Base-Net Informatik AG

Doku M216

Dario Krieger

Dario Krieger

Inhaltsverzeichnis

Einstieg IoE

Die Säulen von IoE

- People, Process, Data, Things

Einsatzmöglichkeiten IoE

- Netzwerke aus Sensoren und elektronischen Geräten
- Komplexe Aufbauten wie VR, Konzerte, 4D-Kino
- Gesundheits- und Wellnessdienste
- Einrichtung einer Smart City
- Verkehrsinfrastruktur
- Industriemaschinen und verteilte, intelligente Hardware

Definition of Computergerät (Dinge)

Führt Berechnungen basierend auf einer Reihe von Anweisungen durch.
Drei Hauptkomponente:

- CPU (zentrale Verarbeitungseinheit)
- RAM (Speicher)
- Ein-/Ausgabeeinheiten (I/O)

IoT vs IoE

IoT beschränkt auf physische Objekte zu verbinden. Dabei werden lediglich lokale Daten ausgetauscht, welche meist in Echtzeit von den Geräten im Netzwerk gesammelt + verarbeitet werden.

Im IoE sind Dinge mit externen Daten und Menschen verknüpft. Physische Geräte dienen als Quelle von Daten, zur Verarbeitung und Ausführung der am ende eines Prozesses getroffene Entscheidungen.

Wie sieht es heute aus?

Man rechnet mit etwa 50 Milliarden «Dingen» im Internet

Daten

Was sind Daten?

Schlüsselelement aller Computersysteme. Durch Interpretation können werden diese zu Informationen. Durch weitere Verarbeitung werden diese zu Wissen. Werden von Sensoren gesammelt.

Daten im IoE

Daten im IoE werden als Informationen betrachtet, die im Laufe der Zeit von externen Systemen gesammelt wurden. Sensoren und Geräte sind eine ständige Quelle neuer Daten.

Big Data

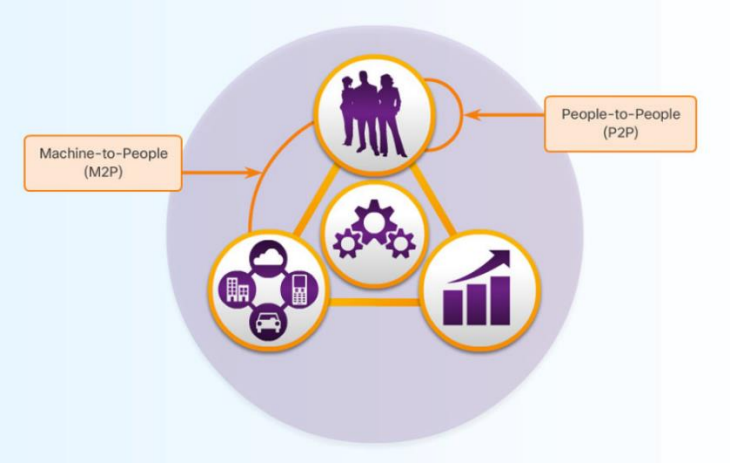
Unter Big Data versteht man die unendliche Fülle von Informationen, welche im Internet durch die wachsende Anzahl verbundener Geräte generiert werden.
Drei Haupteigenschaften: Volumen, Vielfalt und Geschwindigkeit

Volumen = Menge der transportierten und gespeicherten Daten
Vielfalt = Beschreibt Typ (Audio, Video etc.)
Geschwindigkeit = Zeigt, wie schnell Daten produziert, empfangen und evtl verarbeitet werden

Menschen

Definition

Menschen sind eine **zentrale** Figur jedes **Wirtschaftssystems**. Diese können **Konsumenten** oder auch **Produzenten** sein.
Dabei nutzen sie Kontakte und Verbindungen von:
Mensch zu Mensch (person-to-person, P2P)
Maschine zu Mensch (machine-to-person, M2P)
Maschine zu Maschine (machine-to-machine, M2M)



Menschen im IoE

Im IoE greifen Menschen auf extern gewonnene Daten und Dinge zu, um auf dem daraus gewonnenen Wissen Massnahmen zu ergreifen und Entscheidungen zu treffen.

Prozesse

Ein Prozess ist ein geregelter Ablauf von mehreren Aktionen, die von einem oder mehreren Akteuren durchgeführt werden und dazu dienen, Information im Sinne des Endverbrauchers aufzubereiten, zu transportieren und bereitzustellen. Verarbeitung der Daten.

Prozesse im IoE

Im IoE erleichtern optimierte Prozesse die Interaktion zwischen menschen, Dingen und Daten, indem sie dafür sorgen, dass die richtigen Informationen zur richtigen Zeit zugestellt werden.
Dabei werden alle Verbindungen genutzt (M2M, M2P und P2P)

Das Internet of Everything

Das IoE stellt Verbindungen zwischen Menschen, Prozessen, Daten und Dingen her. Diese vier Säulen werden zusammengebracht, um Synergien zu nutzen, wodurch jede Säule die Wirkung und Fähigkeiten der anderen verstärkt.

IoT – Das Netz der Dinge

Vier Kernkomponenten

- Physische Objekte, Konnektivität, Sensorik und Infrastruktur

Physische Objekte

Physische Objekt, die verbunden werden sollen: Ob Druckmaschinen, Paletten, Pakete oder Strassenlaternen. Was wir aus dem IoT machen, hängt davon ab, wie kreativ wir sind.

Konnektivität

Kein Internet ohne Verbindung. Im Falle des IoT gibt es viele Wege, die ans Ziel führen. Dafür kommt es auf stromsparende Modems an den Geräten selbst, aber auch auf die richtige zugrundeliegende Funktechnologie an

Sensorik

Da es etwas gibt, worüber die Dinge funken können, ist die richtige Sensorik wichtig. Das IoT kann seine Umgebung auf viele Weisen erfassen und auch Aussagen über sich selbst treffen.

Infrastruktur

Erst mit einer Daten-Infrastruktur, die die Daten verknüpft und daraus Erkenntnisse zieht, wird der Datenschatz auch gehoben.

IIoT – Industrielle Internet der Dinge

Definition

Es ist eine Unterkategorie des IoT. Das IIoT ist eine Schlüsseltechnologie der Industrie 4.0, der nächsten Phase der industriellen Transformation. Diese basiert auf intelligenter Technologie, Daten, Automatisierung, Vernetzung, künstlicher Intelligenz, sowie weiteren Technologien und Fähigkeiten.

Das IIot bietet viele derselben Vorteile wie das IoT: Intelligente Sensoren in Fertigungsmaschinen, Energiesystem und Infrastruktur wie Rohr- und Kabelleitungen

Was macht das IIoT?

Es optimiert die Kommunikation zwischen Maschinen und liefert Werksmanagern Daten, die ein klareres Bild davon vermitteln, wie eine Einrichtung arbeitet.

Durch das kontinuierliche Sammeln detaillierter Daten können Industrieunternehmen genauer kontrollieren, wie viel Elektrizität, Wasser und andere Ressourcen sie verbrauchen, wann ihre Maschinen laufen und wie viel diese produzieren.

Durch die kontinuierliche Optimierung können Unternehmen viel Energie, Wasser und Ressourcen sparen, während die Produktivität konstant bleibt oder auch steigt.

Unterschied zwischen IIot und IoT

- **Marktorientierung**: Das IoT ist dem Fokus nach eher auf allgemeinere Anwendung, da es viele Nutzer und unterschiedliche Sektoren gibt. Das IIoT ist im Gegensatz nur in industriellen Umgebungen von Spezialisten eingesetzt. Zu den IIoT-Haupteinsatzbereichen zählen Kraftwerke, Öl- und Gasraffinerien sowie Produktionsanlagen.
- **Ziele**: IoT-Bereitstellungen zielen in der Regel auf mehr Effizient, einen besseren Arbeitsschutz und erhöhte Benutzerfreundlichkeit ab. IIoT-Bereitstellungen verfolgen in der Regel nur die ersten beiden Ziele, während der Benutzer weniger im Mittelpunkt steht.
- **Endgeräte**: Die Endgeräte unterscheiden sich im IIoT sehr, da es industrielle Maschinen sind.
- **Ausfallsrisiko**: Das Ausfallsrisiko im IIoT sollte möglichst klein sein
- **Kompatibilität mit Altsystemen**: Es ist die Vorgabe, somit man nicht immer als frisch haben muss (z.B. alte Word formate)
- **Umgebungsanforderungen**: Hitze, Feuchtigkeit, Umweltbelastungen sind im IIoT wichtiger.

Künstliche Intelligenz

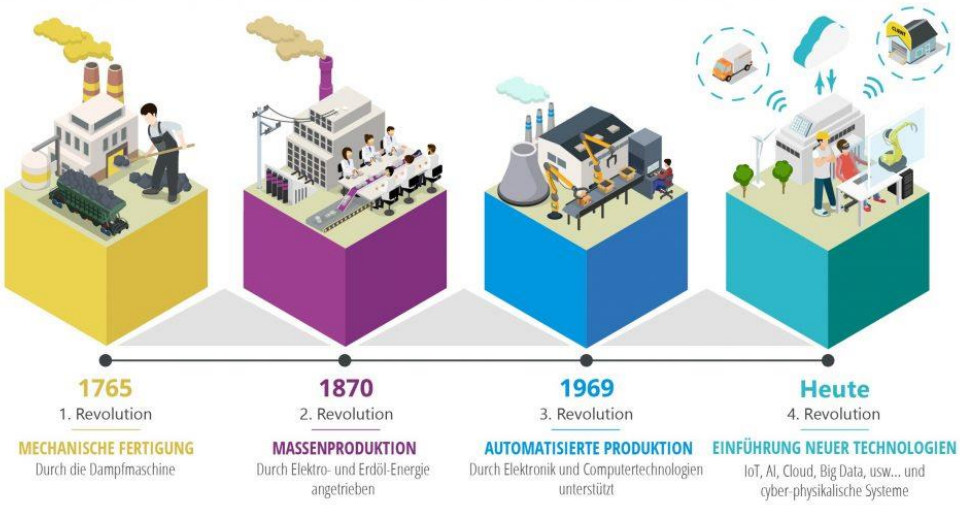
Die KI kann z.B. Muster in den Messwerten aus der Produktion erkennen und kann sogar den Fertigungsprozess immer weiter verbessern.

IoE vs IoT

Beim IoT (Internet of Things) werden Gegenstände intelligent gemacht, das heisst durch Logiken und Netzwerkfunktionalität wird es diesen ermöglicht mit anderen Geräten Informationen auszutauschen.

Beim IoE (Internet of Everything) werden die intelligenten **Dinge** mit **Prozessen**, **Daten** und **Menschen** verknüpft, welches zu einer zunehmenden Automatisierung der Wirtschaft führt und verstärkt Auswirkungen auf die Gesellschaft hat, Stichwort „**Big Data**".

Industrie 4.0



Die Industrie 4.0 bezieht sich auf eine neue Generation von vernetzten, robotergestützten und intelligenten Unternehmen. Die Grenzen zwischen der physischen und der digitalen Welt verschwimmen. Mit 4.0 interagieren Menschen, Maschinen und Produkte miteinander.

Cloud und Edge Computing

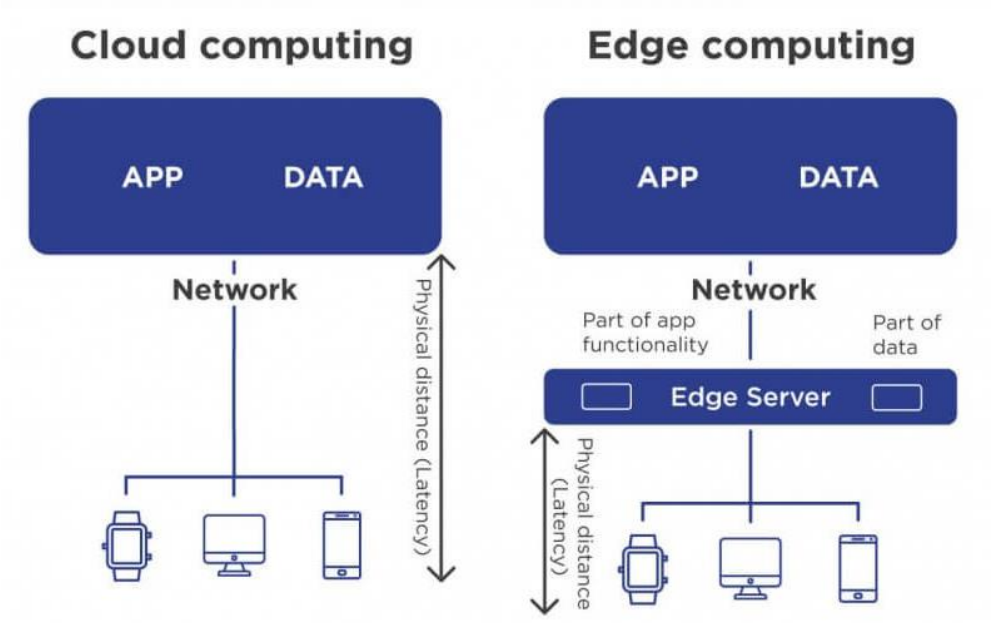
Das Zusammenspiel von Cloud und Edge Computing ist in der Industrie zum Standard geworden (z.B. IoT-Daten arbeiten mit KI)

Definition Cloud Computing

Datenverarbeitung in einer Cloud – Ist ideal, um grosse Datenmengen zu speichern, zu verarbeiten und KI-Modelle zu trainieren. Die Cloud ist über das Internet mit dem Feld verbunden.

Definition Edge Computing

= Wenn Felddaten nicht direkt in die Cloud gespeichert werden, sondern wenn sogenannte Edge Devices – Rechner, die physikalisch dicht bei den Datenerzeugern liegen – diese Rohdaten aufbereiten (z.B. analysieren) und nur die relevanten Ergebnisse an die Cloud übermitteln.



Protokolle

Drahtgebundene Übertragungen werden in 2 verschiedenen Kategorien unterteilt:

Analoge Signale

- Signale sind fliessend
- Spannung wird kontinuierlich verändert

Bsp. Audiosignal zum Lautsprecher, Temperaturfühler, Dimmer

Digitale Signale

- Signale sind stufenweise oder Binär
- Spannung wird stufenweise verändert oder als Binär-Signal ein-/ausgeschaltet

Bsp. Ethernet per Kabel, Lichtschalter, Digitalthermometer, Treppe

Anmerkung zu Digitalen Übertragung (Protokolle)

Simplex

Daten werden nur in eine Richtung übertragen

Duplex

Daten werden in beide Richtungen übertragen

Half-Duplex

Zeitgleich nur in eine Richtung

Full Duplex

Zeitgleich in beide Richtungen

Asynchron

Daten werden nach Belieben übertragen

Synchron

Daten werden nach einem bestimmten Takt (Uhr) übertragen

Parallel

Daten werden gleichzeitig auf mehreren Drähten übermittelt

Seriell

Daten werden auf einem Draht hintereinander gesendet

Master

Hauptgerät, welches in einem Verbund die Priorität hat oder die Steuerung übernimmt

Slave

In der Regel ohne Master nicht nutzbar

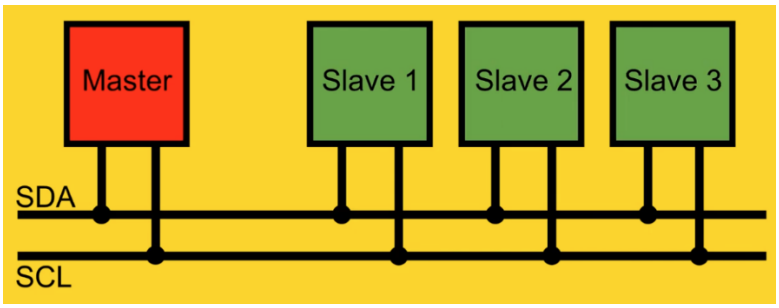
I²C - Inter-Integrated Circuit

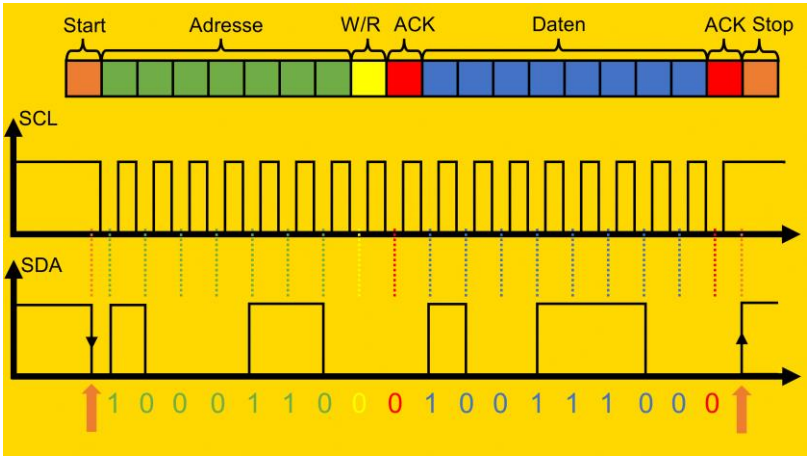
Der I²C-Bus ist eine Zweidrahtverbindung zwischen Master (Controller) und an angeschlossene Sensoren oder IC-Bausteine (Slaves) → Für kurze Distanzen, Master steuert Verbindung

An einer Kommunikation können auch mehrere Master und max. 128 Slaves beteiligt sein. Die zwei notwendigen Datenleitungen sind SDA (Datenleitung) und SCL (Taktleitung); SDA und SCL bilden den Datenbus. Maximale Reichweite ca. 10m

SDA (Serial Data Line: serielle Datenleitung) und SCL (Serial Clock Line: serielle Taktleitung)

Insgesamt 4 Leitungen: 5V DC GND, SDA, SCL





MQTT

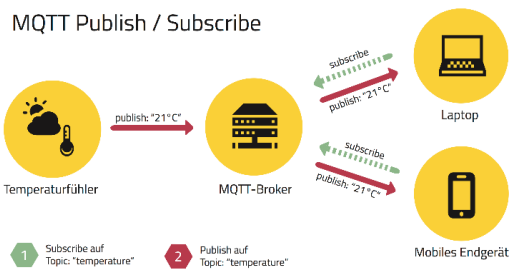
MQTT (Message Queue Telemetry Transport) ist ein schlankes Protokoll für die Kommunikation zwischen verschiedenen Geräten (M2M – machine-to-machine). Es nutzt das publisher-subscriber Modell um Nachrichten über das **TCP/IP Protokoll** und **UDP auf Transportebene** zu senden.

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.

Jedes Datenpaket muss eine Information zur Identifikation haben = Topic Name.

Das MQTT-Protokoll benötigt einen Datenbroker. Alle Geräte senden ihre Daten nur zu diesem Broker. Der Broker sendet diese Daten dann an alle Geräte, die dieses Topic abonniert haben. Topics sind sehr bequem, um verschiedene Beziehungen zu organisieren: one-to-many, many-to-one und many-to-many

MQTT-Port 1883 (unverschlüsselt) und 8883 (verschlüsselt)



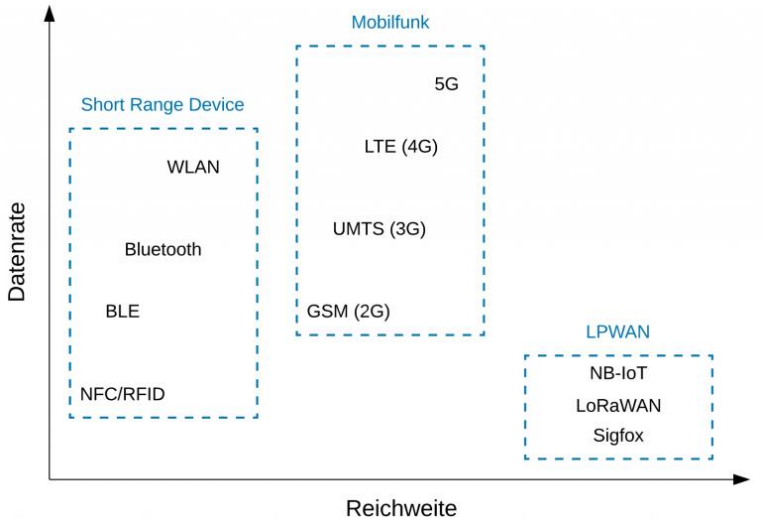
Funktechnologien und deren Einsatzgebiet

Durch Nutzung von Funktechnologien entfällt bei den IoT-Sensoren der Kosten-/Zeitaufwand für die Verkabelung. Dazu können sie somit auch an Standorten ohne Zugang zum Stromnetz und Netzwerk verbaut und über eine Batterie mit Strom versorgt werden.

Bei IoT-Lösungen im Consumer-Bereich werden meistens Funktechnologien wie z.B. WLAN, Bluetooth oder ZigBee eingesetzt (Short Range Device). Diese Funktechnologien haben einen geringen Energieverbrauch, aber auch geringe Reichweite (100m)

Für industrielle IoT-Lösungen wird noch häufig der klassische Mobilfunk (GSM, UMTS, LTE) als Funktechnologie genutzt. Diese Funktechnologien haben jedoch einen hohen Energieverbrauch und ist mit hohen Anschaffungs-/Betriebskosten verbunden.

Daher haben sich mittlerweile für IoT-Lösungen Funktechnologien etabliert, di aus dem Bereich der Low Power Wide Area Network (LPWAN) stammen. LPWAN-Funktechnologien haben geringe Anschaffungs- und Betriebskosten, geringen Energieverbrauch, gute Durchdringung von Objekten und können Datenpaket mit einer geringen Datenraten über Kilometer übertragen. → Durch diese hohe Latenz bei der Datenübertragung, sollten LPWAN-Funktechnologien allerding nicht für zeitkritische Anwendungen genutzt werden.



Die bekanntesten LPWAN-Funktechnologien sind LoRaWAN, Sigfox und NB-IoT.

Funktechnologien ++

Bluetooth

- Kurze Distanzen Daten, Musik, Videos oder Bilder übertragen

Für die Funkverbindung nutzt Bluetooth das ISM-Band (Industrial, Scientific and Medical). Da der Frequenzbereich um 2.4 GHz auch für WLAN oder Funkfernsteuerungen genutzt wird, führt Bluetooth ein Frequenz-Hopping durch. Das bedeutet: Der Sender und der Empfänger können nur für den Bruchteil einer Sekunde auf einen Kanal Daten austauschen und dann gemeinsam auf einen anderen Kanal wechseln.

BLE – der Niedrigenergiemodus von Bluetooth-Geräten / Bluetooth Low Energy

➔ Im BLE werden Verbindung schneller aufgebaut und die Ruhephasen zwischen Sendezyklen verkürzt.

SBC – Standard-Audio-Codec

ZigBee

Bei der Heimautomation verbreitetes Kommunikationsprotokoll. Es vernetzt Produkte im SmartHome herstellerübergreifend.

Das ZigBee-Protokoll regelt, wie Geräte im vernetzten Heim miteinander kommunizieren und Signale übertragen.

- Vernetzt Produkte über kurze Entfernungen
- Funksignal in lizenzfreien ISM-Bändern 868 MHz, 915 MHz und 2.4 GHz übertragen
- Funkreichweite zwischen 10-20 Meter (unter Idealbedingungen bis zu 100m)
- Datenübertragungsrate bei 250 kBit/s

Vielseitiges, Energieeffizientes Heimvernetzungs-Funkprotokoll

Z-Wave

Es wurde für Heimautomatisierung und angrenzende Aussenanlagen entwickelt und für Smart-Home-Anwendungen weltweit lizenziert wurde. Diese Funkkommunikation ist auf geringen Energieverbrauch und hohe Kommunikationssicherheit optimiert.

- Herstellerübergreifend
- Sensoren usw. können über Smartphones, Tablets oder Internetanwendungen gesteuert werden
- Energieversorgung durch Batterie oder Netzspannung
- Bei Netzspannung fungieren sie als Repeater
- Falls Signale nicht direkt zum Empfänger geschickt werden, werden diese über Knotenpunkte umgeleitet
- Reichweite innerhalb Gebäude bis zu 25m
- Reichweite im Freien bis zu 100m
- Vorteil sind die 868 MHz Funkwellen, da sie Wände besonders gut durchdringen

Z-Wave Plus – Erweiterung, z.B. längere Batterielebensdauer, schnelleren Betrieb, grössere Reichweite, einfachere Geräteinstallation.

WLAN

Wireless Local Area Network

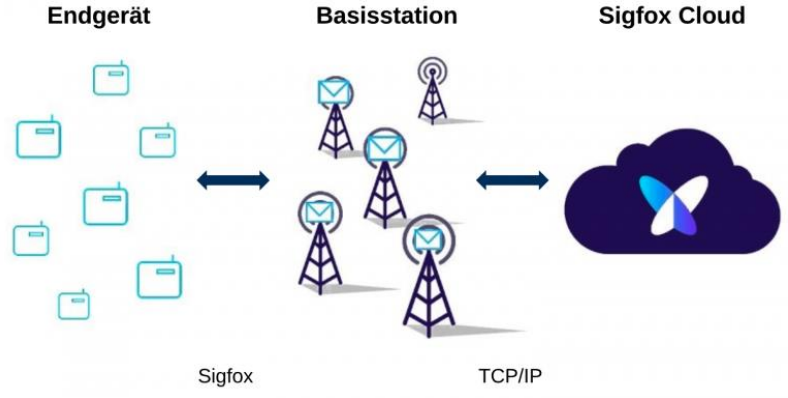
- **Betriebsarten:** WLANs werden je nach Hardwareausstattung und Bedürfnissen unterschiedlich angewendet
- **Tethering / Hotspot:** Verbindung mit einem Client, um diesem eine Internetverbindung zu ermöglichen. Tethering: USB-Kabel, Hotspot = Mobiltelefon = Modem
- **Ad-hoc-Modus:** In diesem Modus ist keine Station besonders ausgezeichnet, sondern alle sind gleichwertig.
- **Infrastruktur-Modus:** Ein drahtloser Router oder Access Point übernimmt die Koordination aller anderen Clients. Dieser sendet in einstellbaren Intervallen kleine Datenpakete, auch Beacons genannt, an alle Stationen im Empfangsbereich. Beacons enthalten die SSID, Liter unterstützter Übertragungsraten und Art der Verschlüsslung
- **Frequenzen und Spezifikationen:** Zwei Lizenzfreie Frequenzblöcke (2.4 GHz und 5 GHz) auf den ISM-Bändern
- **Wi-Fi 6**: Das ist die nächste Generation des Wi-Fi-Standards, der seit Jahren kontinuierlich weiterentwickelt wird. Bessere Effizienz, Flexibilität und Skalierbarkeit.

Energieverbrauch ist mittel

Sigfox

Sigfox betreibt ein gleichnamiges, proprietäres Funknetzwerk, das Anwender gegen eine Gebühr nutzen können, um kleine Datenpaket zu übertragen.

- Sendet im lizenzfreien ISM-Band mit 868 MHz
- Grosse Reichweite bis 40km
- Verbraucht nur wenig Energie, lange Batterielaufzeit der Endgeräte
- Maximal 140 Datenpakete am Tag mit einer maximalen Grösse von 12 Byte



Datenpaket an Basisstation senden = Uplink, Datenpaket von Basisstation empfangen = Downlink

Narrowband-IoT

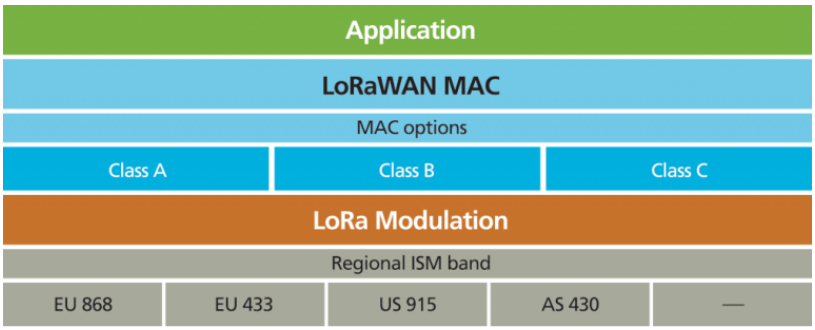
Erweiterung zum LTE-Mobilfunkstandard, wird von Telekommunikationsanbietern bereitgestellt.

- Geringerer Energieverbrauch
- Preiswerter als LTE-Funkmodule
- Sendet im lizensierten LTE-Frequenzspektrum von 450-2200 MHz mit einer Kanalbreite von 200 kHz
- Gute Gebäudedurchdringung mit Frequenzbändern B8 und B20
- Hohe Reichweite
- Abo nötig z.B. Swisscom, Sunrise

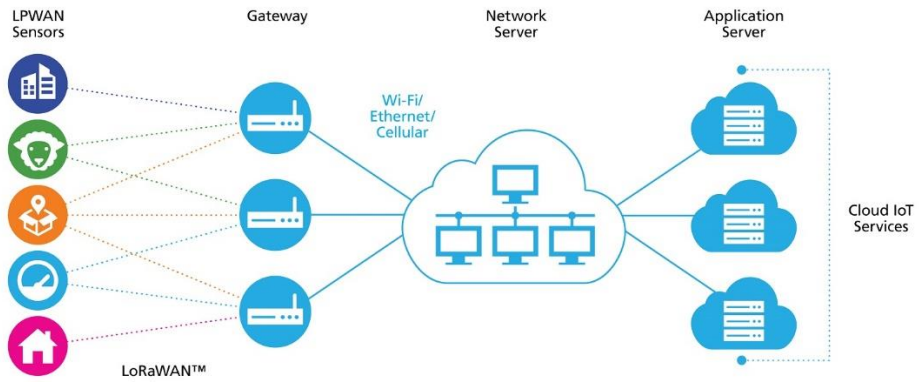
LoRa – LoRaWAN

Long Range Wide Area Network

- Low-Power-Wireless-Netzprotokoll (Auf dem Network Layer)
- Es nutzt das LoRa-Übertragungsverfahren (auf dem Physical Layer)
- Sendet auf dem lizenzfreien ISM-Band
- Tiefe Übermittlungsrate



- Architektur von LoRaWAN-Netzwerk ist als Sterntopologie angeordnert



Endgerät zum Wandungsserver übermitteln = Uplink

Anwendungsserver zum Endgerät = Downlink

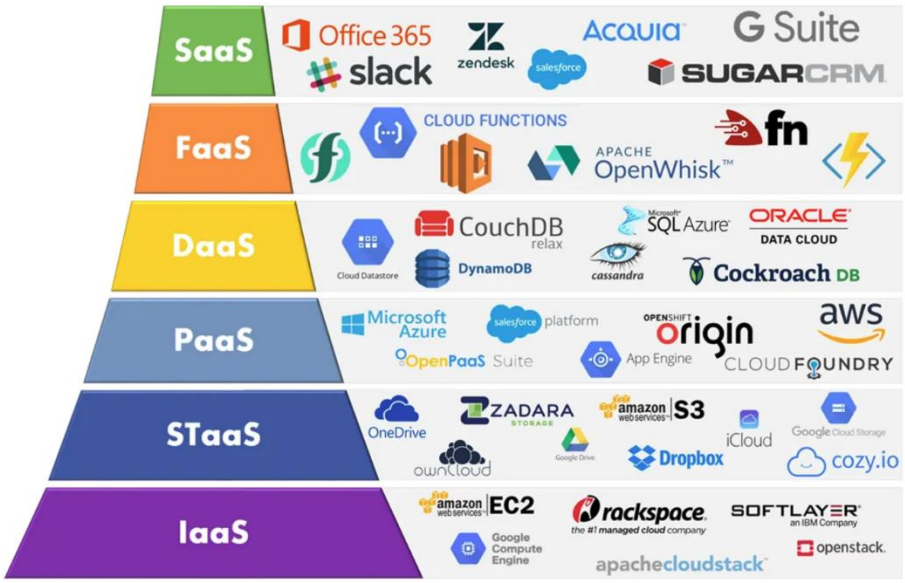
Sensoren & Aktoren

Sensoren nehmen Daten auf / erfassen, Aktoren führen etwas aus (z.B. Schrittmotor)

Reichweiten Beispiel (Reichweite Gross → Klein)

NB-IoT, 5G, ZigBee, WLAN, BLE, NFC/RFID

Cloud-Service-Modelle



Security

Netzwerk ist der Brennpunkt für die IoT-Sicherheit. → Geräte verbinden sich mit dem Netzwerk und das Netzwerk berührt alle Daten und Arbeitslasten. Oft sind die Ursachen, dass Arbeitsplätze usw. nicht genug überwacht werden. Auch ist die Verbindung mit externen Clouds problematisch.

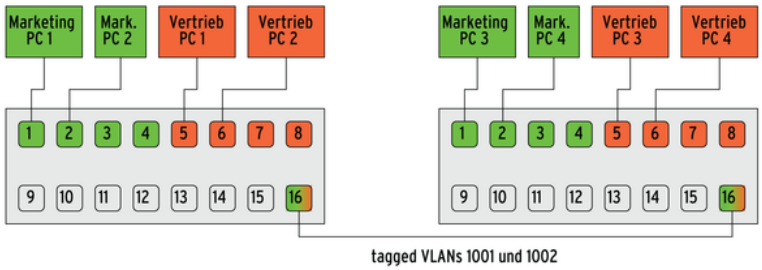
Sicherheitsmassnahmen

- Bestimmen Sie, was das «Ding» im Netzwerk tun darf
- Überwachen Sie abnormales Verhalten
- Verbieten Sie anonyme Verbindungen
- Verwenden Sie das Netzwerk, um diese Regeln durchzusetzen

Netzwerk

Segmentierung der Netzwerke

Die IoT Device sollen in einem eigenen WLAN operieren und keinen Zugriff auf andere Netzwerke haben. Auch lässt sich eine Segmentierung mit VLANs durchführen. → Ports von Switch werden dem entsprechenden VLANs zugewiesen (Virtual Local Area Networks)



Firewall

Herzstück eines Netzwerkes → Sicherungssystem, welches das Rechnernetz vor unerwünschten Netzwerkzugriffen schützt. → Teil des Sicherheitskonzepts. Über Richtlinien kann der Netzverkehr stark limitiert und eingeengt werden.

Firmware

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

Speicherort der Firmware: Flash-Speicher, ROM, EPROM, EEPROM

Zweck eines Firmware-Updates

- Beheben Fehler in der Software
- Optimieren Vorgänge
- Häufig wird die Benutzeroberfläche verändert
- Erweiterung des Systems
- Beheben von Sicherheitslücken im System

Schützenswerte Daten

Das Datenschutzgesetz (DSG) der Schweiz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten, die bearbeitet werden.

- Personendaten
- Besonders schützenswerte Personendaten (Religiöse, weltanschauliche, politische, gewerkschaftliche Ansichten oder Tätigkeiten)
- Persönlichkeitsprofile

Sicherheitsempfehlungen IoT

IT-Grundschutz-Bausteine sind in 10 unterschiedliche Schichten aufgeteilt (von dem deutschen Bundesamt für Sicherheit in der Informationstechnik, kurz BSI)

IoT Geräte können für Spam-Mails oder DDoS-Angriffe verwendet werden. Darum ist es wichtig, diese Geräte auch regelmässig zu Updaten (obwohl es bei einem Smart-Kühlschrank vielleicht nicht so scheint, als würde er sie brauchen). Auch sichere Passwörter oder Benutzernamen können zu besserer Sicherheit beitragen.

Präventive Massnahmen

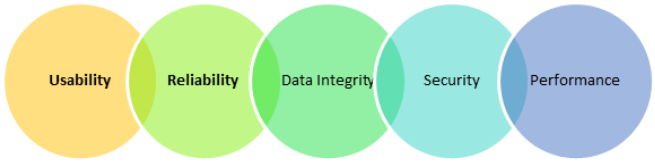
- Wie oft erscheinen Software-Updates?
- Werden diese automatisch eingespielt oder ist eine Interaktion des Benutzers notwendig? Wie erfährt der Benutzer, dass ein Update verfügbar ist?
- Ist das Gerät über Internet erreichbar?
- Welche Schutzmechanismen hat das Gerät? Unterstützt das Betriebssystem eine geschützte Verbindung wie SSH oder HTTPS
- Benutzername und Passwort änderbar?

Bei Internetverbindung

- Vernetzte Geräte in ein eigenes Netzwerksegment, welches kein Zugriff auf PC, NAS etc. hat
- Zugriff zum Internet einschränken
- SSH oder HTTPS verwenden
- Keine Standard-Ports wie 23 – Telnet, 443 – HTTPS usw.
- 2 Faktor Authentifizierung

Testing

IoT-Tests sind eine Art von Tests zur Überprüfung von IoT-Geräten.



Usability / Funktionstest

Da es viele Geräte mit unterschiedlicher Form und Formfaktoren gibt, gibt es die Überprüfung der Benutzerfreundlichkeit des Systems.

Compatibility / Benutzbarkeitstest

Es gibt viele Geräte, die über das IOT-System verbunden werden können. → Geräte habe unterschiedliche Software- und Hardwarekonfigurationen. Daher sind die möglichen Kombinationen riesig. → Überprüfung der Kompatibilität im IoT-System wichtig.

Reliability und Scalability

Dies ist beim Aufbau einer IoT-Testumgebung wichtig → Die Simulation von Sensoren druch den Einsatz von Virtualisierungstools und -technologien.

Data Integrity

Wichtig zu prüfen, da es sich um grosse Datenmengen und deren Anwendung handelt.

Weitere Tests

- Security
- Performance