahmen der sozialen Hilfe
* administrative oder strafrechtliche Verfolgungen und Sanktionen

**Persönlichkeitsprofile**

* Eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt (DSG, Art. 3

Die IT-Grundschutz-Bausteine sind in zehn unterschiedliche Schichten aufgeteilt und reichen thematisch von Anwendungen (APP) über Industrielle IT (IND) bis hin zu Sicherheitsmanagement (ISMS).

## Firmware

Firmware beschreibt Software, die in elektronische Geräte fest implementiert ist. Sie ist im Gegensatz zu herkömmlicher Software mit der Hardware unzertrennlich verankert, beide sind also aufeinander angewiesen.

Updates:

* Schneller
* Änderung des GUI
* Fehlerbehebung
* Neue Fähigkeiten
* Behebung von Sicherheitslücken

# Testing

IoT-Tests ist eine Art von Test zur Überprüfung von IoT-Geräten. Ziel ist es, mehr Einblick und Kontrolle über verschiedene miteinander verbundene IOT-Geräte zu bieten. Daher ist das IoT-Test-Framework wichtig.

**Funktionstest:** Grund ist die Überprüfung der Benutzerfreundlichkeit des Systems beim IoT-Testen sehr wichtig.

**Benutzbarkeitstest:** die Überprüfung der Kompatibilität im IOT-System wichtig.

**Zuverlässigkeit und Skalierbarkeit:** Zuverlässigkeit und Skalierbarkeit sind wichtig für den Aufbau einer IOT-Testumgebung.

**Data Integrity:** Es ist wichtig, die Datenintegrität bei IOT-Tests zu überprüfen, da es sich um grosse Datenmengen und deren Anwendung handelt.

**Security:** wichtig, den Benutzer über die Authentifizierung zu validieren und im Rahmen der Sicherheitstests Datenschutzkontrollen durchzuführen.

**Performance:** Leistungstests sind wichtig, um einen strategischen Ansatz für die Entwicklung und Implementierung eines IOT-Testplans zu entwickeln.

# Cloud-Service-Modelle

Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), Storage as a Service ( STaaS), Data as a Service (DaaS), Function as a Service (FaaS).