Zusammenfassung Ambient Intelligence

Contents

Begriffsbestimmung

Was ist **Ambient Intelligence?** (Umgebungsintelligenz)

- Noch eine Vision, Mensch von Computer umgeben, unsichtbar in Alltagsgegenstände integriert, entspannte Interaktion

Definition: Konvergenz von allgegenwärtigem Computing, allgegenwärtiger Kommunikation und an den Benutzer angepassten Schnittstellen

Ubiquitous Computing: Computer verschwinden im Hintergrund und die Umgebung der Benutzer wird rundum mit „unsichtbaren" Sensoren überwacht, um deren Bedürfnisse jederzeit erfassen zu können und dementsprechend zu handeln.

Beispiele: Unity Systems Home Manager aus 1985, Intelligentes Thermostat

Eigenschaften von AmI-Systemen

- **Sensitive (empfänglich für Umgebungseinflüsse):** Sensoren zur Erfassung von Eigenschaften der Umgebung oder von Personen
- **Intelligent (informationsverarbeitend, selbst lernend):** Das System verarbeitet Informationen aus internen und externen Quellen (Benutzerinteraktionen, Informationen von anderen Diensten)
- **Responsive (reaktionsfähig):** Benutzerwünsche werden erkannt, System reagiert darauf
- **Adaptive (anpassungsfähig):** Verhalten ist situationsabhängig, Personalisierte Reaktion
- **Transparent (nachvollziehbar):** Das System ist unsichtbar bzw. unauffällig und stört nicht
- **Ubiquitous (allgegenwärtig):** Dienste werden überall innerhalb einer Umgebung zur Verfügung gestellt

Entscheidungsprozess

Percieve (Sensoren) → Decide (Steuerung) → Act (Aktoren)

Herausforderungen

- **Kommunikation und Interoperabilität in heterogenen Systemen:** Nicht nur auf syntaktischer Ebene, sondern auch auf semantischer Ebene
- **Context-Awareness:** Modell der Umgebung bilden
- **User Experience:** Bereitstellung von geeigneten Benutzerschnittstellen, Benutzerakzeptanz
- **Sicherheit und Privatsphäre:** Schutz vor vorsätzlichen Angriffen, Bewahrung der informationellen Selbstbestimmung

Sensoren und Aktoren

Definition Sensor: Ein Sensor ist ein Element zur Umwandlung physikalischer Größen in elektrische Werte. Er kann möglicherweise ein Teilnehmer eines Bussystems sein, der physikalische Kenngrößen verarbeitet und gegeben falls ein Telegramm auf den Bus sendet.

Sensorarten: Magnetbrücke, Photowiderstände, Ultraschallempfänger, Drucksensor, Glassensor, Lichtsensor, Beschleunigungssensor, Drucksensor, Temperatursensor, …

Wichtig: Die physikalischen Messgrößen (Wärmestrahlung, Temperatur, Druck, Feuchtigkeit, Licht, …) entsprechen nicht der sinnlichen Wahrnehmung (Sehsinn, Gehörsinn, Temperatursinn, …)

Die analogen Messgrößen eines Sensors müssen in digitale Signale umgewandelt werden, dies kann z.B. durch Analog-to-Digital Converter geschehen.

Wahrnehmbare Sensoren

In AmI-Systemen sind Sensoren entweder direkt wahrnehmbar (am Messobjekt, Line-of-Sight) oder nicht direkt wahrnehmbar (durch Objekt messen, Bestandteil des Objekts) eingebaut.

- **Kamera:** Lichtsensor für meist sichtbares Spektrum, Benötigt Line-of-Sight, Integrierbare und miniaturisierbar, aber nie vollständig
- **PIR – Passiv infrarot sensor:** reagiert auf Bewegungen und Wärmestrahlung, kann nicht durch Hindernisse hindurch erfassen, eingesetzt im Außenbereich
- **HF – Hochfrequenz Sensor:** reagiert auf jede Art Bewegung, kann durch dünne Hindernisse erfassen, eingesetzt im KFZ

In Objekten integriere Sensoren

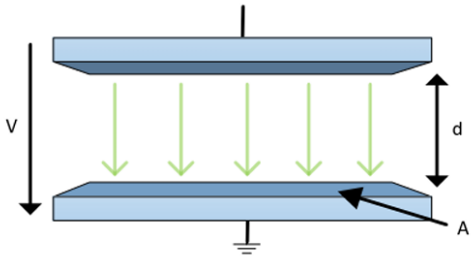
- **Beschleunigungssensor:** Hoch integrierbar, steifere Objekte bieten bessere Messwerte, niedriger Stromverbrauch (µA), eingesetzt in Fitnesstrackern
- **Dehnungsmessstreifen:** Benötigt Kontakt zum gemessenen Objekt, eingesetzt zur Kraft-, Druck-, und Beschleunigungsmessung in z.B. Waagen, Tragwerken, Druckbehältern und Gebäuden

Hinter Objekten verhüllt

- **Mikrofon:** Schall durchdringt viele Flächen oder wird daran reflektiert, komplette Verdeckung ungünstig, da zu große Absorption des Messsignals, eingesetzt in Laptops und Telefonen
- **Kapazitiver Sensor:** Kann durch nicht-leitfähige Objekte hindurch messen, kann zur Abstandsmessung oder Präsenzdetektion verwendet werden, eingesetzt in Touchscreens und Hygrometern

Kapazitive Sensorik

Kapazitive Sensoren sind eine alte Anwendung, erste Anwendung war 1919

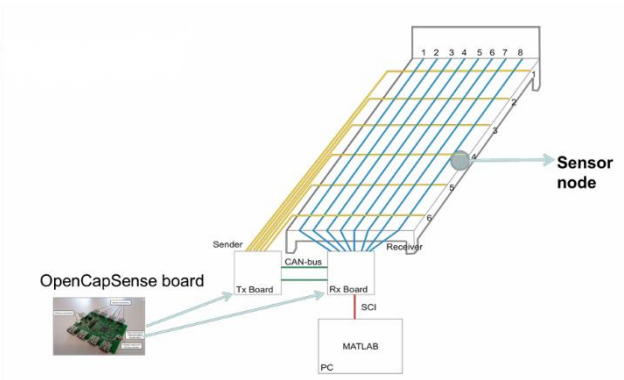


Physikalisches Grundprinzip: Die Kapazität zwischen zwei Platten eines Plattenkondensators hängt ab von der Fläche und dem Abstand

$$C = \varepsilon_0 \varepsilon_r \frac{A}{d}, C \propto \frac{1}{d}$$

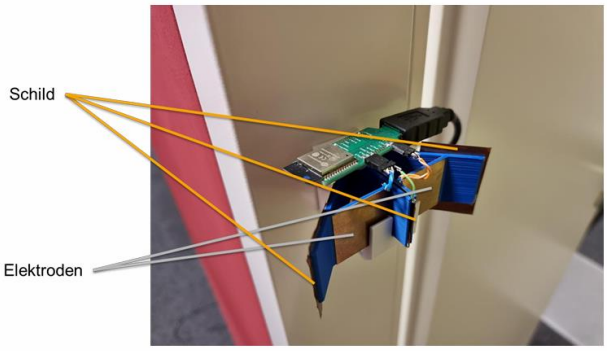
Der Mensch hat eine Grundladung, je näher der Mensch an der Elektrode ist, desto mehr Energie wird zwischen dem Menschen und der Elektrode gespeichert.

Technologie: Aktive Messung durch stetiges Auf- und Entladen einer Elektrode, Anwesenheit ändert die Kapazität der Elektrode, dadurch entsteht eine längere oder kürzere Auf- und Entladezeit



Smartbed

Elektroden: Können einfache Kupferplatte oder ITO (Indium Zinn Oxid) Folie oder PEDOT:PSS Elektrisch leitendes Polymer sein



Anwendungen

Smartbed oder Smartfloor (funktionieren nach dem selben Prinzip) um Schlafposition zu tracken oder Stürze im Zuhause

Türdurchgangssensor: Erfasst wie viele Personen einen Raum betreten, reagiert auch auf Personen, die an der Tür vorbei laufen

- Zwei Elektroden, überprüfen von Herein und Raus gehen in welcher Reihenfolge die Elektroden eine Person messen

Capseat: Elektroden in der Struktur des Stuhls versteckt/integriert, Posen-Erkennung, Physiologische Signale (Atemerkennung), Soft Biometrics (Feststellung von physiologischen Signalen von Personen)

Duoskin: Tragbares, auf der haut liegendes Benutzerinterface (Tattoo ähnlich), kapazitive Sensorik + elektrische Schaltungen, Funktionen: Touch-Input, Thermochromatische Displays, NFC

Hairware: Leitfähige Haarverlängerungen als Elektroden zur Berührungserkennung, Bewusste Benutzung von ansonsten unbewussten Verhaltensmustern

Earfieldsensing: Gesichtsausdrücke als Eingabeverfahren für Mobile- und Wearable Computing, Messung des elektrischen Felds der Muskelaktivität

Pulsoxymetrie

Nichtinvasive Ermittlung der arteriellen Sauerstoffsättigung durch Vergleich von oxygeniertes Hämoglobin (HbO2) und desoxygeniertes Hämoglobin (Hb), aktueller Goldstandard in der Medizion

Messprinzip: Abwandlung der Photophletismographie

Beispiele:

- Oura Ring: Sensorik integriert in einen Fingerring: Photoplethysmographie + Beschleunigungssensor, Schlafanalyse, Aktivität, Atmung, Herzrate, 4-6 Gramm Gewicht, bis zu 1ner Woche Batterielaufzeit
- VIVALINK: Sensorik integriert in einen Klebe-Patch: Elektrokardiographie + Beschleunigungssensor, EKG-Analyse, Herzrate, Atmung, Beschleunigungen, 7,5 Gramm Gewicht, 120 Stunden Batterielaufzeit

Elektrokardiographie

Messung der elektrischen Erregung des Herzmuskels, Medizinische Bewertung der Eigenschaften und Gesundheit des Herzens, Integriert in Smartwatches

Messprinzip: Messung der Spannungsänderungen an der Körperoberfläche

Microsoft Glabella

Kontinuierliche Erfassung des Blutdruckverhaltens, Beschleunigungsmessung zur Erkennung von Bewegungsartefakten, In Form einer Brille

Messprinzip: Optische Messung der Herzaktivität an 3 Punkten (am Nasenflügel, vor und hinterm Ohr), Bestimmung der Pulstransitzeit (PTT), Ableitung des Blutdrucks von der PTT

Kontaktlinse für Diabetiker

Smarte Kontaktlinse mit biometrischer Echtzeit-Analyse und automatischer Medikamentenabgabe, kontinuierliche Glukoseüberwachung, flexibles System zur Verabreichung von Arzneimitteln

Komponenten: Antenne für Energie und Kommunikation, flexible drug delivery system (f-DDS), Glukose-Sensor, ASIC: Power-Management-, Sende- und Empfangs-Einheit und Sensorsteuerung

Weitere Awendungen:

Rovables: Miniature On-Body Robots as Mobile Wearables

Deformwear: Deformation Input on Tiny Wearable Devices

Biohacking: NFC Chip als Körperimplantat

Dermal-Abyss: „Interaktives" Tattoo

Aktoren

Benötigen Steuersignal und Energiequelle (Pneumatisch, Elektrisch, Hydraulisch)

Definition: Ein Aktor (oder auch Aktuator) ist ein gerät, das Informationen empfangen, verarbeiten und demnach Funktionen ausführen kann

Logisches Gegenstück zum Sensor, wandelt elektrische Signale in eine physikalische Größe um, z.B. Bitcode in Temperatur, Spannung in Motorposition, Stromstärke in Helligkeit, …

Eine schaltbare Steckdose macht implizit jedes Gerät zum Aktor (zumindest die Funktion An- und Ausschalten wird unterstützt), Funktion/Nutzen eines Aktors oft erst durch die Verwendung

Mikrocontroller

Steuerung im AmI-Kontext

Anforderungen

- **Eingabe:** Schnittstellen für Sensorik, Aufnahme von Messwerten (= Elektrische Signale von Sensor), Analog-Digital-Wandlung
- **Ausgabe:** Steuerung von Aktoren
- **Echtzeit-Anwendungen**

Echtzeit

Echtzeit bedeutet nicht schnell

Definition: Unter Echtzeit versteht man […], dass die Verarbeitungsergebnisse innerhalb einer vorgegebenen Zeitspanne verfügbar sind.

Harte Echtzeit: Definierte Reaktionszeit wird garantiert und niemals überschritten, Überschreitung würde zu einem (schweren) Unfall führen!, **Beispiele:** Reaktorsteuerung, Autopilot

Weiche Echtzeit: Reaktionszeit wird nur statistisch garantiert, Überschreitung führt nicht zu Fehlern!, **Beispiele:** Streaming, Personal Computer (PC)

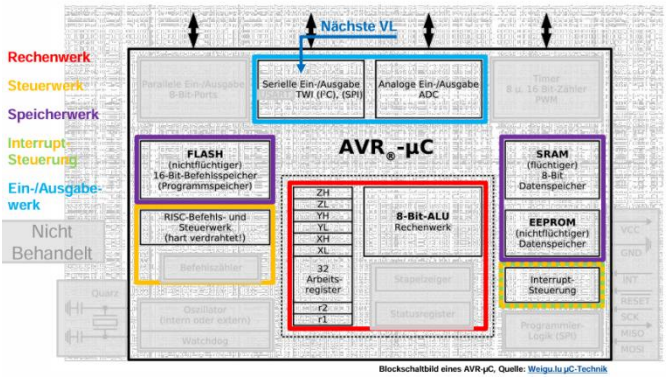
Abgrenzung

- **Mikroprozessor:** Steuerwerk + Rechenwerk (ALU) → CPU
- **Mikrorechner:** Mikroprozessor + Speicher-Werk + E-/A-Werk → PC
- **Mikrocontroller:** Mikrorechner integriert auf einem Chip, optimiert für:
    - Steuerungs- oder Kommunikationsaufgabe

- niedrige Leistungsaufnahme
- harte Echtzeitanforderungen

Mikrocontroller-Aufbau

Rechen- und Steuerwerk

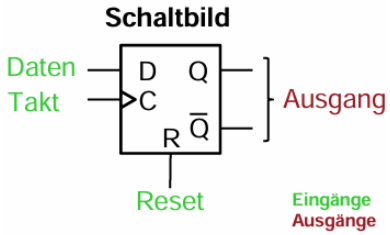


- **Arithmetic Logic Unit (ALU)** / Rechenwerk
  - Führt logische und mathematische Operationen aus
- **Statusregister:** zeigen Statusinformationen zur vorangegangenen Operation an
- **Steuerwerk:** Steuert den Ablauf der Befehlsverarbeitung:
  - Dekodiert Befehle
  - Versorgt die ALU mit Daten und Befehlen
  - Wertet Statusregister der ALU aus
  - Leitet Ergebnisse der ALU an den Speicher weiter
  - Steuert weitere Funktionseinheiten des µC (z.B. Schnittstellen)

Register

Flüchtiger Speicher, Spitze der Speicherhierarchie, besonders schneller Zugriff, ALU hat i.d.R. direkten Zugriff, besteht aus Flip-Flops, Input/Output sind die Pin-Zustände

D-Flip-Flop:



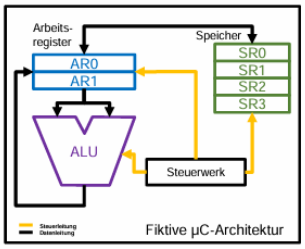
1 D-FF ≙ 1 Bit, Registertiefe entspricht der Anzahl paralleler Flip-Flops, meist mit zusätzlicher Registerauswahl-Leitung realisiert

Weitere Registertypen: Ringregister, Schieberegister,…

Wahrheitstablle

D	C	Q	Q̄	Funktion
0	0	*	*	Speichern
0	1	0	1	Rücksetzen
1	0	*	*	Speichern
1	1	1	0	Setzen

Beispiel-Aufgabe: SR2 = SR0 + SR3



Pseudo-Code:

```
(1)   load   AR0   SR0   Steuerwerk belädt AR0 mit SR0
(2)   load   AR1   SR3   Steuerwerk belädt AR1 mit SR3
(3)   add    AR0   AR1   Steuerwerk stellt ALU auf Addition und Zieladresse AR0 ein
                         ALU führt Addition durch und speichert Ergebnis in AR0
(4)   move   SR2   AR0   Steuerwerk speichert Wert von AR0 in SR2
```

Befehl	Bedeutung
load A B	Register A = Speicher an der Stelle B
add A B	Register A = Register A + Register B
sub A B	Register A = Register A - Register B
move A B	Speicher an der Stelle A = Register B

Speicherwerk

Speicherung und Bereitstellung von Daten und Befehlen

Von-Neumann-Architektur: Befehls- & Datenspeicher kombiniert

Vorteile

- Einfach realisierbar

Nachteile

- Verbindung zum Speicher als Flaschenhals

- Hohe Flexibilität: Freier Speicher kann für Daten und Befehle verwendet werden
- Niedrigere Kosten: Geringerer Verdrahtungsaufwand und einfacheres Steuerwerk

- Langsamer: konkurrierender Speicherzugriff, entweder Daten- oder Befehlscode
- Erzwungener Sequentialismus, keine Parallelität

Harvard-Architektur: Befehls- & Datenspeicher getrennt

Vorteile

- Sicherheit: Code und Daten getrennt, bestimmte Fehler und Angriffe nicht möglich, Selbstmodifizierender Code durch unveränderlichen Speicher vermeidbar
- Buffer-Overflow (Daten überschreiben Code) ist unmöglich
- Schnell, da Daten- und Befehlsspeicher parallel abgefragt werden
- Daten- und Befehlsspeicher können unterschiedlich groß sein (Kostenfaktor)

Nachteile

- Weniger flexibel: Freier Speicher für Daten / Befehle reserviert
- Teurer: Hoher Verdrahtungsaufwand, Komplexes Steuerwerk

Interrupt-Steuerung

Spezielle Komponente des Steuerwerks zur Behandlung von besonderem Ereignis, schnelle und flexible Reaktion auf Ereignisse

Definition Interrupt: Asynchrone Unterbrechung des Programmablaufs: Beim Eintreten wird eine vordefinierte Interrupt-Routine ausgeführt, durch interne und externe Ereignisse auslösbar

Arten:

Interne Interrupts

- Durch µC-interne Ereignisse ausgelöst
- Zeitgeber: Nach Ablauf einer vorgegebenen Zeit
- Schnittstellen: Beim Empfang von Daten
- ALU: Bei Rechen-Ereignissen (z.B. Division durch 0)

Externe Interrupts

- Durch µC-externe Ereignisse ausgelöst
- Nur an speziellen Eingängen/Schnittstellen möglich
- Meist ausgelöst durch Zustandswechsel (0 -> 1 oder 1 -> 0)

Ein-/Ausgabewerk

Bindeglied zur Umwelt – Ein- und Ausgabe von Daten: Zum Anwender oder anderen Systemen

Schnittstellen: I^2C, SPI, UART, …

Analoge und Digitale Ein-/Ausgänge: Logische Schalten

Analog-Digital-Umsetzer

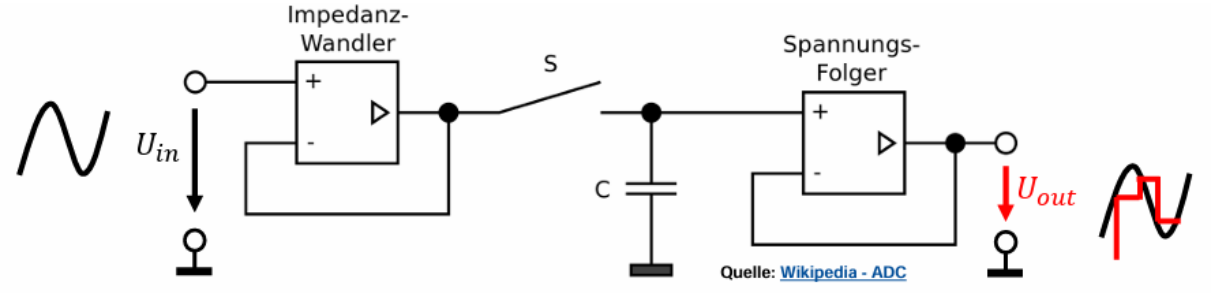
Ein Sensor übersetzt ein nicht-elektrisches analoges Signal in ein elektrisches analoges Signal, dieses muss weiter in ein digitales übersetzt werden

Der Analog-to-Digital Converter (ADC oder A/D-Wandler) ist ein elementarer Bestandteil von Mikrocontrollern und ermöglicht ein „Wahrnehmen der Umwelt“

Digitalisierung des analogen Singals

Zeitliche Diskreditierung:

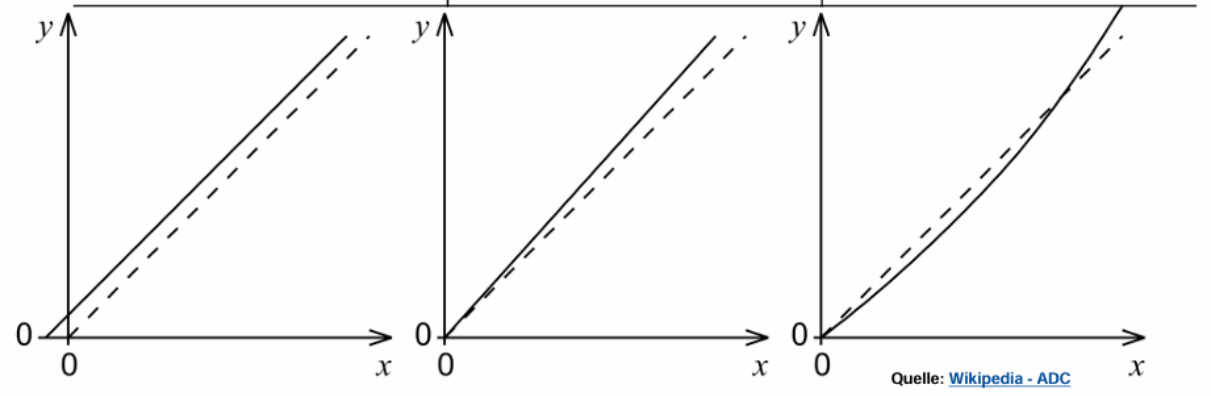
- Zerlegung des Analogsignals in eine zeitdiskrete Signalfolge
- **Nyquist-Shannon-Abtasttheorem** für bandbegrenzte Signale: $f_{abtast} \geq 2 \cdot f_{max}$
- Nicht-Beachtung des Abtasttheorems: Unterabtastung (mit ggf. Aliasing-Effekt)
- Realisierung mittels **Sample-Hold-Glied:** Kondensator hält in der Haltephase (Schalter S offen) die Eingangsspannung U_{in} konstant
    - **Spannungsfolger:** verhindert Entladung des Kondensators C
    - In der Ladephase (Schalter S geschlossen) wird der Kondensator C geladen
    - **Impedanzwandler:** stromfreie Spannungsmessung am Messort



Quantisierung:

- Zerlegung des zeitdiskreten in eine zeit- und wertdiskrete Folge
- Quantisierungsabweichung bzw. Quantisierungsfehler: Abweichung des digitalen vom analogen Signal, abhängig von der Auflösung des ADCs
- ADC-Auflösung: = $2^{Bit-Angabe}$ (2-Bit-ADC hat 4 diskrete Werte)

Nullpunktfehler	Verstärkungsfehler	Nichtlinearitätsfehler
kontinuierlicher Offset	multiplikativer Fehler	Fehler als Funktion f(x)
Behebung: Offset bei Nulleingang bestimmen	Behebung: Vergleich von Null mit Vollausschlag	Behebung: Herstellerkalibration anwenden, linearen Bereich nutzen

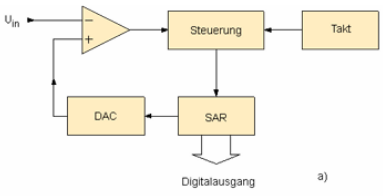


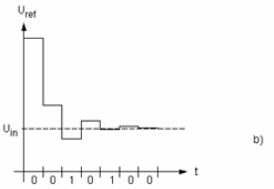
Sukzessive Approximation:

→ U_{in} wird in k Schritten approximiert:

- Über den DAC wird eine Spannung U_{ref} erzeugt
- $U_{ref}^{(n)}$ wird im Komparator mit U_{in} verglichen:
  - $\boldsymbol{U_{ref}^{(n)} < U_{in}}$:
    $U_{ref}^{(n+1)}$ in nächster Iteration um $\frac{U_{ref}^{(n)}}{2}$ hochsetzen
  - $\boldsymbol{U_{ref}^{(n)} \geq U_{in}}$:
    $U_{ref}^{(n+1)}$ in nächster Iteration um $\frac{U_{ref}^{(n)}}{2}$ runtersetzen

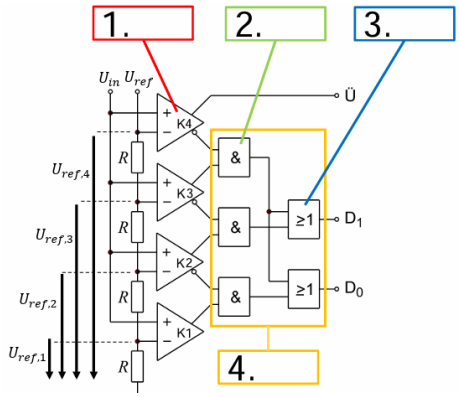
  $(n+1) < k?$
- Anzahl k der Iterationen entspricht der Auflösung des DAC (typischerweise 12 – 14 Bit)





Flash-/Parallel-Umsetzer:

- Direkte Messung der Spannung mittels Komparator-Logik-Schaltung
- Spannung U_{ref} wird an den Vorwiderständen R in Teilspannung $U_{ref,n}$ zerkleinert
  - Teilspannung $U_{ref,n} = U_{ref} \cdot \frac{n}{n_{ges}}$, $n :=$ Nummer der Komparatorstufe
- U_{in} wird über die Komparatoren K mit den Teilspannungen $U_{ref,n}$ verglichen
- Codeumsetzer-Logik erzeugt digitales Signal



1. Komparator
2. UND-Glied
3. ODER-Glied
4. Code-Umsetzer-Logik

Kommunikation

Motivation ist die Interoperabilität, welches ein zentrales Problem in Ambient Intelligence darstellt, wie können die ganzen verschiedenen Systeme miteinander kommunizieren?

Interoperabilität

Herausforderungen:

- Mangelnde Awareness der Hersteller
- Desinteresse der Hersteller (Vendor-Lock-In)
- Menge vorhandener „Standards“
- Altgeräte der Benutzer, die nur nach und nach ersetzt werden
- Kein etablierter Standard für generische Interoperabilität (IoT)
- AmI-Systeme können hunderte Sensoren, Aktoren und IO-Systeme vereinen

Voraussetzungen:

- Standardisierte Schnittstelle(n) für die Vernetzung, Realisierung: kabel- oder funkbasiert, optisch, akustisch, …
- Standardisierte Kommunikation

Ebenen von Interoperabilität

- Protokollebene
- Syntaktische Ebene
- Semantische Ebene

- Benuterebene

Lösungsansatz:

Middleware zwischen Anwendung und Betriebssystem, Dienstleister für den Datenaustausch von entkoppelten Softwarekomponenten und Systemen (Abstraktion der Komplexität), Beispiele: Home Assistant, OpenHAB, COBRA, ColdFusion, …

Middleware als softwareseitige „Lösung“

➔ Konsistente Nutzung erfordert ein hohes Maß an Abstraktion

Relevante Definitionen

ISO/IEC: Interoperability [is] the capability to **communicate**, execute programs, **or transfer data among various functional units** in a manner that requires the user to have little or no knowledge of the unique characteristics of those units → **Viele miteinander kommunizierende Systeme**

IEEE: [Interoperability is] the ability of two or more systems (or components) to **exchange information** and to **use the information** that has been exchanged → **Informationsaustausch**

Wikipedia: Interoperability is a property referring to the **ability of diverse systems** and organizations **to work together** (inter-operate) → **Informationsverständnis**

Wikipedia: (Hardware) Interoperability is a property of a **product or system, whose interfaces are completely understood, to work with other products or systems**, present or future, without any restricted access or implementation → **Definierte Schnittstellen**

Syntaktische Interoperabilität

Korrekte Verknüpfung der Daten

Definition: Fähigkeit zum Austausch von Informationen, basierend auf spezifizierten Dateiformaten und Kommunikationsprotokollen

Voraussetzung: Fähigkeit zum Datenaustausch auf Hardwareebene, liegt dann vor, wenn die ausgetauschten Daten verarbeitet werden können

Semantische Interoperabilität

Definition: Bedeutung von Information wird von den Kommunikationspartnern auf gleiche Weise verstanden

Voraussetzung: Syntaktische Interoperabilität (und Fähigkeit zum Datenaustausch!, Interpretation einer Informationseinheit stimmt bei allen Partnern überein

schwerer zu definieren, zu realisieren und zu verifizieren als die syntaktische Interoperabilität

Technologien

Medium

Kabellos
+ Günstig(er)
+ Einfache Nachrüstbarkeit
+ im Vakuum: höhere Reichweite

- Störanfällig
- Begrenzte Bandbreite
- Unsicher (Zugriff von außen)

Kabelgebunden
+ Robust
+ Sicher
+ Hohe Datenrate
+ Auf der Erde: höhere Reichweite
- Teuer
- Planung zur Bauzeit, da nachrüsten aufwendig

Standards

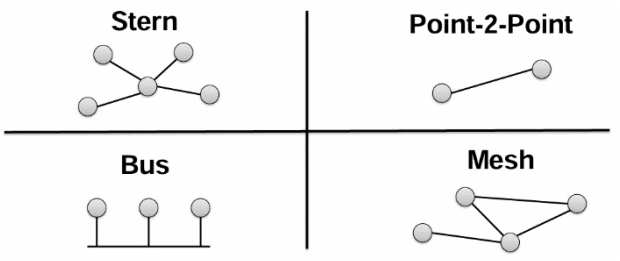
EnOcean, Zigbee, Z-Wave, Thread

KNX, PLC, I²C, Profibus, Ethernet

Topologien

Beispiele:

- HDMI: Kabel, P2P
- Ethernet: Kabel, Stern, Bus, Mesh
- Wifi: Kabellos, Stern, Mesh
- Zigbee/Z-Wave: Kabellos, Mesh
- USB 1.0: Kabel, Bus



Bussysteme

Definition (Wikipedia): [Ein Bussystem] ist ein System zur Datenübertragung zwischen mehreren Teilnehmern über einen gemeinsamen Übertragungsweg […] → **geteiltes Medium**

Definition (Duden): [Ein Bussystem] ist eine Sammelleitung zur Datenübertragung zwischen mehreren Funktionseinheiten eines Computers. → **mehrere Teilnehmer**

I²C – Inter-Integrated Circuit

Schnittstelle für unterschiedlichste Hardwarekomponenten über kurze Distanzen mit mittlerer bis hoher Übertragungsgeschwindigkeit.

1992 von Philips (später NXP Semiconductors) als Standard veröffentlicht

Funktionsweise: Serielles Bussystem für die Kommunikation von Hardwarekomponenten auf Board-Ebene (kurze Distanzen!), einfacher Master-Slave-Betrieb (es kann mehrere Master geben)

- Master: Generiert den Takt, legt Daten auf Datenleitung (SDA)
- Slave: Nimmt Daten taktsynchron auf

Sukzessive Einführung mehrerer Datenübertragungsgeschwindigkeiten: **Standard** (100 kbit/s), **Fast** (400 kbit/s), **Fast Plus** (1 Mbit/s)

Datenformat: Start-Signal + Adresse (7 bit) + Read / Write (1 bit) + ACK (/ NACK) + $n \cdot$ (1 Byte + ACK / NACK) + Stopp-Signal

Beispiel: Auslesen der Daten eines Slaves

1. Master initiiert die Kommunikation mit Start-Signal: LOW-Setzen von SDA
2. Master legt die Adresse 0x41 (7-bit-Slave Adresse + R/W-bit) auf SDA
3. Slave antwortet mit Bestätigungssignal: ACK (Acknowledge)
4. Slave sendet die Payload: 2 Byte mit dem Wert 0x00 (hexadezimal)
5. Master bestätigt den Empfang: 1. ACK nach dem ersten Byte; 2. NACK am Ende der Nachricht
6. Master beendet die Übertragung mit Stopp-Signal

Wie viele Sensorwerte können maximal pro Sekunde von allen Sensoren mit sequentiellen Messungen abgefragt werden? Siehe Kapitel I²C Beispiel

SPI

Entwickelt von Motorola zur Kommunikation von Hardwarekomponenten auf Board-Ebene

Eigenschaften: Master-Slave Bussystem (ein Master, n Slaves) vier Leitungen:

- SCLK (Clock), MISO (Master-in, Slave-out), MOSI (Master-out, Slave-In), SS (Slave Select) ▪
- Vollduplexfähig

- Taktraten: 1 bis 10 MHz
- Hohe Datenraten

Funktionsweise: Kommunikation über vier Leitungen

- **SCLK:** Vom Master generierter Takt
- **MISO** (Master-in, Slave-out): Kommunikationsweg vom selektierten Slave zum Master
- **MOSI** (Master-out, Slave-In): Kommunikationsweg vom Master zum selektierten Slave
- **SS** (Slave Select): Vom Master gesteuerte Leitung zur Auswahl eines Slaves

I²C

- Geeignet für Kommunikation auf Board-Ebene mit kurzen Distanzen
- Halbduplex – nur eine Partei kann gleichzeitig senden
- Geringe Geschwindigkeit: typischerweise 400 KHz
- Jeder Baustein benötigt eindeutige Adresse
- Nur zwei Leitungen notwendig

SPI

- Geeignet für Kommunikation auf Board-Ebene mit kurzen Distanzen
- Vollduplex – beide Parteien können gleichzeitig senden
- Hohe Geschwindigkeit: typischerweise 10 MHz
- Slave Select wird für die Auswahl von Komponenten verwendet (keine Adressierung notwendig, spart Kommunikationszeit)
- Drei Leitungen und mehrere Slave-Select Leitungen bei Sterntopologie notwendig (viele Pins am Microcontroller benötigt!)

USB

Standardisierung der Kommunikation für Computer-Peripherie

Geräteebene: Tastaturen, Maus, Speicher, Drucker

Eigenschaften: Ein Verbindungstyp für unterschiedlichste Arten von Peripherie, Integrierte Stromversorgung (bis zu 5 Ampere pro Gerät bei USB-PD), Hot-Pluggable (Geräte können jederzeit angeschlossen/getrennt werden), i.d.R. Plug-and-play durch vordefinierte Geräteklassen, i.d.R. günstig zu realisieren

Host-gesteuerte Kommunikation (nur ein Host), zuständig für Spannungsversorgung, Transaktionen, Bandbreitenmanagement, Abfrage der angeschlossenen Geräte (max 127 pro Host)

Upstream und Downstream Connectoren (USB Type A und USB Type B)

Ein USB-Steckertyp implementiert nicht notwendigerweise USB, USB Power Delivery oder einen alternativen Anschlussmodus.

USB-C ist 24-polig, Rotationssymmetrisch, soll alle anderen physischen Anschlüsse ersetzten

Drahtlossysteme

Drahtlossysteme sind Datenübertragungsverfahren, die den freien Raum (Luft bzw. Vakuum) als Übertragungsmedium nutzen

Vorteile:

- Keine Verkabelung mehr notwendig, geringere Kosten
- Ermöglicht Unterbringung in beweglichen Gegenständen

- Einfache Einbringung von neuen Geräten
- Komplett passive Komponenten sind möglich – Betrieb über Umgebungsenergie, wie z.B.: Temperaturunterschiede, Licht, kinetische Energie

Besondere **Herausforderungen an die Interoperabilität:**

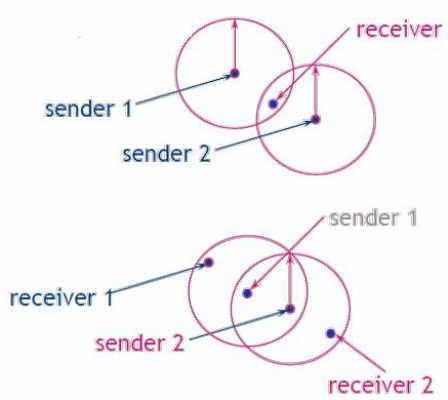
- Häufig batteriebetrieben (Wartungsaufwand!)
- Hoher Energieverbrauch beim Senden Empfangen von Nachrichten und
- In manchen Fällen muss die Übertragung von Nachrichten garantiert sein (bspw. Sicherheitskritische Systeme)

Herausforderungen:

Listen before talk

Daten-Kollisionen beim Zugriff auf den Kommunikationskanal

- Hidden-Terminal Problem: Sender 1 hört nicht, dass Receiver mit Sender 2 kommuniziert
  - Listen-before-talk ist hier sehr optimistisch
- Exposed-Terminal Problem: Sender 1 kann nicht mit Receiver 1 kommunizieren, da Sender 2 mit Receiver 2 kommuniziert
  - Listen-before-talk ist zu pessimistisch



Editors Note: Ich vermute das hier die einzelnen Standards nicht Klausurrelevant sind (keine Garantie)

EnOcean

EnOcean Alliance 2008 gegründet, Spin-Off der Siemens AG

Hauptanwendungsgebiet: Aktoren/Sensoren in der Haus- und Gebäudetechnik, die energieautark arbeiten (Energie Harvesting): Solar-, piezo-, thermische- oder elektromagnetische Energie

Ratifizierter internationaler Standard: ISO/IEC 14543-3-10

- Produkte meistens ohne Batterien mit einer theoretischen Laufzeit von 25 Jahren
- Schmale Bandbreite von 125 kbit/s mit 14 Byte long packages
- Vermeidung von Kollisionen durch pseudo-zufällige Intervalle

Vorteile: Leicht erweiterbar und überall anbringbar

Nachteile: In der Praxis kann die Energieversorgung Probleme machen, kein Rückkanal → Empfangsbestätigung

ZigBee

Seit 2004 etablierter offener Industriestandard basierend auf IEEE802.15.4

Große Anzahl an Spezifikationen von Kommunikationsprotokollen auf Geräten mit Niedrigspannung durch die ZigBee Alliance

Hauptanwendungsbereich: Home Automation

- Vermaschtes Funknetzwerk
  - Rollen: Koordinator, Router und „End Device“
  - Stellt selbstorganisierende Ad-hoc-Netzwerke auf Funkbasis her

- Datentransferraten von 20 bis 900 kbit/s
- Übertragung mittels unslottet CSMA/CA Kanalzugriffsmechanismen

Vorteile: Viele und auch eher günstige Geräte verfügbar und vielseitig einsetzbar

Nachteile: Stellt nur das „Wie“ und nicht das „Was“ bereit → Syntax & Semantik, Kompatibilität von ZigBee-Geräten demnach nur auf Netzwerkebene gewährleistet

Z-Wave

Drahtloser Kommunikationsstandard entwickelt 2001 von dänischer Firma ZenSys

Seit 2005 Z-Wave-Allianz mit über 400 Herstellern und Dienstleistern

Basis für alle Produkte: SoC der Firma Sigma Design mit integriertem Funk Transceiver und 8051 Mikrocontroller

Einheitliche Anwendungsebene mit Pflichtkommandos und -funktionen

- Vermaschtes Netzwerk mit bis zu 232 Knoten
- mehrere Home-Netzwerke parallel mit Routing zwischen den Netzen
- Adressierung: 4 Byte „Home ID“ 1 Byte „Node ID“ – max. 232 Knoten ▪ Datenraten von 9,6 kB/s, 40kB/s oder 100kB/s
- ISM-Band (EU 868 MHz, USA 900 MHz)

Vorteile: Viele und auch eher günstige Geräte verfügbar, vielseitig einsetzbar, höhere Reichweite als ZigBee, Interoperabilität durch Zertifizierung aller Geräte

Nachteile: Geräte aus USA und EU nicht kompatibel, geringe Datenrate

Thread

Energiesparendes Netzwerkprotokoll 2014 entwickelt von der Thread Group (u.a. Google Nest, OSRAM, Samsung, Qualcomm, ARM Holdings, Apple, …)

Protokollspezifikation unter Zustimmung und Einhaltung der EULA kostenlos

Open-Source-Implementierung verfügbar: OpenThread – ursprünglich von Google bereitgestellt, um Nest-Produkte für Entwickler einfacher zu öffnen.

- Selbstheilendes, sicheres Drahtlos-Mesh Netzwerktechnologie
- Nutzt das 2,4 GHz Spektrum
- Baut auf 6LoWPAN (siehe später) auf
- IPv6-adressierbar
- Datenraten von bis zu 250 kB/s

Vorteile: Sehr Energie-effizientes Protokoll (Betrieb mit Knopfzelle über mehrere Jahre möglich), IP-adressierbare Geräte, AES-128-verschlüsselte Kommunikation, selbstkonfigurierendes, selbstheilendes Mesh

Nachteile: Vergleichsweise geringe Datenrate (vgl. WLAN) und geringe Anzahl an Geräten (vgl. Zigbee)

IPv6

Verfügbare Adressen pro Person 4.8×10^28

Jedes Gerät absolut adressierbar

6LoWPAN:

- „IPv6 over Low power Wireless Personal Area Network"
- Drahtloses Datenübertragungsprotokoll für Mesh-Netzwerke
- Definiert die Bitübertragungs-, Sicherungs-, Vermittlungs- und Transportschicht (OSI-Schichtenmodell)

Matter

Quelloffener Kommunikationsstandard für Smart Home und IoT, regelt, wie Geräte miteinander kommunizieren, Lizenzfreigebührenfrei, Zertifizierung jedoch von der CSA gebührenpflichtig

Legt einen Grundumfang an Funktionen fest mit Fokus auf Interoperabilität

- Kommunikation basiert auf IP
- Verschlüsselte Kommunikation über individuelles Gerätezertifikat (DAC)

SmartHome

In den letzten Jahren rapide zugenommen, Prognosen für 2015 1/4 der Bevölkerung mit Smart Home.

Digital vernetzte und kontrollierte Geräte innerhalb eines Hauses, die ferngesteuert werden können, Sensoren, Aktoren und Cloud Services, die die allgemeine Automatisierung unterstützen

Markt: B2C-Verkäufe / Handel von Hard- und Software sowie Abo-Gebühren

Begriffserläuterung

Internet der Dinge (IoT): Digitale Vernetzung von Geräten untereinander und nach außen über das Internet

Digitalisierung: Unter Digitalisierung versteht sich die Implementierung moderner und innovativer Informations- und Kommunikationstechnologien

Smart Home: Ausprägung des IoT bezogen auf eine Wohnung bzw. Privathaus

Smart Building: Meist Nichtwohngebäude z.B. Büros, Hotels, Krankenhäuser, aber auch Wohngebäude wie Mehrfamilienhäuser.

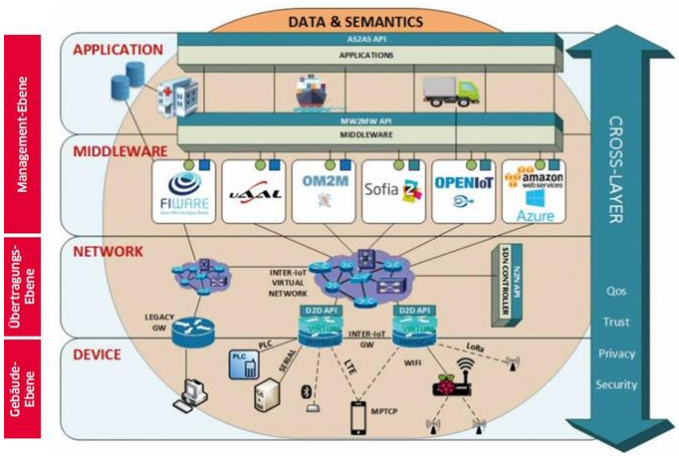
Smart Living: Bezeichnet das Leben in der digital vernetzten Wohn- und Lebensumgebung, geht über die Grenzen der Gebäude hinaus und deckt verschiedene Lebensbereiche ab

Intelligente Umgebungen

Produkt	Smartes Produkt	Smartes, verbundenes Produkt	Produkt System	Ecosystem (Smart Building)
Passiv	Mit Sensoren	Mit Konnektivität	Verbunden mit verwandten Produkten oder Anwendungen	Integration diversere Baufunktionen

Smart Building besteht aus der Gebäude Ebene, der Übertragungsebene, der Management-Ebene sowie Gebäudedaten.

Gebäude-Ebene



Woher kommen die Daten? (technische Gebäudeausstattung, Sensorik, Hardware), auch Feldebene oder Automatisierungsebene genannt

Systemkomponenten: Aktoren, Sensoren, Bussysteme, Protokolle, Standards, Intelligent, Bediegeräte

Aktoren und Controller: sind aktive Komponenten, die eine Aktion ausführen. In einem Wohnhaus wären dies diverse Schalter z.B. für Licht und Dimmen, Heizungsventile, Rolladenmotoren, Türschlösser usw.

Sensoren und Zähler: sind passive Komponenten, die eine physikalische Größe messen. Solche Größen könnten Temperatur, Luftfeuchtigkeit, Bewegung, Kohlendioxidgehalt, Lichtstärke usw. sein

Übertragungsebene

Wie bewegen sich die Daten? (Funk, Lan, Protokoll), hier werden die Datenwege betrachtet, von der Quelle der Daten im Gebäude bis zum Zielort. Bussysteme übertragen die gemessenen Werte und alle anderen Daten zwischen den Systemkomponenten. Damit diese übertragenen Daten von allen Systemkomponenten verstanden werden, nutzen sie Protokolle.

Kompatibilität: folgen Protokolle etablierten Standards können Systemkomponenten von verschiedenen Herstellern genutzt werden und sich untereinander verständigen

In der Gebäudeautomation wird z.B. das **BAC Net** (Building Automation and Control Networks) genutzt.

Aus dem Machine-to-Machine-Communication (M2M) Bereich gehen auch das **MQTT** (Message Queuing Telemetry Transport) hervor.

Es gibt von Unternehmen vorangetriebene Protokolle, die nur durch die Nutzung von „Gateways“, als Übersetzungsstation, untereinander kommunizieren können (KNX, z-wave, enOcean usw.).

Gateways sind wie das Tor zwischen Netzen, jedoch hat sich bisher kein zentrales Gateway durchgesetzt welche für alle Anwendungen im Gebäude zur Verfügung steht. Im Gegenteil, jede neue Anlage in der technischen Gebäudeausstattung hat ein eigenes Gateway.

Management-Ebene

Wohin gehen die Daten? (Software, Plattform, Server, Cloud) wird auch als Gebäudeleittechnik-Ebene bezeichnet und überwacht die Funktionen und Prozesse des Gebäudes und wertet diese aus. Im Unterschied zur reinen Automatisierung können von dieser Ebene aus ereignisbezogenen oder zeitkritischen Reaktionen im System der Gebäudetechnik ausgelöst werden.

Digitale Planungsunterlagen (Building Information Model, BIM): sind digitale und dreidimensionale Planungsunterlagen aller an Bau und Betrieb eines Gebäudes beteiligten, diese digitalen Gebäudemodelle sind die notwendige Grundlage für das Monitoring der Gebäudeperformanz. BIMs sind eine Art digitaler Zwilling. Ältere Gebäude werden mit neuen Anwendungen nachdigitalisiert (z.B. 3D Scanning).

Software für den Gebäudebetrieb: Digitalisierung seit 1990 mit Computer-Aided Facility Management (CAFM), wird von zahlreichen Anbietern auf dem Markt angeboten, auch Vernetzung zu

Systemen, meistens von den Komponentenherstellern der Gebäudeautomation. Ziel ist technisch und kaufmännisch effizientes Management.

Schnittstellen: dienen dem Datenaustausch zwischen Anwendungen und Systemen, Standardisierung ist wichtig. Offene Funk-Schnittstellen sind schwer zu sichern. Zugang auf Datenebene reicht meistens aus, um personenbezogene Daten zu bekommen.

Plattformen: Datenaufbereitung und -bereitstellung, Visualisierung und Analyse, Daten herstellerunabhängig verfügbar.

Gebäudedaten

- Daten erzeugt durch **technische Anlagen**
- Daten erzeugt durch die **Nutzung** des Gebäudes
- Daten aus **externen Quellen**

Intervall zum erheben der Daten ist vom Anwendungsfall abhängig:

- Gebäude sind statisch
- Bedürfnisse der Menschen im Gebäude ändern sich schneller
- Permanente Änderung (Echtzeit)

Daten werden durch die Anlagenhersteller, Dienstleister, Wartungsverträgen, Energielieferanten und Messstellenbetreibern bereitgestellt. Wichtig ist Sicherheit und Datenschutz, der Datenaustausch muss mit definierten Rollen und Zugriffsrechten stattfinden, der Speicherort muss transparent dargestellt werden.

Aufrüsten zum SmartHome

Kabellose Automatisierung der Haushaltsgeräte

1. Funkreichweite prüfen und optimieren, bauliche Gegebenheiten beachten
2. Technische Anforderungen der Geräte prüfen

Umfassende Vernetzung komplexer Elektro-, Heiz- oder Beleuchtungssysteme

Ziele und Schwerpunkte der Anwendungsbereiche definieren:

- Sicherheit: Überwachung, Alarmsysteme, Warnmelder, Zugangskontrolle, …
- Energie/Klima: Heizung, Belüftung, Verschattung, …
- Komfort: Haushalt, Elektronikgeräte, Beleuchtung, …
- Entertainment: TV, Audio, Spiele, …

Viele Geräte in den Bereichen Haushalt, Fitness & Gesundheit, Entertainment, Licht, Heizung und Sicherheit können **selbst nachgerüstet** werden. Hier muss man entscheiden zwischen **Komplettsystemen** um Kompatibilitätsprobleme zu vermeiden oder **modulare Nachrüstsysteme** (häufig als Gemeinschaftsangebot von Firmenzusammenschlüssen).

Kosten für Nachrüstung berechnen: Bestandteile, Anschaffung, Einbau, Handwerker, Expertengutachten, Denkmalschutz, Mieter oder Vermieter? → Förderung durch Staat oder Kreditanstalten

Gesetzliche Rahmenbedingungen beachten!

Anwendungen

Smart Home

Individuelle Smart Home Anpassung:

- Wohnungsausstattung passt sich an die unterschiedlichen Lebensabschnitte und Szenarien an.
- Flexible Ausbaustufen, in den verschiedenen Lebensabschnitten werden verschiedene Funktionen benötigt, dies wird durch verschiedene Komponenten realisiert, wichtig ist hier die einfache Anpassung in Zukunft
- Herausforderungen sind eine individuelle Miete, Aufklärung über Möglichkeiten, der Ein- und eventuelle Rückbau

Smart Building

Wichtig für ein Smart Building sind Monitoring, Effizienz, Energieeinsparung, Mehrwert

Monitoring: Man benötigt ein fundiertes Wissen über den Zustand technische Anlagen, die Datenerhebung ermöglicht Monitoring, Datenanalyse führt zu modernem Gebäudemanagement, man benötigt Kenntnisse zu Verbräuchen und Auslastung. Digitale Planungsunterlagen führe zu einem dynamischen und nutzerorientierten Energiemanagement.

Effizienz: Visualisierung von Messdaten, Analyse und Management von Informationen ist eine Voraussetzung, bildet die Entscheidungsgrundlage für das Steuern, Regeln, Warten und Reparieren eines Gebäudes → vorausschauende Instandhaltung

Energieeinsparung

Größter Teil ist Raumwärme, Klimaziel macht Druck, Energie zu sparen, 16.7% erneuerbare Energien, Experten vermuten 30% Energieeinsparung durch optimieren der vorhandenen Analgen und nutzerspezifische Anpassung, Einsparpotential durch Digitalisierung 14%-26%

Smart Meter

Messstellenbetriebsgesetzt, welches 2016 verabschiedet wurde und die Digitalisierung der Energiewende vorschreibt. Das Gesetzt liberalisiert und ermöglicht weiteren Marktteilnehmern den Zugang. Alle Stromkunden müssten einen Digitalen Stromzähler erhalten, welcher allein noch kein Smart Meter ist. Zum Smart Meter wird dieser durch ein Gateway, welches den Verbrauch detailliert darstellt.

Größere Stromverbraucher (>6000 kWh/Jahr) und Erzeuger erhalten Smart Meter, dieses ermöglicht den Datenaustausch zwischen Erzeugern, Verbrauchern, Stromlieferanten und Netzbetreibern. Die verschlüsselten Messwerte werden an den Netzbetreiber übertragen, dieser kann so den Netzzustand genau feststellen.

Das **Smart-Meter-Gateway** sammelt die Messdaten von den digitalen Zählern der Verbraucher und Erzeuger und sendet diese Daten an den Netzbetreiber, so soll die Stromversorgung gesichert werden.

Beim **Submetering** werden die Wasser- und Wärmekosten in Mehrfamilienhäusern und Gewerbeimmobilien erfasst und individuell abgerechnet, so kann eine Nebenkostenabrechnung per Knopfdruck erstellt werden.

Heizkostenverordnung 2021

Heizkosten müssen aus der Ferne abgelesen werden können, überall bis Ende 2026, gilt für neue Geräte, nicht bei Austausch alter Geräte. Die Messtechnische Ausstattung zur Verbrauchserfassung (Zähler, Heizkostenverteiler) kann dabei durch Walk-by und Drive-by-Technologien abgelesen werden.

Alle Geräte müssen ab 1 Jahr nach in Kraft treten des Gesetzes mit anderen Systemen von anderen Anbietern kompatibel sein und Daten miteinander austauschen, das BSI entwickelt hierfür Technische Vorgaben. Die Geräte müssen an ein Smart-Meter-Gateway angebunden werden können.

Seit 2022 ist eine monatliche Informationspflicht gegenüber dem Nutzer notwendig.

Chancen und Herausforderungen

- Effizienz im Betrieb, zum Beispiel bei der Fahrstuhlkontrolle und -Wartung
- Effizienz beim Management des Lebenszyklus (Lifecycle) eines Gebäudes, zum Beispiel mittels durchgehend digitaler Planungsunterlagen für den Bau-, Umbau und den Rückbau von Gebäuden für einen lückenlosen Prozess- und Informationsfluss
- Effizienz bei dem Gebäudeenergieverbrauch, z.B. der bedarfsgerechten Heizung und Lüftung
- Mehrwerte entstehen z.B. durch den Einsatz von Sensorik für die Überwachung der Standfestigkeit bei Brückenbauwerken
- Sharing (Teilen) von Zustandsdaten ist beispielsweise die Vorrausetzung für den Austausch von Strom, Wärme o. ä. in der Nachbarschaft
- Neue Nutzerrollen und Zugriffsregelungen für die Gebäudetechnik schaffen Mehrwert für Betreiber, Verwalter und Nutzer

Herausforderungen:

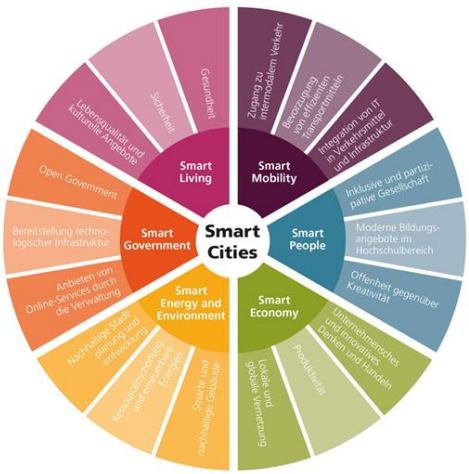
- Aufwand für Installation
- Fehlende Kompatibilität der Systeme
- Konfiguration und Wartung
- Ausfallsicherheit
- Starre Regeln statt intelligenter Systeme
- Sicherheitslücken
- Nutzerakzeptanz
- Neue Berufsbilder & qualifizierte Fachkräfte

Neue Ambient Assisted Living Berufsbilder:

- Bedarf an spezifischen Fähigkeiten in höherem Umfang
- Grundsätzliches Denken in Systemen
- Fähigkeiten zur Installation, Wartung und Programmierung von AAL-Systemen
- Fähigkeiten zur Verknüpfung von Einzelkomponenten und zum Schnittstellenmanagement
- Fähigkeiten zur Gewährleistung der Sicherheit von IT Betriebssystemen und ihren Komponenten
- Viele Verschiedene Berufe möglich

Smart City

Definition: Eine Stadt, die in den Bereichen **Wirtschaft, Menschen, Verwaltung, Mobilität, Umwelt** und **Wohnen** zukunftsweisende Leistungen erbringt und auf der intelligenten Kombination von Fähigkeiten und Aktivitäten selbstbestimmter, unabhängiger und bewusster Bürger aufbaut. Der Begriff "Smart City" bezieht sich allgemein auf die Suche und Identifizierung intelligenter Lösungen, die es modernen Städten ermöglichen, die **Qualität der für die Bürger erbrachten Dienstleistungen zu verbessern.**



Es gibt drei Normen zur Planung und Umsetzung von Smart Cities

Geschäftsprozesse

ISO/IEC 30145-1:2021 - Part 1: Smart city business process framework

Spezifiziert einen generischen Geschäftsprozessrahmen und identifiziert generische Geschäftsprozesse, die zwischen Smart Cities und kommerziellen Organisationen üblich sind

Wissensmanagement

ISO/IEC 30145-2:2020 - Part 2: Smart city knowledge management framework

Spezifiziert einen allgemeinen Rahmen für das Wissensmanagement. Erstellung, Erfassung, gemeinsame Nutzung, Verwendung und Verwaltung von Smart-City Wissen und enthält die wichtigsten Praktiken, die zur Sicherung der Nutzung von Wissen implementiert werden müssen

Technik

ISO/IEC 30145-3:2020 - Part 3: Smart city engineering framework

Spezifiziert ein Rahmenwerk, das in Schichten von IKT-Technologien gegliedert ist und enthält Zuordnung der IKT-Techniken zu verschiedenen Systemeinheiten, um die Geschäfts-, Wissensmanagement- und Betriebssysteme der Smart City aus technischer Sicht zu unterstützen.

Smart Living

Smart Living besteht aus den drei Punkten Gesundheit, Sicherheit und Lebensqualität und kulturelle Angebote.

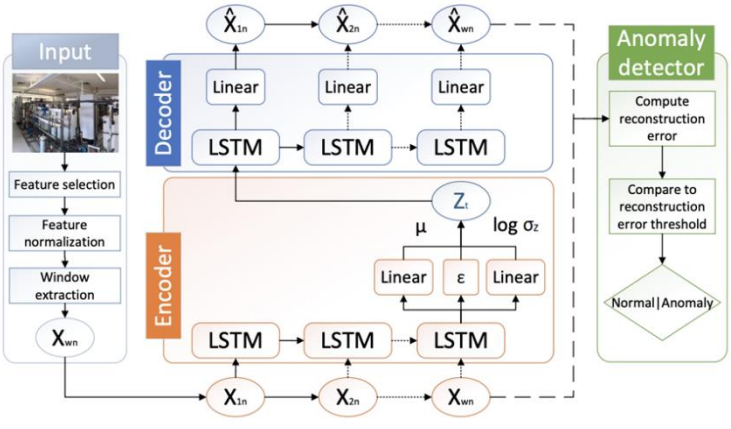
Gesundheit

Medizinische Überwachung, bessere Gesundheit durch Telemedizin, sichere Übertragung von privaten Daten und Monitoring ansteckender Krankheiten.

Durch zum Beispiel Vermeidung von Stromausfällen (Gesundheitliche Beeinträchtigungen Hitze und Kälte) und Überwachung der Luftqualität (Warnung vor schlechter Luftqualität) und Überwachung der Wasserversorgung, um Zugang zu sauberem Wasser zu gewährleisten, ausfallende Komponenten identifizieren und Anomalien detektieren.

Anomalie Detektion für kritische Infrastruktur

Erhöht die Sicherheit vor Cyber-Angriffen und für das Personal und verringert gleichzeitig Ausfallzeiten und Kosten durch Lokalisieren der Fehlerursachen.



Anomalie Detektion mit Autodecodern:

- Rekonstruktion des Inputs
- Encoder projiziert Input in niedrigdimensionalen Raum (Z)
- Decoder rekonstruiert den ursprünglichen Input $E_\phi: X \rightarrow Z, D_0: Z \rightarrow X$
- Optimierung nur mit normalen Daten, Anormale Daten können nicht akkurat rekonstruiert werden
- LSTM: Long Short-term Memory
- Einfaches Beispiel: Keras Deep Learning Autoencoder

Sicherheit

Durch Kriminalitätsvorhersagen (Datenbasiert, soll Polizeiarbeit erleichtern), Sicherheitssysteme (Wohnhäuser sicherer machen und kritische Infrastruktur schützen) und in Kommunikations- und anderer Infrastruktur durch Ausfallsicherheit (durch Redundanzen), Cyberrisikomanagement, Schulung von Personal und Nutzern, Schnittstellenstandards und Einhalten des Datenschutzgesetztes.

Smart Mobility

Zugang zu intermodalem Verkehr, Bevorzugung von effizienten Verkehrsmitteln durch Integration von IoT in Verkehrsmittel und Infrastruktur

Ziel dieser Integration ist Ressourceneinsparung, geringere Umweltbelastung, Zeiteinsparung und Sicherheit und Komfort.

Intelligente Ampeln steuern den Verkehrsfluss anhand Verkehrslage durch z.B. Induktionsschleifen und Schalter für Fußgänger aber auch die Umgebung (Sensoren in der Straße, Stau- und Positionsdaten, Statistische Auswertung)

Zugang zu Intermodalem Verkehr bei zwei oder mehr Verkehrsträgern, bei denen der Ladeinhalt das Verkehrsmittel wechselt bietet entlastete Verkehrsnetze und ein effizientes Verkehrswesen (Kosten- und Zeiteinsparung)

CAR2X-KOMMUNIKATION

Fraunhofer IOSB Projekt „IForsee“

- **Problem:** Autonome Fahrzeuge brauchen Informationen
- **Voraussetzung:** Viele vernetzte Fahrzeuge
- **Nutzer-Motivation:** Anwendung für kooperative Fahrfunktionen
- **Ziel:** Kooperatives Fahren ab 5-10% Vernetzung
- **Vorteile:** Erhöhung der Verkehrssicherheit; Effizienzsteigerung

Car2X besteht aus Car2Car und Car2Infrastructure Kommunikation.

Die Technische Grundlage bildet pWLAN (WLAN in Personen-KFZ) 5,9 GHz Funktechnik oder Cellular-C2X, Nachrichten werden per Unicast, Broadcast oder Geocast (Nachrichten in ein bestimmtes Gebiet) übertragen.

Anwendungsfälle: Engstellenassistent, Auffahrassistent und Einparkassistent

Smart People

Inklusive und partizipative Gesellschaft mit modernen Bildungsangeboten im Hochschulbereich und Offenheit gegenüber Kreativität

Smarticipate ist eine digitale Stadtplanung (häufig zu geringe finanzielle Ressourcen und Mangel an Expertise) mit Mitgestaltung und Mitspracherecht der Bürger

Partizipative Kommunikation: Entscheidungsprozesse unterstützen (Bürgerbeteiligung), Verfügbarkeit, Maßnahmen und Koordination und Einbindung öffentliche Behörden & Rettungsdienste (First-Responders)

Vorteile: 3D Stadt-Modell visualisieren und interaktive Analyse, mit Geodiensten-Integration und es sind keine Programmierkenntnisse notwendig

Mängelmelder: Eine interaktive Karte auf der Bürger Mängel eintragen können, die dann zur Verbesserung der Stadt führen soll.

Smart-City-Initiativen können sich auf staatlicher und privater Ebene finanziell rentieren. Beteiligung der Privatgesellschaft erhöht die Akzeptanz von Smart-City-Technologien und die Kreativität.

Smart Economy

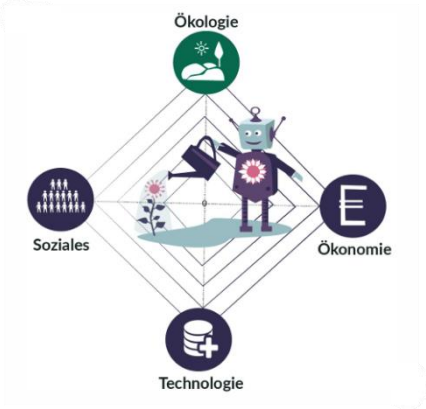
Unternehmerisches und innovatives Denken und Handeln mit dem Ziel Steigerung der Produktivität durch Lokale und Globale Vernetzung

Produktivität: Smart City als Technologieführer: Installation und Wartung von Smart-City-Projekten durch Fachpersonal. Viele Technologien unterstützen die Wirtschaft durch z.B. Verbesserung des Transportwesens, Schaffung von Arbeitsplätzen, Gewährleistung von Warenfluss und E-Business und E-Commerce

Lokale und Globale Vernetzung: Smart-City-Technologien fördern Kooperationen zwischen öffentlichen und privaten Einrichtungen, um Initiativen zu gründen und um flexibler auf Änderungen zu reagieren

Smart Energy & Environment

Nachhaltige Planung und Entwicklung von smarten und nachhaltigen Gebäuden und Ressourcenschonung und erneuerbare Energien



Nachhaltigkeitsraute: Designprinzip und Wirksamkeitsmaßsystem ist im Vorhinein anzuwenden und wird auf Handlungsfelder in der bürgerfreundlichen Stadtplanung angewandt.

Ökologie: Umweltressourcen berücksichtigen, Energie und Verschmutzung reduzieren

Ökonomie: Finanzielle Ressourcen berücksichtigen, Effizienz und Effektivität steigern, Tragfähige Geschäftsmodelle suchen, nicht allein auf monetäre Aspekte reduzieren

Technologie: Soft- und hardwarebedingte Ressourcenverbräuche reflektieren, Nachhaltige Software-Entwicklung berücksichtigen, Standardisierung und Interoperabilität sicherstellen

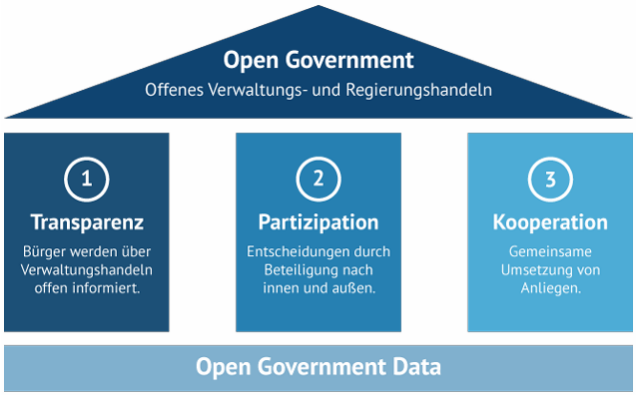
Soziales: Verlässlichkeit, Sicherheit und Vertrauen berücksichtigen, Akzeptanz und Legitimation durch Beteiligung und Wissen fördern, Soziale Folgen wie Beschäftigungseffekte berücksichtigen

Konsumenten übernehmen Aufgaben des Produzenten → Trend “Eigenstrom in der intelligenten Stadt”, **Eigenstrom generieren** und ins öffentliche Netz einspeisen durch Photovoltaikanlagen und Kleinwindenergieanlagen.

Problem: Lastspitzen durch hohe Bevölkerungsdichte, Lösung Smarte Geräte und Smart Meter

Beleuchtung spielt eine wichtige Rolle für Energieeffizienz, Moderne, smarte Straßenleuchten können unter anderem folgende Features haben: Bewegungssensoren, Meldung von Parkplätzen, Ladesäulen für Elektroautos, Freies Internet, Notrufeinrichtungen, Integrierte Umweltsensorik.

Ladesäulen verwenden Elektrofahrzeuge als Speicher und Verbraucher, so können Lastspitzen ausgeglichen werden und regenerative Quellen verwendet werden.



Smart Government

Open Government durch bereitstellen technologischer Infrastruktur und Anbieten von Online-Services.

Beispiele für Online Services:

Problem	Lösung	Vorteile
Deutschland – Datengestützte Fangquotenüberwachung		
• Umsetzung von EU-Vorgaben • Verteilte Datenbestände • Medienbrüche • Manuelle Stichproben	• Datenplattform Fischerei-Informationstechnologie (FIT) • Übergreifende Fischereikontrolle in Echtzeit	• Zusammenführung von Datenbestände • Überwachung von Fischereifahrzeugen • Erhöht Effizienz der Kontrolleure • Maßnahmen gegen Fangquotenverstöße
USA – Sichere Schulwege in Los Angeles		
• Verkehrsunfälle 20% Schulkinder	• Vision Zero Initiative • Identifizierung von Risikostraßen	• Identifizierung von Hochrisikostraßen • Verbesserung der Straßensicherheit • 0% Verkehrstote bis 2025
Schweden– Schnelles und fehlerfreies Bearbeiten von Sozialhilfeanträgen		
• Komplizierte Anträge • Viele Behörden involviert • Prüfung durch Sachbearbeiter	• Datenplattform SSBTEK • Automatischer Abruf von Informationen	• Zeiteinsparung Kunden und Behörden • Einholen und Verifizieren von Daten • Reduzierung der Fehlerquote • Weniger Betrug

Technik & Konflikte

Wie verändert die Technik unser Leben? Am Ende hilft die beste Technik nicht bei Konflikten, Technik fördert Kommunikation. Der Mensch sollte im Vordergrund stehe, vor allem Personen mit eingeschränkten Handlungsfähigkeiten.

Beispiele:

Technik	Situation	Konsequenzen /Lösung	Konflikt
Autonome Autos	Kinder stoppen autonome Autos	Straße betreten verboten, Rückbau zur Autogerechten Stadt	Kinder dürfen Straßen nicht ohne Eltern betreten
Heinerleiner App	Fahrten per App buchen, zahlen per Kreditkarte, Senioren besitzen kein Smartphone und keine Kreditkarte	Kundenkonto im Kundenzentrum mit Guthaben und per Telefon buchen	Senioren sind benachteiligt

Gesundheitsversorgung

Fallbeispiel Pflege:

- Organisiert durch Medizinische Pflege in Krankenhäuser, stationäre Pflegeheime, häusliche / ambulante Pflege
- Pflege wird durch Angehörige, Pflegehilfskraft und Pflegefachkräfte geleistet
- Die Pflege wird bezahlt von Pflegekassen, Unfallkassen und Angehörigen
- Der Pflegegrad entscheidet, welche Zuschüsse Versicherte durch ihre Pflegekasse erhalten

AmI kann Pflege unterstützen durch Ambient Assisted Living / Active Assisted Living (AAL)

Ambient Assisted Living

AAL umfasst Methoden, Konzepte, (elektronische) Systeme, Produkte sowie Dienstleistungen, welche das alltägliche Leben älterer und auch behinderter Menschen situationsabhängig und unaufdringlich unterstützen.

Die verwendeten Techniken und Technologien sind nutzerzentriert, also auf den Menschen ausgerichtet und integrieren sich in dessen direktes Lebensumfeld. Die Technik passt sich folgerichtig an die Bedürfnisse des Nutzers an.

Der Begriff AAL ist **nicht eindeutig definiert** oder geschützt, es wird aber an einer Norm gearbeitet. Aktuell gibt es nur wenige zugelassene/geprüfte Geräte.

Smart Home und Follow Me Features

- Nacht Beleuchtung mit Lokalisierung und Tracking Funktionalität
- Raum Temperatur Regelung bei Präsenzdetektion
- Diese Funktionalität zielt auf bessere Komfort und mehr Energie Effizienz
- Räumlichkeiten müssen mit Sensoren und Aktoren ausgestattet sein.

Ambient Sensorsysteme

Smart Floor: siehe Kapitel Anwendungen.

Verwendungszweck: Lokalisierung, Sturzerkennung, Ganganalyse, Verhaltensanalyse, Aktivitätsanalyse

→ Hat eine hohe räumliche Auflösung, ist nicht im Weg, Privatsphärefreundlich und kein Line-of-Sight notwendig aber großer Installations- und Wartungsaufwand.

Smart Furniture: siehe Kapitel Anwendungen

Verwendungszweck: Emotionsanalyse, Anwesenheitserkennung, Aufsteherkennung, Assistenz für orthopädische Übungen

→ Kann viele Vitalwerte erfassen und nicht vergessen werden aber hat einen stationären Anwendungsort

EmotionalAI

Research an **Schmerzdetektion von Demenzpatienten** anhand der Mikro-Gesichtausdrücken von Videodaten.

Demenzpatieten können auf Grund ihrer Krankheit oft **nicht mehr selbst klar ausdrücken**, wann sie Schmerzen haben. Diese Tools sollten den Ärzten helfen, diese besser einzuschätzen.

Jedoch ist es schwierig die Mikro Expressions zu detektieren, weil die Bewegungen der Gesichtszüge minimal sind. → Mögliche Lösung durch Fusion von Audio-Daten

Activity of Daily Living#

Aktivitäten des täglichen Lebens (ADLs) wird von Fachleuten des Gesundheitswesens verwendet, um auf die grundlegenden Selbstversorgungsaufgaben zu beziehen, die eine Person tagtäglich ausführt.

Die Fähigkeit oder Unfähigkeit einer Person, ADLs auszuführen, wird von Ärzten häufig als Mittel zur **Messung der Selbständigkeit** genutzt.

Embedded Sensoren zur ADL-Detektion: Physiologisches Monitoring von Patienten, KI-basierte Signal- und Datenverarbeitung. Und die intelligente Vernetzung und Visualisierung der Daten.

Wearable Device: DHCPCare

- Sensorbasiertes Patientenmonitoring und individuelle Therapiemodelle auf Basis von Clinical Grade Wearables
- Herzfrequenz und -intervall zwischen zwei Herzschlägen geben Hinweise auf das Stressniveau
- Körpertemperatur geben Hinweise auf das Wohlbefinden

Wearable Device: CardioTEXTILE

- Mehrkanal-EKG integriert in Textilien für eine kontinuierliche und zuverlässige Detektion von Herzrhythmusstörung
- Herzrhythmusstörung können in schlimmsten Fällen zu Schlaganfällen führen. Eine frühzeitige Erkennung und Warnung können somit Leben retten.
- Herausforderung: technische Umsetzung für eine genaue Signalerfassung in medizinischer Qualität

AmI in Krankenhäusern/Institutioneller Pflege

Pflegedokumentation:

- Bei der Dokumentation der Pflegefortschritte handelt es sich um eine begleitende Maßnahme, die bei allen Pflegeleistungen im Pflegeverlauf erbracht werden muss
- Das Sozialgesetzbuch (SGB) verlangt in § 137 eine Qualitätssicherung in Form einer Pflegedokumentation.
- Pflegedokumentation ist haftungsrechtlich relevant
- Fehler in der Pflegedokumentation können (gesundheitliche) Schäden verursachen
- Automatisierung in der Dokumentation kann den hohen zeitlichen Aufwand reduzieren.

Körpernahe Sensoren

Pflegebett: Zentrales Möbel im Pflegezimmer, Ausstattbar mit **Technologien** für Aufstehhilfe, Dynamische Sitz- und Liegepositionen, Aufsteherkennung → Nachtlicht, Schwesternruf, Posen- und Aktivitätserkennung, Dekubitusprophylaxe, Anfallerkennung bei Epilepsiepatienten, Feuchtigkeitssensorik

Herausforderungen:

- Notwendige Strom- / Datenversorgung
- Fehlalarme/Diagnosealarme durch Lösen der Kabelverbindungen
- Entstehen von Stolperfallen
- Verrutschen von Einlagen

Exoskelett: Unterstützt Pflegekräfte bei Trag- und Hebetätigkeiten, kann bei Patienten Motorik wiederherstellen und therapiebegleitend eingesetzt werden. Der Vorteil ist eine geringe körperliche Belastung aber die Nachteile sind eine fehlende Akzeptanz, und die Anschaffungs-, Vorbereitungs- und Wartungskosten

Robotik

- Serviceroboter für sekundäre Pflegetätigkeiten (Hol- und Bringdienste)
- (Humanoide) Interaktionsagenten

Optische Assistenzsysteme

Optische Medikationskontrolle: Optische Erkennung von Tablette beim Stellen von Medikamenten, Automatisierter Abgleich mit Medikationsplan, Hinweise bei Fehlmedikation, Dokumentation

Optisches Tracking und Monitoring: Diskrete optische Erfassung und Analyse des prä- und postoperativen Patientenverhaltens

Erfassen von:

- Allgemeines Aktivitätsverhalten
- Tracking von Erfolgskontrolle von therapeutischen Übungen
- Flüssigkeits- und Nahrungsaufnahme
- Einnahme von Medikamenten
- Puls
- Emotionen, Schmerz

Erfassung und Unterstützung von interventionellen Prozeduren im OP: Gekoppeltes Tracking – rauminstalliert und mobil – von Instrumenten und Personen, mit IR-Kameras und ArUco-Markern und Objekterkennung

Zweck:

- Navigationsunterstützung bei Interventionen
- AR-Anwendungen für Diagnose und Eingriffe
- Instrumentenverfolgung und –zählung („nothing left behind“)
- Erfassung von Abläufen: Personenbewegungen, Gerätestandorte, Instrumentenübergabe, allgemeine Behinderungen des Ablaufs

Weitere Assistenzsysteme

Rufanalage: Zweck ist das Herbeirufen von Pflegepersonal, ist ein genormtes Bauteil, welches eine eigene Spannungsversorgung hat und manuelle Bedienung benötigt und darf nur durch Fachkräfte eingebaut werden.

Steuerplattform: Steuerplattform, für verbinden der Rufanlage, Steuerung der Pflegezimmer & Station, Datenaggregation, Gebäudeautomation, Situationserkennung, Notrufbehandlung, Notfallabschaltung, Prozessvisualisierung, Leitstand und Dokumentation

Digitaler Zwilling: Derzeitiger Fokus vor allem auf Digitalen Zwillingen für Industrie 4.0 und zunehmendes Interesse an Digitalen Avataren auf Basis von individuellen Daten und Kohortenwissen ergänzt um Prozessmodelle

Telemedizin: Telemedizin ist ein Teilbereich der Telematik im Gesundheitswesen und vereinfacht die Diagnostik und Therapie zwischen Arzt, Therapeut, Apotheker und Patienten trotz einer räumlichen oder auch zeitlichen Distanz.

Medizinprodukte

Medizinprodukte sind Produkte mit **medizinischer Zweckbestimmung**, die vom Hersteller für die **Anwendung beim Menschen** bestimmt sind.

Dazu gehören Implantate, Produkte zur Injektion, Infusion, Transfusion und Dialyse, humanmedizinische Instrumente, Software, Katheter, Herzschrittmacher, Dentalprodukte, Verbandstoffe, Sehhilfen, Röntgengeräte, Kondome, ärztliche Instrumente, Labordiagnostika, Produkte zur Empfängnisregelung sowie In-vitro-Diagnostika.

Medizinprodukte sind auch Produkte, die einen Stoff oder Zubereitungen aus Stoffen enthalten oder mit solchen beschichtet sind, die bei gesonderter Verwendung als Arzneimittel oder Bestandteil eines Arzneimittels (einschließlich Plasmaderivate) angesehen werden und in Ergänzung zu den Funktionen des Produktes eine Wirkung auf den menschlichen Körper entfalten können.

Anders als bei Arzneimitteln, die pharmakologisch, immunologisch oder metabolisch wirken, wird die bestimmungsgemäße **Hauptwirkung** bei Medizinprodukten **primär auf physikalischem Weg** erreicht.

Zulassung: Zertifizierungsstellen (Benannte Stelle) prüfen die Voraussetzungen für die Zulassung des Medizinprodukts, keine Produktprüfung, **nur Bewertung**, ob Hersteller alles unternimmt, um ein **sicheres Medizinprodukt herzustellen**. **Danach analysiert** das Bundesamt für Arzneimittel und Medizinprodukte die **Risiken** und entscheidet über die Aufnahme in Verzeichnisse für Medizinprodukte bzw. DiGA (Digitale Gesundheitsanwendungen).

Gesundheitsversorgung

Digitalisierung in Gesundheit und Pflege kann den Menschen nicht ersetzen, neue Technologien können unterstützen und die Gesundheitsversorgung verbessern.

Herausforderungen:

- Starke bzw. fehlende Reglementierung
- Silo-Bildung und fehlender Austausch zwischen den Systemen
- Engineers are from Venus and doctors are from Mars
- Budget- und Ressourcenverantwortung
- Fehlende Daten und Evidenz

Benutzerinteraktion

Benutzerschnittstelle (User Interface (UI)): alle Bestandteile eines interaktiven Systems, die Informationen und Steuerelemente zur Verfügung stellen, die für den Benutzer notwendig sind, um eine bestimmte Arbeitsaufgabe mit dem interaktiven System zu erledigen

Benutzererlebnis (User Experience (UX)): alle Emotionen, Gedanken, Einstellungen, Wahrnehmungen, physische und psychologische Reaktionen, Verhaltensweisen und Ergebnisse, die vor, während und nach einer Nutzung bei einer Person auftreten

Human Computer Interaction (HCI) beschäftigt sich mit dem Entwurf, der Bewertung und der Implementierung interaktiver Computersysteme für die menschliche Nutzung und mit der Erforschung der sie umgebenden Phänomene

Interaktionsmodell

Konzeptionelles Modell: Mentales Modell, wie das Produkt funktioniert, entsteht durch Erfahrung, Übung und Anleitung

Das Interaktionsmodell ist ein konzeptionelles Modell bestehend aus Affordances, Sichtbarkeit, Mapping und Feed-Forward und Feedback.

Affordance (Aufforderungscharakter): Ein Interaktionselement muss aus sich und seiner Gestaltung heraus kommunizieren, wie es zu nutzen ist und welche Konsequenzen seine Nutzung wahrscheinlich für den Systemstatus (und damit für die Ziele der Nutzer) haben wird. Affordances bieten starke Hinweise, wie etwas benutzt werden muss, sodass auf weitere Erklärungen („PUSH/PULL“) verzichtet werden kann.

Sichtbarkeit: Sichtbarkeit von in den Hintergrund gerückten Sensoren durch Percieved Affordances (gelernte konventionen), Feed-Forward Mechanismen und Feedback-Mechanismen

Mapping: Die Verbindung von UI-Elementen mit der realen Welt erleichtert 4 das Verstehen und das Erinnern daran, wie etwas bedient werden muss.

Feedback: Informationen, die helfen, das Geschehene zu verstehen

Feed-Forward: Informationen, die helfen, Fragen der Ausführung zu beantworten

Regeln für gutes Design

1. Streben nach Konsistenz
Ähnliche Situationen sollten ähnliche Abläufe/Ausführungen haben. Gleiche Terminologie, gleiches Layout,…
Nutzer erwarten, dass das Programm sich ähnlich verhält und sie auch neue Aufgaben ohne tiefgehende Erklärung lösen können. Nutzer wollen nicht überrascht (verwirrt) werden.

2. Universelle Benutzbarkeit
Bedürfnisse unterschiedlicher Benutzer berücksichtigen. Personalisierung ermöglichen, Abkürzungen für Expertennutzer erlauben
Barrierefreiheit, leichter Übergang von bewusster zu intuitiver Bedingung ermöglichen.

3. Informatives Feedback
Rückmeldung für jede Aktion des Benutzers, besonders bei seltenen und größeren Aktionen.
Nutzer wollen wissen, was gerade passiert, Statusmeldung, vor allem, wenn etwas schief geht!

4. Dialoge sollten zu einem Abschluss führen
Handlungsabläufe sollten zu einem klaren Abschluss führen und dann Feedback geben.
Interaktion beginnt und endet bewusst, Gefühl der Erleichterung, Vorbereitung auf nächste Interaktion.

5. Design zur Fehlervermeidung
Fehler (vor allem größere) sollten durch das Design bereits vermieden werden und eine Wiederherstellung erleichtert werden.
Kalender zur Datumsauswahl statt Eingabefenster.

6. Einfaches „Rückgängigmachen“ von Aktionen
Aktionen sollten so weit wie möglich umkehrbar sein. Nimmt auch Ängste des Benutzers und lädt zum Erkunden unbekannter Optionen/Funktionen ein.

7. Kontrolle bleibt beim Benutzer
Vor allem Expertenbenutzer wollen das Gefühl, die Schnittstelle kontrollieren zu können.
Keine Überraschungen, zusätzliche Hindernisse oder Änderungen im gewohnten Verhalten.

8. Reduzierung der Belastung des Kurzzeitgedächtnisses des Benutzers
Der Nutzer sollte (und will) sich keine Informationen merken müssen.
Transferieren von bereits eingegebenen Daten, Sachen anzeigen, Kontext!

Interaktionsarten und Modalitäten

Explizite Interaktion: Explizite Interaktion zielt auf die direkte Interaktion zwischen Benutzer und Geräten ab. Der Benutzer initiiert eine direkte Aktion und erwartet eine zeitnahe und entsprechende Reaktion vom Gerät.

Implizite Interaktion: Implizite Interaktion benutzt passive, unaufdringliche Beobachtung des Benutzers über längere Zeit und reagiert dann entsprechend

Modalitäten ist die Art und Weise wie interagiert werden kann, Ein- und Ausgabe.

Werden verschiedene Modalitäten in der Schnittstelle Mensch-Maschine parallel verwendet, spricht man von **multimodaler Interaktion.** Es gibt drei Arten von multimodaler Interaktion:

Komplementär: Vermeidet Redundanzen und erlaubt natürliche Art der Interaktion, kann aber Probleme durch Widersprüche erzeugen

Alternativ: Auswahl einer geeigneten Modalität, aus einer Reihe von möglichen Modalitäten mit Informationsverlust

Redundant: Verschiedene Modalitäten zur gleichen Zeit für die gleiche Interaktion

Merkmale eines Ambient-Intelligence-Interaktionssystems:

- Vielzahl an Sensoren & Aktoren
- Interaktion erfolgt häufig/meist implizit
- Systeme haben Verständnis der eigenen Funktionalität, der Umgebung und der aktuell vorherrschenden Situation
- Systeme nehmen die Umgebung über Sensoren wahr und interpretieren die Daten als Verhalten des Benutzers

Aktuelle Forschungsbereiche

Robotic Interfaces: “Roboter”, um die menschliche Wahrnehmung zu verbessern. Zwei-direktionale, transparente HCI: Afferent (sensorisch) und Efferent (motorisch)

Verarbeitung von Gebärdensprache: Gebärdensprachen sind visuelle Sprachen mit komplexem Vokabular und Grammatik, die vor allem unter Gehörlosen verbreitet sind. Aktuelle Arbeiten befassen sich mit Computer Vision-basierter Gebärdenerkennung und der automatisierten Übersetzung in gesprochene Sprache.

Affective Computing: Erforschung und Entwicklung von Systemen mit Fähigkeiten, menschliche Emotionen zu detektieren, zu interpretieren, zu validieren und zu stimulieren

Forschung am Fraunhofer IGD

Digital Signage: Interaktive Display mit personalisierten Werbungen, Individualisierung/Group Individualisierung durch soft-biometrische Charakteristiken, Vorhersage von soft-biometrischen Charakteristiken aus Gesichtsbilder für die Personalisierung

Augmented & Virtual Reality Machine@Hand:

- AR führt Nutzer mithilfe von visuellen Anweisungen durch Wartungs- und Montagetätigkeiten, Blick in das Innere der Maschinen durch AR möglich
- VR, um am virtuellen Abbild der Maschine zu üben, auch wenn Maschine physisch nicht am Ort, Praxisnahes Lernen für Aus- und Weiterbildung

Brain Computer Interface: EEG- (Elektroenzephalogramm) Signale zur Steuerung von Anwendungen, Soziale Interaktion in der digitalen Gemeinschaft → z.B. Steuerung von VR-Spielen, Inklusion von Personen mit eingeschränkter Mobilität

Context Awareness

Geräte **erkennen das Benutzerziel** und kommunizieren untereinander, um die Strategie und die Ausführung zu übernehmen. Z.B. morgens nach dem Wecker geht das Licht automatisch an und ein Kaffee wird vorbereitet.

Context-Awareness bedeutet Kontextabhängigkeit, das Scenario stellt ein anderes Paradigma der Verwaltung von Umgebungsdaten dar (weg vom konventionellen, stationären Desktop-Paradigma hin zu überall und jederzeit Informationen mit einem leichten mobilen Gerät erhalten). Der Zugriff auf die Informationen und Informationsdatenbanken erfolgt **nicht an einem einzigen Ort** und in einem einzigen Kontext, sondern in einer **Vielzahl von Situationen und Orten** wie Büro, Flugzeug, Besprechungsraum, zu Hause usw.

Wandlung von **Content-Based** Datenzugriff zu **Context-Based** Datenzugriff.

Verschiedene Kontextinformationen können bei der Datenverwaltung helfen den Informationsbedarf der Nutzer/innen besser zu verstehen und ihnen zu helfen, **das Beste aus den Daten zu machen**.

Der Kontext bietet Hinweise wie Datenfragen optimal bearbeitet werden können, da sie eine Art **Semantik in Bezug auf das Was, Warum, Wann, Wo und Wie der Datenquellen** darstellen und so kann das Verständnis zwischen Datenverwaltung und Nutzern/innen bereichert werden.

Eigenschaften:

- Ubiquitous (allgegenwärtig)
- Transparent (unsichtbar)
- Sensitive (wahrnehmend)
- Responsive („mitdenkend“ und Reaktiv)
- Adaptive (angepasst an Menschen und deren Situationen)
- Intelligent (weil es nach Wahrnehmung adaptiv reagiert)

Herausforderungen

- Wie können wir die Datenverwaltung durch Kontextbewusstsein **anpassungsfähiger**, **reaktionsfähiger**, **personalisiert**, **dynamisch** und **vorausschauend** machen, wie es von AmI beschrieben wird?
- Wie lassen sich kontextbezogene **Informationen erfassen**, **kategorisieren**, **modellieren** und **schützen**, um sie in die Datenverwaltung einzubringen?
- Wie kann man den Benutzern kontextbezogene **Datenmanagement-Unterstützung bieten**?
- Wie kann man eine benutzerfreundliche und **leicht zu bedienende** kontextbezogene **Abfragesprache** für die Benutzer entwickeln?
- Wie kann man **effektiv und effizient** mit den Nutzern interagieren, wenn es ein kleines Gerät mit einer **begrenzter Rechenleistung und Energieversorgung ist**?

Kontext und Context-Awareness

Definition Kontext (Linguistisch): inhaltlicher Gedanken-, Sinnzusammenhang, in dem eine Äußerung steht, und Sach- und Situationszusammenhang, aus dem heraus sie verstanden werden muss.

Definition Kontext: Kontext ist jede Information, die zur Charakterisierung der Situation einer Entität (einer Person, eines Ortes oder eines Objekts) verwendet werden kann.

Definition Context-Aware: Ein System ist kontextbewusst (context-aware), wenn es den Kontext nutzt, um dem Benutzer relevante Informationen und/oder Dienste anzubieten, wobei die Relevanz von der Aufgabe des Benutzers abhängt.

Context: Aus der Sicht eines AmI-Systems sind Daten, die innerhalb eines Systems auf der Grundlage einer Reihe gemeinsamer Modelle (Shared Models) gemeinsam genutzt werden können.

- Was passiert gerade? Was sind die wichtigen Parameter?
- Wer interagiert mit dem System? Wer benutzt das System?
- Wann passiert es?
- Wo befindet sich der Benutzer? Wo passiert etwas?
- Wie interagiert der Benutzer?

Mögliche Kontextinformationen können **generell** (Benutzer und die Situation, in der er sich befindet, Umgebung und die Situation in dieser Umgebung) oder **konkret** (Ort, Zeit, Datum, Identität, Emotionaler Zustand) sein.

Context-Awareness: ist die Qualität der Nutzung relevanter Teile des Kontextwissens bei der Ausführung von Handlungen in der virtuellen Welt.

Reasoning: Nutzung des Kontexts zur Erleichterung des Kontextbewusstseins (Context Awareness), z. B. Ableiten und Hinzufügen neuer Fakten zum Kontext.

Kontext-Kategorisierungsmöglichkeiten

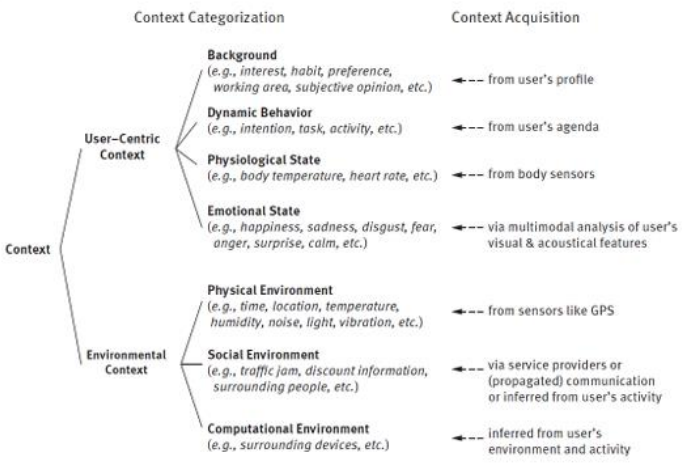
Konzeptionelle Kategorisierung

Extern (physikalisch):

- Von Hardware gemessen, z.B. Bewegung, Temperatur, …
- Von Hardware gesteuert, z.B. Licht, Sound, …

Intern (logisch):

- Spezifiziert durch den Benutzer oder Administrator (z.B. Profil)
- Von Applikationen stammend (z.B. Kalender)
- Abgeleitete Informationen (Reasoning)



Operationelle Kategorisierung

Auf der Grundlage der Art und Weise, wie Kontextinformationen erfasst, modelliert und behandelt werden:

- Erfasster Kontext
- Statistischer Kontext
- Profilierter Kontext
- Abgeleiteter kontext

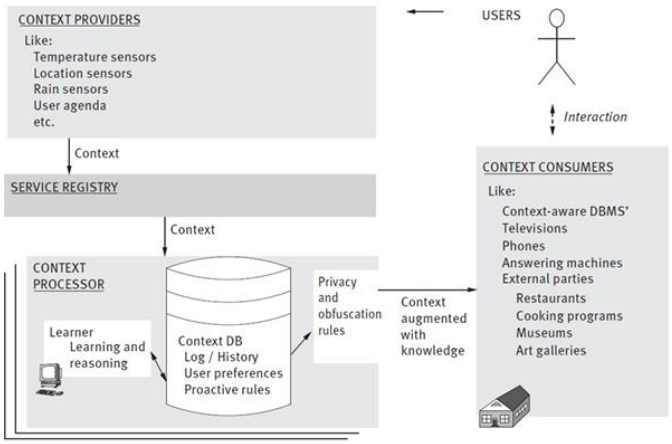
Kontext Eigenschaften

Erfassung von Kontextinformationen findet zwischen **verteilten Quellen** in einer **mobilen Umgebung** statt. Die Eigenschaften des Kontexts werden in hohem Maße durch die Art und Weise seiner Erfassung bestimmt:

- **Sensorisch erfassbar**
- **Limitiert durch eingeschränkte Geräte** → Stromverbrauch durch Kommunikation bzw. Datenverarbeitung
- **Verteilt auf verteilte Datenquellen** → braucht Aggregation der Daten
- **Kontinuität vs. kontinuierlicher Wandel des Nutzerkontexts** → verursacht enorme Datenmengen, die gespeichert werden müssen, komprimiert und diskretisiert werden, was zur Ungenauigkeit der Daten führt
- **Mobilität** → Objekte, von denen man Kontextinformationen erhält → Neue Informationsquellen, unbekannte Umgebung
- **Zeitlichkeit und Räumlichkeit**
- **Unvollkommenheit und Ungewissheit:** die erworbene Kontextinformationen sind nicht perfekt
    - **Unbekannt** - es liegen keine Informationen über die bestimmte Eigenschaft vor
    - **Zweideutig** - es liegen mehrere verschiedene Informationen über die gleiche Eigenschaft z.B. Ortung per GPS und per WLAN
    - **Unpräzise** - Die gemeldeten Informationen sind korrekt, aber zu ungenau, z.B. Ortung im Gebäude vs. Raum
    - **Fehlerhaft** - Die Informationen stimmen nicht mit den tatsächlichen Informationen überein

Kontextabhängige Datenverwaltung

Kontextbezogenes Datenmanagement besteht aus vier Hauptkomponenten: Den Kontextanbietern, Dienstregister, Kontextprozessor und Kontextverbraucher



Kontextanbieter (Context Provider)

- Bereitstellung des Kontext in Form von Diensten → unterschiedliche Kontextinformationen werden von unterschiedlichen Diensten geliefert
- Durch Wechselbeziehung können zuverlässigere Informationen erhalten werden
- Dienste bieten auch Metadaten zu den Kontexten ▪ Dienste tragen zu Wahrung von Sicherheit und Privatsphäre bei

Dienstregister (Service Registry)

- Ermöglicht Kommunikation zwischen Context Provider und Context Processor
- Verteilte Context Provider registrieren sich beim Service Registry
- Context Processors greifen auf die Informationen zu indem sie Requests starten
- Dynamische Abmeldung von Diensten → dynamischer Verbindungsaufbau (Mobilität, steter Wandel)
- Bietet Konvertierungsdienste, die mit alternativen Darstellungen unter Verwendung von Metadaten umgehen können

Kontextprozessor (Context Processor)

- speichert und protokolliert einige der vergangenen, gegenwärtigen und zukünftigen Kontextinformationen in Bezug auf einen Benutzer, Umgebungen und entsprechende frühere Aktionen des Benutzers in einer Kontextdatenbank
- Stellt Konsistenz bei dynamischem Verbindungsaufbau sicher
- Daten werden zum Lernen und Reasoning genutzt z.B. können aus Verhaltensweisen proaktiv Regeln erstellt werden, Nutzerin kann diese ändern und auch einen Accuracy-Wert setzen, ab dem die Regel erst greift, → Nachvollziehbarkeit
- Output wird bearbeitet und verschleiert, um die Privatsphäre zu wahren

Kontextverbraucher (Context Consumer)

- sind entweder kontextbewusste Datenverwaltungssysteme oder Dritte (z.B. Restaurants, Museen, Maschinen)
- z.B. ein kontextabhängiges Multimedia Datenbanksystem, das alle Videos und Szenen speichert, die man zuvor gesehen hat

Kontext Eigenschaften werden von verschiedenen Komponenten adressiert

Characteristic	**Context Provider**	**Service Registry**	**Rules**	**Learner**	**Context Database**
Being sensed	X				
Through constrained devices	X				
From distributed sources	X	X			
Continuous change	X	X			
Mobility	X	X			
Temporality and Spatiality	X		X	X	
Imperfectness and uncertainty	X		X	X	

Implikationen des Context-Awareness die von verschiedenen Komponenten adressiert werden

Implication	**Context Provider**	**Service Registry**	**Rules**	**Learner**	**Context Database**
Adaptiveness and personalization			X		
Privacy and security	X	X	X		X
Proactiveness			X	X	
Tracability			X		
Dynamic connection		X			X
Interrelationship	X				
Learning and reasoning				X	
Alternative representations		X			
Meta data	X	X	X	X	
Storage and logging					X

Kontextmodellierung

Die Modellierung des Kontexts ist der erste Schritt zur Entwicklung kontextbezogener Computersysteme und Anwendungen. Sie bestimmt die **Organisation** und die **Art des Zugriffs** auf Kontextinformationen in kontextabhängigen Anwendungen.

Methoden: Key-Value; Entity-Relationship; Objektorientierung; Markup-Schema; Logik; Ontologie

Perspektive:

- **Entitäten:** Orte (Räume, Gebäude), Personen (Individuen, Gruppen), Rollen (Assisted Person, Caregiver, Administrator, Verwandte), Dinge (physikalische Objekte, Computerkomponenten)
- **Attribute von Entitäten:** Identitäten (jede Entität hat ein eindeutige ID, z.B. URI), Orte (Position einer Entität, Nähe zu anderen Entitäten), Zustand / Status / Aktivität
- **Zeit:** Aktuelle Zeit und Zeitpunkt von relevanten Ereignissen

Key-Value

- Einfache Datenstruktur, z.B. können Informationen (wie Ortsinformationen) als Umgebungsvariablen den Applikationen zur Verfügung gestellt werden
- z.B. “Location:campus” beschreibt das das Kontext Element Location den Wert campus annimmt
- Rekursion anwendbar: “Address:(Building:FIT, Room:216)”
- **Pro:** einfach zu verwalten, weit verbreitet auf Grund der Einfachheit
- **Con:** keine Möglichkeit für komplexe Strukturen, keine inhärente Modellierungsmöglichkeit für die Keys und deren Bedeutung, Schwäche bei verteilten Kontextinformationen

Entity-Relationship

Erweitert die Key-Value Struktur um

- Entitäten: beschreiben ein physisches oder konzeptuelles Objekt
- Attribute: Eigenschaften von Entitäten
- Assoziationen:
    - Uni-direktionale Links zwischen Attributen und Entitäten
    - “Behauptungen” zwischen Attributen und Entitäten
    - Kontextbeschreibung = Sammlung an Behauptungen

Objektorientierung

- Ermöglicht Verkapselung und Wiederverwendung von Kontextinformationen
- Abstrahiert und kapselt einen oder mehrere physische oder logische Sensoren. Wenn neue Sensoren mit anderen Eigenschaften vorhanden sind, werden nur Änderungen an den beteiligten Merkmalen vorgenommen
- Definiert auf abstrakte Weise Klassen, Objekte, Typen und Instanzen für Instanzen für Kontextinformationen
- Modellierungssprachen wie ORM (Object-Role Modeling Language) und UML (Unified Modeling Language) beschreiben Kontextinformationen
- **Pro**: einfache Integration und Fusion von verteilten Kontextquellen und generische Struktur, hohe Flexibilität
- **Con:** schwierig zu verwenden bei großen Modellen

Markup Scheme

- Hierarchische Datenstrukturen durch Markup-Tags mit Attributen und Content
- Basiert meist auf der Serialisierung von einem Derivat der Standard Generic Markup Language (SGML)
- Oft verwendet für Profile, Konfiguration
- Beispiel: XML (eXtensible Markup Language)
- kann die Anforderungen an partielle Verifikation und Anforderungen an den Formalismus gerecht werden
- **Pro:** komplexere Strukturen möglich

Logik

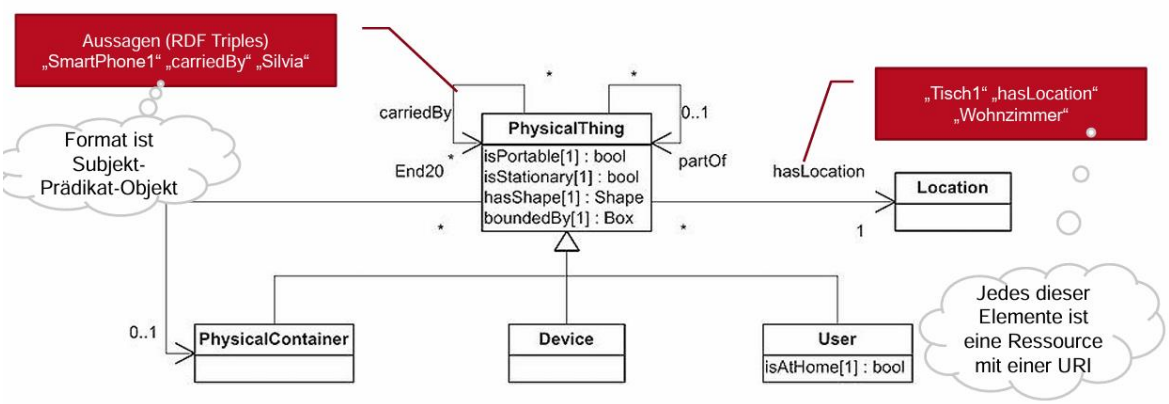
- Kontextinformationen in der Regel in Form von Fakten, Ausdrücken und Regeln definiert
- Weitere Fakten und Ausdrücke logisch ableiten
- Um kontextbezogenes Reasoning zu erleichtern
- **Pro:** gut in der Formalisierung und Argumentation
- **Con:** schwach in der partiellen Verifikation und Anwendbarkeit

Ontologien

- Begriff kommt ursprünglich aus der Philosophie (“die Lehre vom dem, was ist”)
- Definiert ein gemeinsames Vokabular für den Informationsaustausch in einem bestimmten Bereich → gemeinsame Konzeptualisierung der Domäne
- für die Darstellung personalisierter Informationen geeignet
- hierarchische Darstellung von groben bis feinkörnigen Benutzerinteressen → Benutzerpräferenzen
- Kerntechnologie des Semantik Web
- **Pro:** generische Struktur, sehr hohe Flexibilität, erlaubt nicht nur Modellierung sondern auch Reasoning
- Ontologien können mit OWL beschrieben werden, OWL baut auf RDF auf
- Mit Ontologien beschreibt/modelliert man Teile der realen Welt, um dieses Modellwissen maschinenlesbar dem Computer bereitzustellen
- Vergleichbar mit UML-Diagrammen, die „Entitäten“ und die Beziehungen zwischen diesen darstellen (z.B. Stammbaum aller Säugetiere / Bestandteile eines VW Golf)
- Ontologien sind die „shared models“ die in der Definition des Kontext erwähnt werden

Semantic Web

- URI (Uniform Resource Identifier): spezielle Form → URL
- RDF (Resource Description Framework)
- OWL (Web Ontology Language)
- Verwendet RDF-Modell & Syntax für die Beschreibung von Ressourcen
- OWL (auf RDF-Basis) für die Modellierung von Ressourcentypen, -eigenschaften und -beziehungen
- Ressource: alles, was mit einer URI eindeutig identifiziert werden kann
-
- RDF-Triple: einfache Aussage (Statement), bestehend aus Subjekt, Prädikat, Objekt



Kontextinformationen und der Schutz der Privatsphäre

Kontextabhängige Systeme müssen Kontextinformationen über die physische Umgebung sammeln, wie z. B. den Standort des Benutzers, Aktivität, Gewohnheiten usw., um intelligente Entscheidungen

ohne Benutzerinteraktion zu treffen **aber** der Kontext ist oft mit Personendaten verknüpft (z. B. der Standort einer Person) die unter die Datenschutzrichtlinien fallen.

Die Intelligenz von kontextbewussten Systemen ist an die Qualität und Quantität der Genauigkeit des verfügbaren vergangenen und gegenwärtigen Kontexts gekoppelt.

Ziel ist es die **Smartness der Umgebungen** (durch Context-awareness) und den **Schutz der Privatsphäre** (automatische Erfüllung der Datenschutzwünsche der Nutzer) in Einklang zu bringen.

Persönliche Daten sind sensibler als Kontextinformationen, falls diese aber mit einem Individuum verbunden werden können, fällt sie unter die Datenschutzverordnung. Die Durchsetzung des Schutzes der Privatsphäre in kontextabhängigen Anwendungen erzeugt die Schwierigkeit, **den Inhalt** (Umfang und Genauigkeit) **von Kontextverläufen** zu kontrollieren und zu verwerten.

Techniken zum Schutz der Privatsphäre:

Zugriffskontrolle

Benutzerbestimmbare Zugriffskontrolle (Discretionary Access Control): Der Eigentümer entscheidet, wer auf die Ressource zugreifen darf und welche Privilegien er/sie hat.

Zwingend erforderliche Zugangskontrolle (Mandatory Access Control): Definiert spezifische Bedingungen für den Zugriff auf eine angeforderte Ressource.

Rollenbasierte Zugriffskontrolle (Role Based Access Control): Eine Zugangspolitik, die vom System und nicht vom Eigentümer bestimmt wird → Rollen, Gruppen.

Zwecksgebundene Zugriffskontrolle (Purposed-based Access Control): Zugang zu diesen Ressourcen auf der Grundlage des Zwecks, zu dem der Zugriff erfolgen soll, es liegt in der Verantwortung des Systems, den Zugriffszweck zu bestimmen und zu entscheiden, ob der Zugang gewährt wird oder nicht.

Platform for Privacy Preferences (P3P)

Gibt Benutzern die Kontrolle über ihre persönlichen Daten beim Surfen auf Websites. Vorgestellt vom World Wide Web Consortium (W3C), ermöglicht es Websites, die beabsichtigte Verwendung von Informationen programmatisch mit den Datenschutzpräferenzen der Nutzer zu verglichen.

Der/die Nutzer/in legt er seine/ihre eigenen Richtlinien fest und gibt an, welche persönlichen Informationen auf den besuchten Websites gesehen werden dürfen. Wenn die beiden nicht übereinstimmen, informiert P3P den/die Nutzer/in und fragt, ob er/sie bereit ist die Seite zu besuchen.

Hippocratische Datenbanken (Hippocratic Databases)

Eid des Hippokrates: Und über alles, was ich in der Behandlung oder auch ohne Behandlung im Leben der Menschen sehe oder höre - Dinge, die niemals nach außen dringen sollten - werde ich schweigen, da ich solche Dinge für unsagbar halte.

→ Datenbanken die Daten in Anlehnung an diesen Eid praktizieren

Anonymisierung (Anonymity)

Bekanntes Verfahren zur Wahrung der Privatsphäre. Dabei werden freigegebene Daten so verändert, dass die Datenelemente nicht mehr direkt mit der Person in Verbindung gebracht werden können.

Der Begriff **Datenanonymität** bezieht sich auf die Identität einer Person oder persönlich identifizierbare Informationen. Lediglich Löschen der Daten führt nicht zwangsweise zur

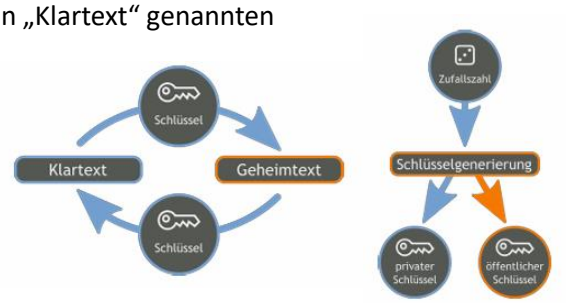
Anonymisierung, verbleibenden Daten in Kombination mit anderen Informationsquellen können immer noch mit den Personen in Verbindung gebracht werden.

K-Anonymität ist, wenn die Informationen für jede enthaltene Person von mindestens (k-1) Personen nicht unterschieden werden kann

Die Ansätze hierfür sind **Generalisierung** (Attributwert wird durch eine umfassendere Kategorie ersetzt) und **Unterdrückungstechniken** (Attributwert oder einen Teil eines Attributwertes wird durch das Symbol * ersetzt).

Verschlüsselung (Encryption)

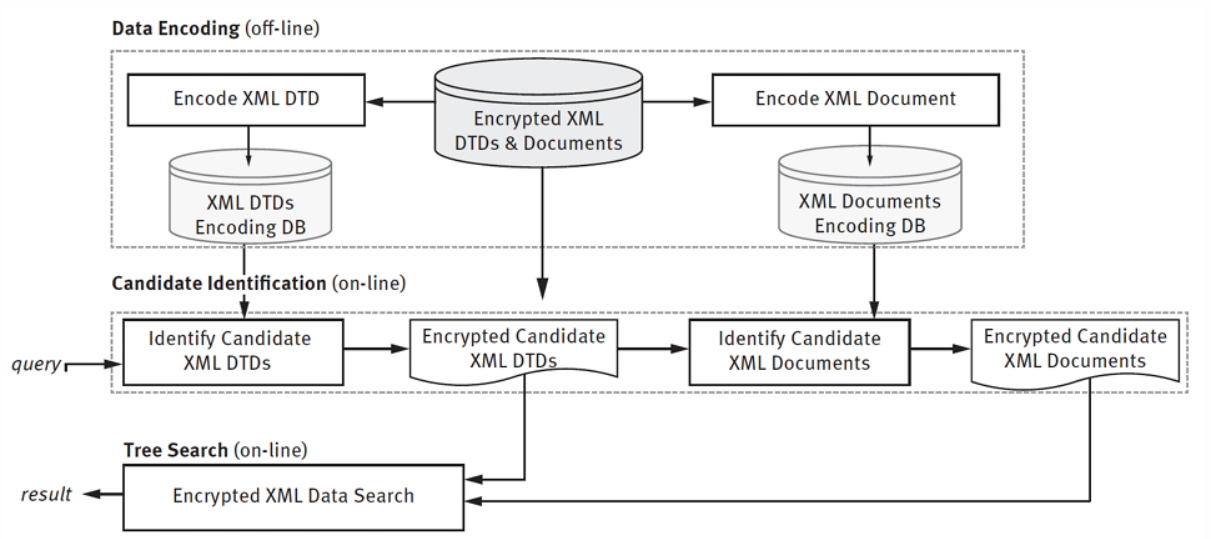
Die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“.



Es wird unterschieden zwischen Symmetrischer Verschlüsselung (Austausch von identischem Schlüssel zum Ver- und Entschlüsseln) und Public-Key-Verschlüsselungsverfahren (generieren von privatem und öffentlichem Schlüssel).

Suche in verschlüsselten XML-Datenbanken:

1. **Datenkodierung:** bevor die Verschlüsselung erfolgt, Vorauswahl potenzieller Zieldokumente
2. **Identifizierung** der Kandidaten: Vorverarbeitungsphase, um unmögliche Kandidaten herauszufiltern
3. **TreeSearch:** Suche wird auf verschlüsselten Daten durchgeführt



Life-Cycle Management

Die Auflösung der Informationen werden in Leveln dargestellt und sind dementsprechend abrufbar (Level 1 = Position, Level 2 = Raum, Level 3 = Stockwerk, …).

Je nachdem wann Daten abgefragt werden, wird eine unterschiedliche Auflösung der Daten zurück gegeben.

Es wird unterschieden zwischen **Organisationsorientierten LCPs** (Life-Cycle-Policies), **Nutzerorientierten LCPs** und **Kombinierten LCPs**.

Bei Nutzerorientierten LCPs verschwinden zunächst die Nutzerspezifischen Daten, bei Organisationsorientierten LCPs werden nur Organisationsrelevante Daten behalten, bei den Kombinierten LCPs, werden je nach Anfrage unterschiedlich spezifische Daten geliefert.

Reasoning

Erzeuge neue Kontextinformationen aus existierenden, Ziel ist oft „Semantic Uplifting“, d.h. höherwertige Kontextinformationen erzeugen. Hier ist häufig keine einmalige Lösung möglich, da die Datenquellen und Methoden sich ändern.

Special-purpose Reasoners

Spezialisiert auf ein Thema

Beispiel: Location Reasoner unter Verwendung von

- Ort der persönlichen Geräte und “Wearables”
- Ort eines Mikrophons, das Benutzerstimme erkannt hat
- Termine des Benutzers im Kalender
- Basierend auf Computer Vision (Analyse von live Video-Streams)

General-purpose Reasoners

Keine thematische Expertise, sondern konfigurierbar, deckt dafür ein großes Spektrum von ableitbarem Kontext ab unter Verwendung spezifischer logischer Methoden (z.B. Aggregation, statische Analyse, Logik, …) an Daten von spezifischen Quellen. Die Konfigurierbarkeit ist sehr wichtig, weil themenspezifische Schlussfolgerung nicht hart kodiert sind, sondern Konfigurationsparameter.

General-purpose Reasoning kann mit OWL erstellt werden, z.B. „Lamp“ ist Subklasse von „Device“. OWL bietet mehrere Konstrukte, die über die Strukturbeschreibung hinausgehen, z.B. Vergleichen von zwei Klassen oder Objekten.

Herausforderungen

- Die geteilten Modelle („shared models“) beschreiben nur bestimmte Teilbereiche
  - Kontext ist nicht umfassend (kann aber erweiterbar sein)
- Jedes Modul im System hat nur eine bestimmte Sicht auf den Kontext (je nachdem welche Modelle sie unterstützt)
  - Perspektiven können unterschiedlich sein oder sich überlappen
- Es gibt keine Garantie über die Verfügbarkeit von Kontextinformationen
- Kontextinformationen können ihre Gültigkeit verlieren und Genauigkeitsprobleme haben (Messfehler)
  - Kontextsensitive Module müssen fehlertolerant sein
- Schutz der Privatsphäre und Verarbeitung der Kontextinformationen gegenläufig

Künstliche Intelligenz

Definition: KI ist der Versuch einer Reproduktion von menschlichem Reasoning und intelligentem Verhalten durch rechnerische Methoden.

KI ist der Versuch Computer intelligenter zu machen und ein besseres Verständnis für menschliche Intelligenz zu erhalten.

Es gibt **4** Ansätze: Handeln wie Menschen, denken wie Menschen (mit den menschlichen Fehlern), rational Handeln, rational Denken.

Denken und handeln, wie der Mensch ist meistens nicht erwünscht, das Ziel ist meistens, die bestmögliche Antwort zu geben mit den verfügbaren Informationen.

Beim Denken ist das Problem, **wie** man **Regeln** des Denkens **beschreibt** und diese dem Computer bereitstellt.

Beim Handeln gibt es **rationale Agenten** (oder Aktoren) welche Ziele erreichen durch ihr Handeln, rationales Denken ist hierfür häufig aber nicht notwendigerweise eine Voraussetzung.

Wenn man Intelligenz rein als **Informationsverarbeitung** betrachtet, sind Maschinen Intelligent, wenn man Intelligenz nur in **Verbindung mit einem Menschen** betrachtet, ist diese Eigenschaft nicht gegeben.

Künstliche Intelligenz in AmI

In AmI wird vor allem **rationales** Denken und Handeln benötigt, um auf z.B. Änderungen in der Umgebung zu reagieren. Manchmal ist aber auch menschliches Denken und Handeln gefordert.

Ein AmI-System soll auf **Änderungen** der **Umgebung**, des **Nutzers** und des **Systems** während der **Laufzeit** reagieren können.

Auch hier gelten die Regeln zu Context-Awareness und Reasoning. Durch Verfeinern eines Low-Level Kontextes mithilfe von Reasonings erhalten wir eine **Situation**.

Aktivitäten sind ein höher geordneter Kontext mit einer Referenz zu einem Nutzer → Activities of daily living (ADL)

Situationen

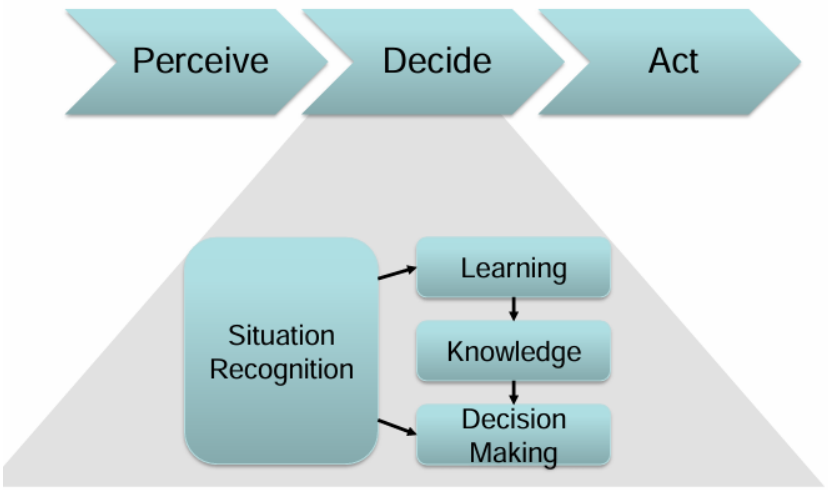
Situationen sind ähnlich zu Aktivitäten aber enthalten weitere Informationen:

- **Zeitpunkt** der Situation: bestimmte Situationen haben verschiedene Bedeutungen zu verschiedenen Zeitpunkten
- **Dauer** der Situation: können verschiedene Länge haben
- **Häufigkeit** der Situation: können unterschiedliche häufig auftreten
- **Reihenfolge** der Situationen: können in verschieden Abfolgen mit anderen Situationen auftreten

Eigenschaften von Situationen:

- **Generalisierung** (Generalizability): Level der Abstraktion, z.B. Medien Konsum ist generischer als TV schauen
- **Komposition** (Composition): Situationen können häufig unterteilt werden, z.B. Kochen besteht aus mehreren einzelnen Situationen
- **Abhängigkeit** (Dependency): Situationen können gegenseitig abhängig sein, sodass Situation A nur stattfinden kann, nachdem Situation B gestartet ist
- **Gegensätzlichkeit** (Opposition): Situationen können mutually exclusive sein
- **Abfolge des Zeitlichen Auftretens** (Time occurance sequence): Situationen können zeitabhängig sein

Abfolge eines KI-basierten Entscheidungsprozesses:



Typen von Künstlicher Intelligenz

Rule-based Systeme

Expertenwissen wird direkt in das System eingespeist, dann werden **Logik-basierte Regeln** angewandt.

Grundlage ist, dass Wissen diskretisiert (in diskrete Einheiten unterteilen) werden kann.

Ontologien erlauben die strukturierte Darstellung von Wissen, räumliche und zeitliche Abhängigkeiten sind häufig die **Basis in Situationserkennung**.

Ungenaue Logik kann mit nicht präzisen Kontexten helfen.

Supervised Learning

Expertenwissen ist die Basis des maschinellen Lernens, die Klassifikation wird durch die bereitgestellten Daten erreicht.

Definition: Ein Computerprogramm lernt aus Erfahrung E in Bezug auf eine Klasse von Aufgaben T und ein Leistungsmaß P, wenn sich seine Leistung bei Aufgaben in T, gemessen durch P, mit der Erfahrung E verbessert.

Wissen ist in einer exemplarischen Form vorhanden, mit einem Teil dieser Wissensbasis wird das System trainiert (Training Set) und mit einem anderen Teil wird das System getestet (Test Set).

Unsupervised Learning

System lernt Muster ohne Expertenwissen, durch z.B. Cluster Recognition.

Große Datensätze vorhanden und ohne Zuweisung von Wissen. System sucht selbstständig nach Mustern.

Wann welches Learning?

- Wenige, genaue Sensoren, wenige Situationen: Rule-based
- Ungenaue Sensoren, Rule-based, Supervised
- Ungenaue Sensoren, komplexe Situationen: Supervised, Unsupervised

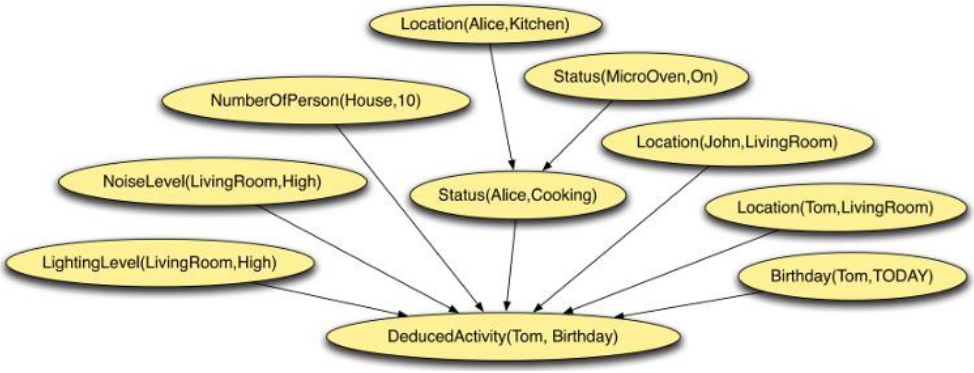
Formen von Reasoning

Fuzzy Logic: Mappend der fuzzines in den Daten, Weg von fixen Werten.

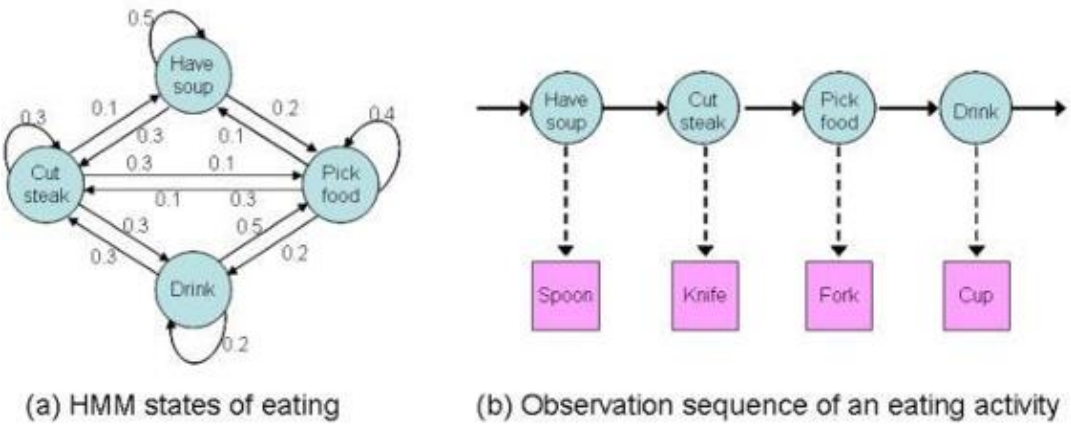
Ontologie: Wissen ist in Form von Ontologien, Regeln basieren auf diesen Ontologien, Mappen von Expertenwissen

Example: (?user rdf:type socam:Person), (?user, socam:locatedIn, socam:Bedroom), (?user, socam:hasPosture, 'LIEDOWN'), (socam:Bedroom, socam:lightLevel, 'LOW'), (socam:Bedroom, socam:doorStatus, 'CLOSED') -> (?user socam:status 'SLEEPING')

Bayes'sches Netz: Gerichteter Azyklischer Graph, Nodes als Kontextevent, Links als Casual Connection, Situationen folgen aus dem Tree Traversal des Netzes.

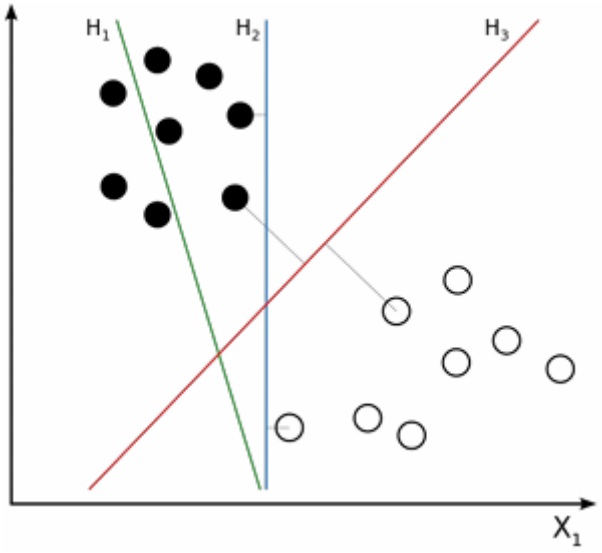


Hidden Markov Modell: Dynamisches Bayes'sches Netzwerk, nur ein Teil der States ist beobachtbar, Wahrscheinlichkeiten für Statusübergänge sind bekannt oder gelernt.



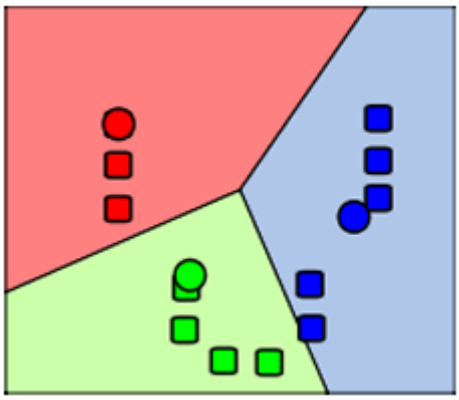
(a) HMM states of eating (b) Observation sequence of an eating activity

Support Vector Machines: Klassifikation von Objekten oder Events, Subdivision sodass Klassen-Boundary so groß wie möglich. Höherdimensionale Datensätze können mit Hyperplanes separiert werden



Beispiel: H2 Separiert mit enger Boundary, H3 separiert mit weiter Boundary

K-Means Clustering: Unsupervised Learning Methode, Teilen der State-Spaces in Cluster, Zuweisen von neuen Elementen in Relation zum Abstand vom Cluster-Mittelpunkt.



Der Nutzer in lernenden Systemen

Formen von Einfluss:

- **Datenursprung:** Nutzeraktivitäten sind die wichtigste Basis für Entscheidungen, Experten können das System konfigurieren
- **Operator der gelernten Regeln:** Operator triggert viele Regeln, und kann Rückmeldung über Erfolg geben
- **Anpassung des Lernens**: Der Nutzer kann den Lernprozess beeinflussen

Datenursprung:

- Grundannahme, dass Datenbasis wahr ist, häufig gelabelte Daten
- Nutzeraktivitäten stellen diese Wahrheit dar
- Beispiel: Pose Recognition, Sensoren liefern Basis für mehrere Posen, Anpassung der Threshold Werte
- Nutzerprofil

Operator der gelernten Regeln:

- Selbsterstellte Regeln: Selbstkonfigurierte Regeln werden gesetzt, diese können die Regellogik oder Parameter beeinflussen
- Framework-Regeln: Bestimmte Framework Bedingungen für Regeln können durch den Operator gesetzt werden, Scope des lernenden Systems ist limitiert
- Feedback: Wenn Regeln ausgeführt werden ist der Nutzer normalerweise direkt betroffen, System kann nach Feedback fragen
- Beispiel: Voice Assistant konfiguriert durch Nutzer

Anpassung des Lernens:

- Anpassen der Steuerungsparameter
- Fuzzy Sets: Anpassen der zugewiesenen Werteparameter und Wahrscheinlichkeiten
- Parameter
- Profile
- Beispiel: Durch Unfall Sichtbehinderung, System passt an und gibt hörbares Feedback, passt Schriftgröße an etc.

Trends in intelligenten Umgebungen

Deep Learning: Hoch performant für viele Probleme in der Computer Vision, aber Herausforderungen Blackbox und Systemvoraussetzungen, kann bei Situationserkennung eingesetzt werden, zeitliche Abfolge in Sensordaten kann verwendet werden

Hybrid Reasoning: Regelbasiertes System hat Probleme mit hoher Komplexität, Learning-basierte Systeme können schnelle Änderungen und Nutzerpräferenzen nicht gut darstellen, Hybrid Reasoning ist Kombination von beiden, um die jeweiligen Nachteile auszugleichen.

Smart Speaker: Assistenzsysteme im Lebensraum, Kombination von Spracherkennung und Regeln mittels Natural Language Processing

Maschinelles Lernen

Maschinelles Lernen ist immer eine **Funktionsoptimierung** auf Daten. Hierfür wird eine Hypothese $h(x, \omega)$ formuliert. Der Lernschritt erfolgt über eine **Anpassung der Gewichte** ω über Optimierung einer Funktion anhand gegebener Daten. Ziel ist es, die Hypothese so zu wählen, dass sie auf unbekannten Daten richtige Aussagen treffen kann.

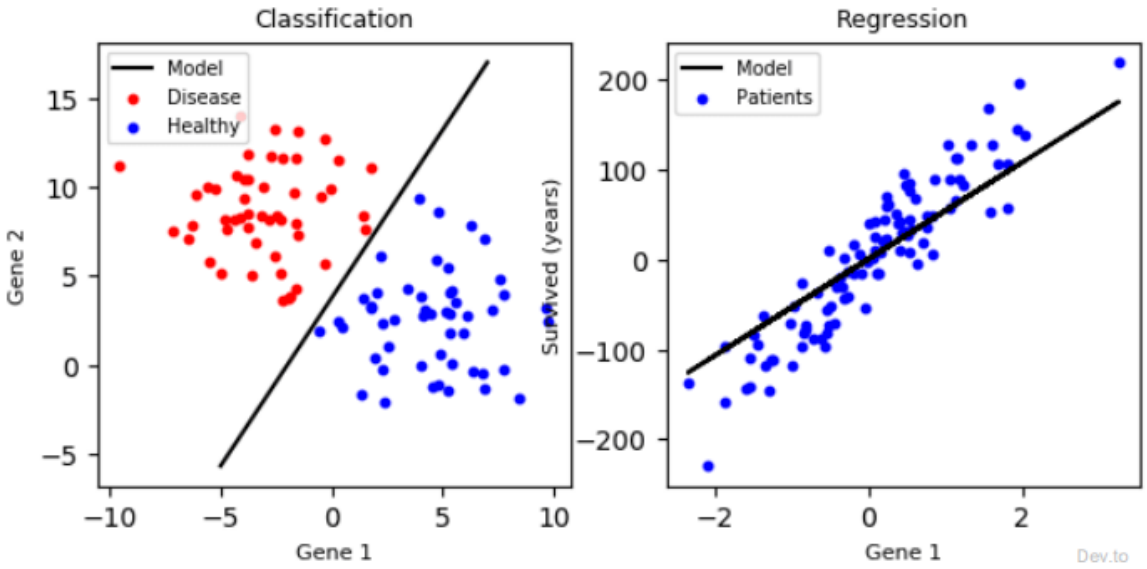
Supervised Learning

Bei Supervised Learning liegen **Daten und entsprechende Labels** vor, das System erhält **direktes Feedback** beim Lernen. Das Ziel ist die Vorhersagen zukünftiger Ereignisse.

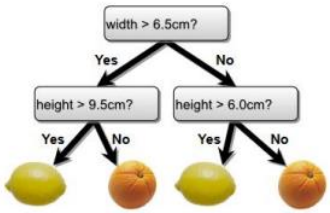
Wir haben m Trainingsdaten $\{(x^{(i)}, y^{(i)}); i = 1 \dots m\}$, hierbei ist $x^{(i)}$ der Inputvektor und $y^{(i)}$ das Target, wenn y kontinuierlich ist, spricht man von Regression, wenn y diskrete Werte sind spricht man von Klassifikation. Ziel ist es, eine Hypothese / Funktion h so zu lernen, dass es für unbekannte Inputvektoren den richtigen Output vorhersagt.

Klassifikation und Regression

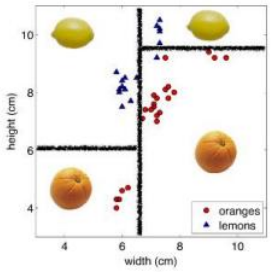
Klassifikation ist ein Prozess in der Datenanalyse, bei dem Datenpunkte in vordefinierte Kategorien oder Klassen eingeordnet werden. Regression hingegen beschreibt die Beziehung zwischen einer abhängigen Variablen und einer oder mehreren unabhängigen Variablen, um Vorhersagen oder Trends zu ermitteln.



Decision Trees



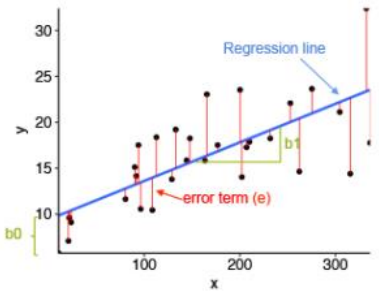
Klassifikator in Braumstruktur, bei dem jeder Knoten ein Test für eine variable ist. Der Ausgang jeden Tests entscheidet, zu welchem Nachbarknoten man sich bewegt, die Endknoten stellen die Vorhersage/Prediction dar. Auf jeder Ebene wird bestimmt, welche Variable gesplittet werden soll und wo diese gesplittet werden soll. Die Bewertung der Splits kann über Entropie erfolgen.



Lineare Regression

Wir betrachten unsere Trainingsdaten m und gewichten jedes Feature linear. Die Hypothese lautet:

$$h(x) = \sum_{i=1}^{n} \theta_i x_i = \theta^T x$$

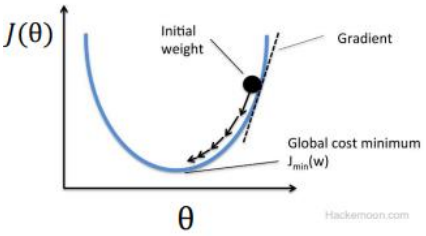


Die folgende Kostenfunktion wird minimiert (Least-Square):

$$J(\theta) = \frac{1}{2}\sum_{i=1}^{m} h_\theta\left(x^{(i)}\right) - y^{(i)})^2$$

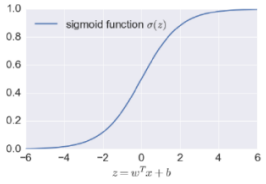
Durch Ableiten der Kostenfunktion erhalten wir unsere Update-Regel:

$\theta_j := \theta_j + \alpha \sum_{i=1}^{m} \left(y^{(i)} - h_\theta\left(x^{(i)}\right)\right) x_j^{(i)}$ für jedes j



Logistische Regression (Klassifikation)

Lineares Model für binäre Klassifikation (basierend auf der linearen Regression). Hierbei geht man von der Annahme aus, dass sich die Wahrscheinlichkeiten der beiden eintretenden Klassen über Sigmoidfunktionen darstellen lassen:



$$p(y = 1|x, w, b) = \sigma(w^T x + b), p(y = 0|x, w, b) = 1 - \sigma(w^T x + b),$$

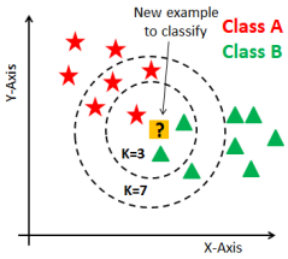
$$\sigma(z) = \frac{1}{1 + e^{-z}}$$

Das Model kann als Bernoulliverteilung beschrieben werden:

$$p(y|x,w,b) = \left(\sigma(w^T x + b)\right)^y \cdot \left(1 - \sigma(w^T x + b)\right)^{1-y}$$

Das Training findet über Maximum Likelihood Estimation (MLE) statt, d.h. $p(y|x,w,b)$ wird über Gewichte optimiert.

K-Nearest Neighbor



Hier wird ein **Lazy Learner** verwendet, das bedeutet, es werden alle Trainingsdaten einfach abgespeichert. Während der Vorhersage werden die k nächsten Nachbarn gefunden.

Für Klassifikation:

- Abstimmung der Nachbarn für welche Klasse diese sind (Label auslesen) → Mehrheit entscheidet
- Evtl. gewichtet mit der Distanz zum Query

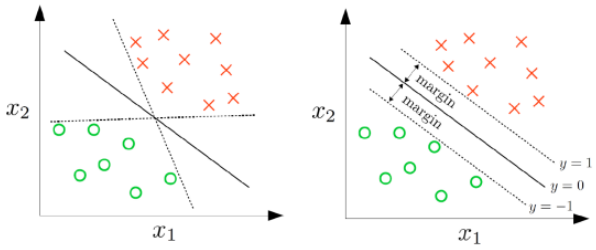
Für Regression:

- Mittelwert der Nachbarlabels → Mittelwert der Labels werden zurückgegeben
- Evtl. gewichteter Mittelwert

Support Vector Machine Klassifikation

Support Vector Machines (SVM) sind aus der statistischen Lerntheorie entstanden. Diese wählt ein „optimales“ Modell aus einer Menge von Modellen und nimmt nicht vorher an, das korrekte Modell zu kennen. „Optimal“ bezieht sich auf die Generalisierungsfähigkeit des Modells und daher auf die Fähigkeit, die Fehlerwahrscheinlichkeit auf allen Daten zu minimieren.

$R(w) \leq R_{emp}(w) + \epsilon(n, p^*, h)$, wobei $R(w)$ das echte Risiko, $R_{emp}(w)$ der Trainingsfehler (Empirisches Risiko) und der letzte Teil die Komplexität ist.

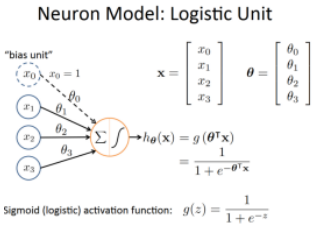


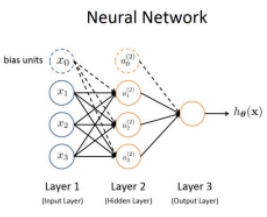
(a) Possible decision boundaries (b) Maximum margin principle

Bei linearen SVMs geht man folgendermaßen vor: Finde eine Decision Boundary, die die Margin zwischen Decision Boundary und den nächstliegendenden Punkten maximiert.

Neuronale Netze

Neuronale Netze lernen Funktionen, deren Komplexität sehr variable modelliert werden kann.

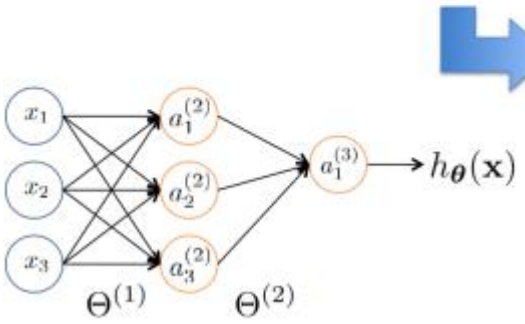




Neuronale Netze bestehen aus **Knoten** und **Verbindungen**, jeder Knoten hat eine Aktivierungsfunktion und einen Output, jede Verbindung ist mit einem Gewicht assoziiert.

Für das Training muss eine nicht-konvexe Kostenfunktion bestimmt werden, diese wird meist über ein Gradientabstiegsverfahren minimiert.

$$a_1^{(2)} = g\left(\Theta_{10}^{(1)}x_0 + \Theta_{11}^{(1)}x_1 + \Theta_{12}^{(1)}x_2 + \Theta_{13}^{(1)}x_3\right) = g\left(z_1^{(2)}\right)$$
$$a_2^{(2)} = g\left(\Theta_{20}^{(1)}x_0 + \Theta_{21}^{(1)}x_1 + \Theta_{22}^{(1)}x_2 + \Theta_{23}^{(1)}x_3\right) = g\left(z_2^{(2)}\right)$$
$$a_3^{(2)} = g\left(\Theta_{30}^{(1)}x_0 + \Theta_{31}^{(1)}x_1 + \Theta_{32}^{(1)}x_2 + \Theta_{33}^{(1)}x_3\right) = g\left(z_3^{(2)}\right)$$
$$h_\Theta(\mathbf{x}) = g\left(\Theta_{10}^{(2)}a_0^{(2)} + \Theta_{11}^{(2)}a_1^{(2)} + \Theta_{12}^{(2)}a_2^{(2)} + \Theta_{13}^{(2)}a_3^{(2)}\right) = g\left(z_1^{(3)}\right)$$



Feed-Forward Steps:

$$\mathbf{z}^{(2)} = \Theta^{(1)}\mathbf{x}$$
$$\mathbf{a}^{(2)} = g(\mathbf{z}^{(2)})$$
$$\text{Add } a_0^{(2)} = 1$$
$$\mathbf{z}^{(3)} = \Theta^{(2)}\mathbf{a}^{(2)}$$
$$h_\Theta(\mathbf{x}) = \mathbf{a}^{(3)} = g(\mathbf{z}^{(3)})$$

Wobei $a_i^{(j)}$ die Aktivierung der Einheit i in Layer j beschreibt und $\Theta^{(j)}$die Gewichtsmatrix Kontrollfunktion, welche von Layer j auf Layer $j+1$ mappt. Wenn das Netzwerk s_j Einheiten in Layer i und s_{j+1} Einheiten in Layer $j+1$ hat, dann hat $\Theta^{(j)}$ die Dimension $s_j + 1 \times (s_j + 1)$.

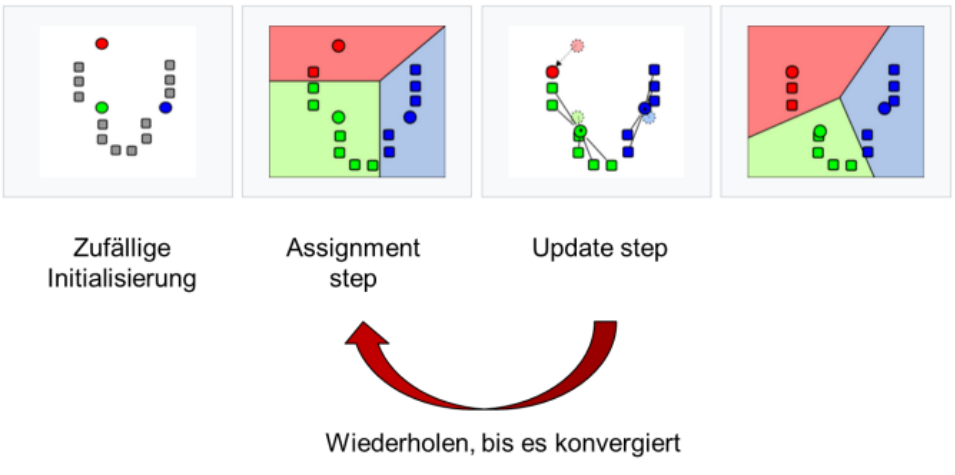
Unsupervised Learning

Bei Unsupervised Learning liegen Daten **ohne** Labels vor und das System erhält **kein Feedback**, das Ziel ist das Erkennen von Mustern in den Daten.

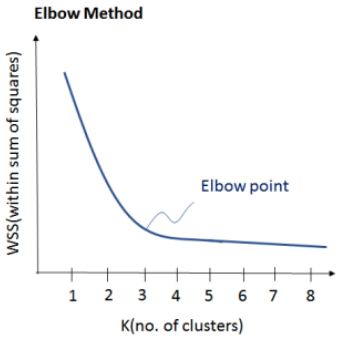
K-Means Clustering

Bei K-Means Clustering ist das Ziel, Daten Gruppen (**Cluster**) von Datenpunkten, die **ähnliche Eigenschaften** besitzen, einzig anhand der Daten. Dafür initialisiert man zufällig **Centroids** μ_i für jeden Cluster und löse folgendes **Optimierungsproblem**: $\arg\min_s \sum_{i=1}^{k} \sum_{x \in S_i} \|x - \mu_i\|^2$, indem folgende zwei Schritte abwechselnd wiederholt werden:

1. Weise jeden Datenpunkt einem Cluster zu, indem die **kürzeste** Distanz, als dessen Zugehörigkeit interpretiert wird. (Assignment)
2. Berechne die neuen Centroids, indem die Schwerpunkte pro Cluster anhand deren Datenpunkte neu berechnet wird (Update)



Um die Anzahl der Cluster zu bestimmen, verwendet man die **K-Fold Cross Validation** (siehe Evaluierungskonzepte)und die Ellenbogen-Methode („**k im Knick**“ wählen).



Vorteile:

- Simple und effektive (auch heute noch das meist genutzt Clustering-Verfahren)
- Gute Skalierbarkeit

Nachteile:

- Anzahl der Cluster muss manuell gewählt werden
- Probleme, wenn die Cluster in Größe und Dichte variieren
- Sensitiv gegenüber Outlier

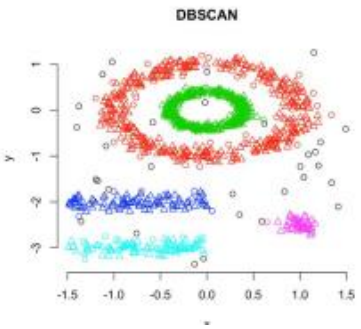
DBSCAN

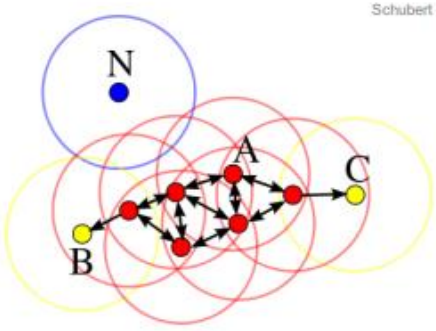
DBSCAN steht für Density-based spatial clustering of applications with noise, also ein Dichte-basiertes Clustering Verfahren, welches Outlier detektieren kann. Es hat zwei Parameter, **epsilon**: maximale Distanz, die zwei benachbarte Punkte in einem Cluster besitzen dürfen und **minPoints**: die minimale Anzahl an Datenpunkten, die zusammen ein Cluster bilden dürfen.

ALGORITHM 2: Abstract DBSCAN Algorithm

```
1 Compute neighbors of each point and identify core points   // Identify core points
2 Join neighboring core points into clusters                 // Assign core points
3 foreach non-core point do
4     Add to a neighboring core point if possible            // Assign border points
5     Otherwise, add to noise                                // Assign noise points
```

Schubert et al. 2017





Vorteile:

- Kann sehr gut mit Outlier umgehen
- Anzahl von Clustern muss nicht vorgegeben werden

Nachteile:

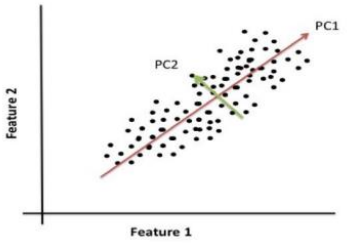
- Kann nicht gut mit Clustern unterschiedlicher Densities umgehen
- Probleme bei hochdimensionalen Daten

Representation Learning

Ermöglicht das Erlernen von niedrig-dimensionalen (kompakteren) Repräsentationen als Cluster (PCA, Autoencoder), es handelt sich trotzdem noch um Unsupervised Algorithmen.

Principal Component Learning (PCA)

Das Ziel, ist eine kompaktere (niedrig-dimensionale) Feature-Repräsentation für Daten zu finden.

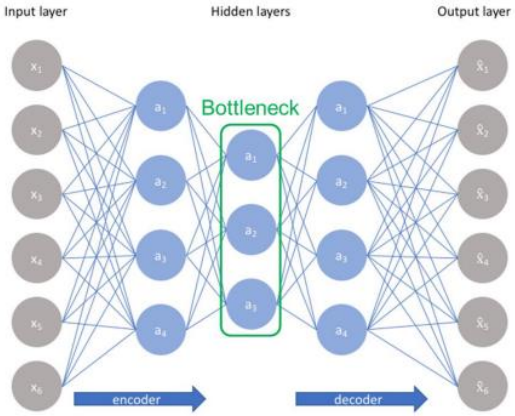


1. Subtrahiere den Mittelwert pro Feature von jedem Feature
2. Bestimme die Kovarianzmatrix dieser Daten
3. Bestimme die Eigenvektoren und dazugehörige Eigenwerte dieser Matrix
4. Projiziere die Daten auf die m Eigenvektoren mit den höchsten Eigenwerten (über Matrixmultiplikation der Daten mit dem neuem Eigenvektorraum)

Die Eigenvektoren werden principal components genannt und decken pro Achse die meisten Variationen ab.

Autoencoder

Bei Autoencodern handelt es sich um ein neuronales Netz, welches zum Kodieren komprimierter Repräsentationen verwendet wird. Die Idee ist, dass man im Training versucht, den Input als Output zu rekonstruieren und verwendet dabei eine Netzstruktur mit einem Bottleneck. Die Features in diesem Bottleneck stellen eine komprimierte Repräsentation dar.



Autoencoder	**PCA**
+ Lernen nicht linearer Ebenen ist möglich	+ Einfaches finden der Hyperparameter
	+ stabileres Training
- Komplizierte Hyperparameteroptimierung notwendig	- Nur lineare Komponenten lernbar (ohne **Kernel-Trick**)
- Aufwendiges Training	

Anomalie-Detektion

Anomalie-Detektion beschreibt den Prozess, unerwartete Gegenstände oder Events in einem Datenset zu finden. Besonderheiten von Anomalien sind, dass sie selten auftreten und sich signifikant von ihren Eigenschaften unterscheiden. Anomalie-Detektion wird bei DBSCAN eingesetzt.

Weitere Lernmethoden

Semi-Supervised Learning: In den meisten Fällen ist es sehr **aufwändig**, **Labels** für seine Datenpunkte **zu bekommen**. Die Folge ist, dass man nur einen Teil der Daten labeln kann, man aber möglichst alle Daten zum Training nutzen möchte. Diese Art von Lernalgorithmen wird als semi-supervised Learning bezeichnet. Sie sind in der Lage, Daten **mit und ohne Labels** zum Trainieren zu verwenden, um ein deutlich besseres Ergebnis zu erlangen, als wenn man nur die gelabelten Daten verwendet.

Reinforcement Learning: Reinforcement Learning erlaubt es, das Verhalten (**actions**) eines Agenten in einer interaktiven Umgebung zu lernen. Dabei lernt es mit Trial und Error über ein Feedback (**reward**) Mechanismus.

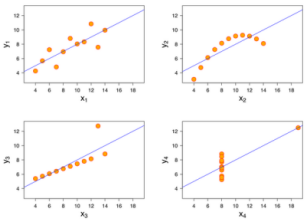
Sequence Learning: Beim sequenziellen Lernen wird eine Sequenz von Daten in das Modell gegeben (anstatt von Feature-Vektoren fixer Größe). Diese Daten haben eine beliebige Länge, aber eine fixe Anordnung!

Online-Learning: Im Klassische ML wird ein Modell vor der Laufzeit trainiert und bleibt während der Laufzeit unverändert. Im Online-Learning lernt das Modell während der Laufzeit weiter

Active Learning: Active Learning ist ein Spezialfall von Semi-Supervised Learning. Ein AL-Modell ist in der Lage, **interaktiv mit dem Nutzer zu kommunizieren**, um Labels für neue Datenpunkte zu erhalten. Dies erlaubt es dem Modell, mit wenig Datenpunkten eine hohe Aussagekraft (z.B. durch eine Gute Decision Boundary) zu erlernen.

Tipps und Tricks

Anscombe's Quartett: Alle vier Verteilungen besitzen denselben Mittelwert, Standardabweichung und Korrelationswerte, aber die wichtigsten Information fehlen! Die Annahme einer Normalverteilung ist eine Vereinfachung, deren Sinnhaftigkeit immer überprüft werden sollte!

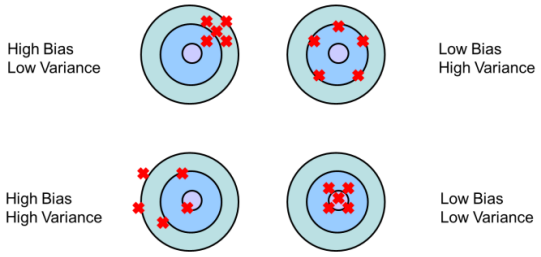


Feature Scaling: Verbessert die Trainingseffizient, sorgt für schnelleres Training und einfacheres Finden von Optima mittels einer Min-Max Normalisierung, welche jedes feature in den Wertebereich [0,1] bringt.

Kernel Trick: Löst das Problem, dass das Auffinden einer geeigneten Transformation für nicht-lineare Separierbarkeit aufwendig ist. Daten können in einen höherdimensionalen Raum transformiert werden, wo sie dann linear Separierbar sind. Dabei ersetzt man das Skalarprodukt $x^T y$ durch den Kernel $K(x, y)$, ein Kernel beschreibt eine Ähnlichkeitsfunktion, ohne weiteren Rechenaufwand werden alle Transformationen abgedeckt, deren Skalarprodukt den Kernel ergeben.

Bias-Variance Tradeoff:

- High Bias /Low Variance: Modell zu einfach, Komplexität der Daten nicht erfasst.
- Medium Bias /Medium Variance: Guter Tradeoff
- Low Bias / High variance: Modell ist zu complex, Datenpunkte werden auswendig gelernt, was zu Overfitting führt.



Regularisierung: Dropout: Die Idee ist, pro Batch ein Subnetz zu trainieren, die Subnetze werden durch zufälliges Löschen von Knoten und deren Kanten erstellt, nach jeder Epoche werden die Gewichte gemittelt, das führt zu Generalisierung und Ensemble Learning.

„Double-Descent" Phänomen: In der klassischen Maschinenlerntheorie gibt es einen Kompromiss zwischen Verzerrung (Bias) und Varianz, wobei zu einfache Modelle die Datenstruktur nicht vollständig erfassen können und zu komplexe Modelle zu Überanpassung (Overfitting) neigen und schlecht auf neue Daten generalisieren. Überraschenderweise zeigen Deep-Learning-Modelle, die oft stark überparametrisiert sind, eine Verbesserung der Leistung auf Testdaten, entgegen der klassischen Theorie. Eine mögliche Erklärung dafür ist das Phänomen des "Deep Double Descent", bei dem größere Modelle trotz ihrer Komplexität und des damit verbundenen Trainingsaufwands bessere Ergebnisse liefern. Dieses Phänomen tritt sowohl bei Deep-Learning-Ansätzen als auch bei klassischen Maschinenlernmodellen wie dem Random Forest auf. Im Deep-Learning-Kontext gibt es zwei wichtige Bereiche: das "Under-parametrized Regime", bei dem die Modellkomplexität deutlich geringer ist als die Anzahl der Trainingsdaten und das zu einer U-förmigen Kurve im Testfehler führt, und das "Over-

parametrized Regime", bei dem die Modellkomplexität die Anzahl der Trainingsdaten weit übersteigt, was zu einem fast null Trainingsfehler führt und anschließend den Testfehler verringert.

Evaluierungskonzepte

Cross-Validation: Um Overfitting zu vermeiden, sollten Training- und Testset immer unabhängig voneinander sein, um trotzdem das meiste aus seinen Daten rauszuholen verwendet man **Cross-Validation,** dabei werden Daten in k Folds eingeteilt. Damit kann auch die mittlere Performanz mit Standardabweichung angegeben werden. (Mean und STD über die k Folds)

Konfusionsmatrix: Eine Konfusionsmatrix visualisiert die Performanz eines Modells.

	Positive classified	Negative classified	
Is positive	True positives (TP)	False negatives (FN)	$TP + FN = P$
Is negative	False positives (FP)	True negatives (TN)	$FP + TN = N$
	$TP - FP$	$FN + TN$	$P + N = \|E\|$

Precision: Anteil der positiven Vorhersagen, die korrekt sind, Fähigkeit des Modells nur relevante Elemente auszugeben. $Precision = \frac{TP}{TP+FP}$

Recall: Anteil der positiven Daten, die korrekt vorhergesagt wurden, Fähigkeit des Modells, alle relevanten Elemente zu identifizieren. $Recall = \frac{TP}{TP+FN}$

ROC-Kurve: ROC steht für Reciever Operating Characteristic, die ROC-Kurve erlaubt es, einen binären Klassifizierer für alle Thresholds gleichzeitig zu untersuchen. Die Area Under the Curve (AUC) ist ein allgemeines Evaluationskriterium eines binären Klassifizierers und gibt die Wahrscheinlichkeit an, dass ein positives und ein negatives Sample richtig erkannt werden.

- X-Achse: False Positive Rate (FPR): Wahrscheinlichkeit, dass ein negatives Sample fälschlicherweise als positiv klassifiziert wird. $FPR = \frac{FP}{FP+TN}$
- Y-Achse: True Positive Rate (TPR): Wahrscheinlichkeit, dass ein positives Sample korrekt als positiv klassifiziert wird. $TPR = \frac{TP}{TP+FN}$

Sicherheit

Sicherheit in IT Systemen besteht aus Security (Sicherheit eines Systems vor Störungen durch höhere Gewalt, technisches Versagen, versehentliche oder fahrlässige menschliche Fehlhandlung, vorsätzliche menschliche Handlungen) und Safety (Betriebssicherheit, Sicherheit der Umgebung eines Systems vor Störung durch das System).

IT-Sicherheitsziele

- **Verfügbarkeit:** Daten/IT-Ressourcen sollen zur Verfügung stehen, wenn benötigt.
- **Vertraulichkeit:** Daten sollen nicht von Unbefugten gelesen werden können.
- **Integrität:** Daten sollen nicht unbemerkt von Unbefugten modifiziert werden können.
- **Authentizität:** Der Urheber von Daten/Aktionen soll eindeutig identifiziert werden können.
- **Nichtabstreitbarkeit (Non-Repudiation)**: der Urheberschaft (Der Urheber von Aktionen soll seine Urheberschaft nicht abstreiten können) und des Empfangs (Der Empfänger von Daten soll deren Empfang nicht abstreiten können).
- **Anonymität:** Der Urheber von Daten/Aktionen soll nicht identifiziert werden können.

IT-Sicherheitsmaßnahmen

IT-Sicherheitsmaßnahmen kosten Zeit und Geld und sind unbequem für den Nutzer, aber sollten dennoch in allen Phasen des Lebenszyklus von IT-Systemen berücksichtigt werden.

Authentisierung: Prüfung der Zugriffsberechtigung auf IT-Ressourcen durch Geräteauthentisierung mit kryptographischen Verfahren oder Benutzerauthentisierung ahand von Besitz, Wissen oder biometrischen Merkmalen (biologische oder Verhaltensmerkmale).

Kryptographische Verfahren: Verfahren mit mindestens einem Parameter (Schlüssel) zur Transformation von Klartext in unverständlichen Geheimtext (Verschlüsselung) und zur Rücktransformation von Geheimtext in Klartext (Entschlüsselung). Hierbei werden symmetrische und asymmetrische Systeme unterschieden. Es gibt aber auch schlüssellose Verfahren und kryptografische Protokolle.

Sicherheit Kryptographischer Verfahren: Schwierigkeit (Komplexität) der Berechnung der Umkehrung (Abbildung, die jedem Funktionswert die zugehörigen Urbilder zuordnet): Einwegfunktionen mit und ohne Hintertür. Die Sicherheit sollte auf der Geheimhaltung von Schlüsseln beruhen anstatt auf der Geheimhaltung von Algorithmen.

Einwegfunktion: Eine mathematische Funktion, die leicht zu berechnen, aber schwer umzukehren ist, wird als Einwegfunktion bezeichnet. Die Berechnung der Funktionswerte einer Einwegfunktion sollte effizient sein, während die Umkehrung praktisch unmöglich sein sollte, selbst bei Einsatz von Brute-Force-Methoden, bei denen alle möglichen Werte durchprobiert werden.

Einwegfunktion mit Hintertür: Eine Einwegfunktion mit Hintertür ist eine spezielle Art von Funktion, bei der die Umkehrfunktion, also die Berechnung des ursprünglichen Inputs aus dem Output, normalerweise schwierig ist, aber deutlich einfacher wird, wenn man über eine bestimmte zusätzliche Information verfügt.

Natürlich gibt es auch **Hybridsysteme**, bei denen eine Vereinbarung symmetrischer Sitzungsschlüssel aus Zufallszahlen, die mittels asymmetrischer kryptographischer Systeme verschlüsselt zwischen den Kommunikationspartnern ausgetauscht werden

Symmetrische Kryptographische Systeme

Verschlüsselungs- und Entschlüsselungsfunktion verwenden denselben geheimen Schlüssel, dadurch erreicht man einen hohen Datendurchsatz.

Blockverschlüsselung:

- **DES** (Data Encryption Standard, 1977): Schlüssellänge: 64 Bit, davon 8 Paritätsbits, also effektiv nur 56 Bit, kann heutzutage mittels Brute-Force-Angriffe gebrochen werden
- **Triple-DES:** modifiziertes DES-Verfahren mit dreifachem Aufruf des DES-Algorithmus mit drei Schlüsseln
- **AES** (Advanced Encryption Standard): 2000 von NIST als Nachfolger von DES ausgewählt, hat eine variable Schlüssellänge (z.B. 128, 192 oder 256 Bit)

Stromverschlüsselung: Blockverschlüsselungsverfahren im Output-Feedback-Modus zur Erzeugung eines pseudozufälligen Schlüsselstroms.

Schlüsselverteilungsproblem: Wenn n Kommunikationspartner jeweils paarweise untereinander vertraulich kommunizieren wollen, werden $\frac{n(n-1)}{2}$ verschiedene Schlüssel benötigt. Bevor die Übertragung geheimer Nachrichten möglich ist, müssen Schlüssel verteilt werden, die ebenfalls geheim bleiben müssen. Dafür wird ein weiterer gesicherter Übertragungskanal benötigt.

Asymmetrische Kryptographische Systeme

Verschlüsselungs- und Entschlüsselungsfunktion verwenden zwei verschiedene Schlüssel, die zusammengehören, aber nicht mit vertretbarem Aufwand aus dem jeweils anderen berechnet

werden können. Auch wenn ein Schlüssel veröffentlicht wird, bleibt der andere geheim, das sorgt für eine einfachere Schlüsselverteilung als bei symmetrischen kryptographischen Systemen.

RSA (Algorithmus von Ron Rivest, Adi Shamir und Leonard Adleman, 1977):

- Sicherheit beruht darauf, dass es schwierig ist, große Zahlen in ihre Primfaktoren zu zerlegen. Primfaktorzerlegung sehr großer Zahlen ist mit den heute bekannten Verfahren praktisch nicht durchführbar, auch wenn nicht unmöglich.
- Schlüssellänge variabel, empfohlene Schlüssellänge 2048 Bit (256 Oktetts)
- relativ langsam
- $n = \prod_{i=1}^{N} p_i$, wobei alle p_i Primzahlen sind

ECC (Elliptic Curve Cryptosystem):

- Sicherheit beruht darauf, dass es schwierig ist, das diskrete Logarithmus-Problem im Kontext elliptischer Kurven zu lösen.
- Schlüssellänge variabel
- Schlüssellänge nur 224 Bit (28 Oktetts) für die gleiche Sicherheit wie mit 2048-Bit-RSA-Schlüssel
- erfordert weniger Rechenzeit und kürzere Schlüssellänge als RSA-Kryptosystem
- noch nicht so weit verbreitet wie RSA-Kryptosystem
- $x = \log_b a$, wenn $a = b^x$

Hashverfahren

Hashfunktionen (Streuwertfunktion) sind mathematische Funktion mit der Eigenschaft, Eingabewerte einer beliebigen, endlichen Länge auf einen Ausgabewert mit fester Länge abzubilden (Datenreduktion).

Kryptographische Hashfunktionen:

- Hashfunktion h mit den Eigenschaften, dass es nicht mit vertretbarem Aufwand möglich ist, zwei verschiedene Eingabewerte x und x' zu bestimmen, deren Funktionswerte h(x) und h(x') übereinstimmen (Kollisionsresistenz), und dass es nicht mit vertretbarem Aufwand möglich ist, aus einem Funktionswert y einen Eingabewert x mit der Eigenschaft h(x) = y zu bestimmen (Einwegfunktion).
- wird eingesetzt z.B. um unbefugte Modifikationen an Datenobjekten entdecken zu können (Sicherung der Integrität, dank Kollisionsresistenz), und um Passwörter sicher zu speichern (Sicherung der Vertraulichkeit, da Einwegfunktion).
- Kollisionen sind möglich, da sehr großer Definitionsbereich auf kleineren Wertebereich abgebildet wird.
- Um Kollisionsresistenz und die Einweg-Eigenschaft zu erreichen, muss Länge der Hashwerte groß sein (mindestens 28 Oktetts empfohlen).
- SHA-224 (Secure Hash Algorithm 224 Bit)

Kryptographische Protokolle

Ein kryptographisches Protokoll beschreibt eine Abfolge von Schritten, um bestimmte Sicherheitsanforderungen zu erfüllen.

Digitale Signatur

Eine digitale Signatur sind Daten, die anderen Daten beigefügt oder mit ihnen logisch verknüpft sind und zum Nachweis der Authentizität und Integrität verwendet werden. Sie sind mit einem asymmetrischen Verschlüsselungsverfahren erzeugbar und überprüfbar.

Signaturerzeugung: unter Verwendung eines asymmetrischen Verschlüsselungsverfahrens zur Sicherung der Authentizität und einer kryptographischen Hashfunktion zur Sicherung der Integrität. Der Vorteil durch das Verwenden einer Hashfunktion ist, dass ein relativ kurzer Hashwert mit einem privaten Schlüssel transformiert werden kann.

Signaturprüfung: Wenn der neue Hashwert dem Original-Hashwert entspricht, dann muss die digitale Signatur mit Hilfe des privaten Schlüssels von A und aus den gleichen Daten erzeugt worden sein.

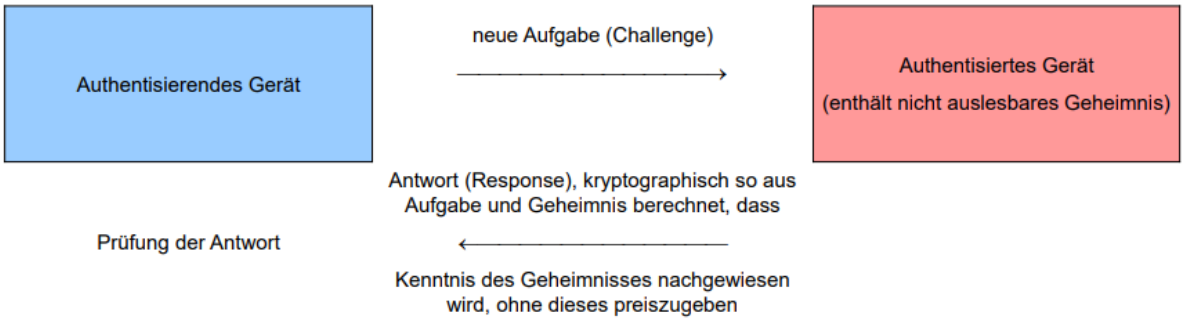
Schutz der Vertraulichkeit des privaten Schlüssels: Privater Schlüssel ist zu lang zum Merken (256 Oktetts empfohlen bei RSA) daher muss er kryptographisch geschützt oder in einem Hardware Security Module gespeichert werden.

Schutz der Authentizität und Integrität des öffentlichen Schlüssels: durch digitale Signatur in einem „Zertifikat". Nach der Schlüsselgenerierung wird das Zertifikat durch einen Zertifizierungsdiensteanbieter (Trusted Third Party) in einer Public-Key-Infrastruktur (PKI) oder andere Benutzer in einem „Web of Trust" (PGP – Pretty Good Privacy) signiert. Vor Benutzung des öffentlichen Schlüssels wird die digitale Signatur des Zertifikats mit Hilfe des öffentlichen Schlüssels des Zertifikatausstellers geprüft.

Zertifikat

Ein Zertifikat ist eine elektronische Bescheinigung, mit der ein öffentlicher Schlüssel (und eventuell weitere Informationen) einer Person oder einem Gerät zugeordnet werden. Das Zertifikat beinhaltet neben dem öffentlichen Schlüssel und den Informationen über den Schlüsselinhaber auch eine digitale Signatur über den übrigen Zertifikatsinhalt.

Challenge-Response-Verfahren



Risikoanalyse

Abwägen zwischen Sicherheit und Kosten und Benutzerfreundlichkeit

1. Identifikation der zu schützenden Werte
2. Identifikation der Bedrohungen
3. Bewertung des Risikos (Eintrittswahrscheinlichkeit von Schadensfällen × Schadenswert)
4. Auswahl von Gegenmaßnahmen (dabei Balance von Kosten und Risiko beachten), technische Sicherheitsmaßnahmen und eventuell Versicherung (bei großem Schadensumfang und kleiner Eintrittswahrscheinlichkeit)
5. Bewertung des Restrisikos

Anwendung auf AmI-Systeme

Bedrohungen in AmI-Systemen sind z.B. Fernsteuerung durch Unbefugte, Verlust der Verfügbarkeit, Einbindung in Botnetze und Verlust der Privatsphäre / Ausspähen der Wohnung.

Smart-Home-Basisschutz:

- Software aktualisieren, wenn Sicherheitsupdates verfügbar
- Keine voreingestellten Standardpasswörter verwenden
- Firewall des Routers aktivieren
- Verschlüsselung der Kommunikation der IoT-Geräte aktivieren und IoT-Geräte nur mit dem Internet verbinden, wenn ein Fernzugriff unbedingt notwendig ist
- VPN für eine gesicherte Verbindung ins Heimnetz nutzen
- Separates WLAN für IoT-Geräte einrichten
- Physischen Zugriff auf Geräte durch Dritte verhindern
- Risiken, die mit der Nutzung von IoT-Geräten einhergehen können, bedenken

Datenschutz

Definition: Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

Definition personenbezogene Daten: alle Informationen, die sich auf identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen

Identifizierbarkeit: direkt oder indirekt, insbesondere unter Bezugnahme auf eine Kennung wie einen Namen, eine Kennnummer, Standortdaten, eine Online-Kennung, ein oder mehrere besondere Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität einer natürlichen Person sind.

Problembeschreibung

Personenbezogene Daten sind erforderlich für die Erfüllung vieler Aufgaben. Bedrohungen sind z.B. Missbrauch oder Preisgabe personenbezogener Daten, Unterwerfung unter Entscheidungen, die ausschließlich auf automatisierter Datenverarbeitung (einschließlich Profiling) beruhen, Identitätsbetrug, Überwachung durch staatliche Stellen.

Profiling: automatisierte Verarbeitung personenbezogener Daten, um bestimmte persönliche Aspekte zu bewerten oder vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortwechsel einer natürlichen Person.

Datenschutzgrundlagen

Vor dem EDV-Zeitalter:

- Die Verschwiegenheitspflicht galt traditionell für Heilberufe, Anwälte und Amtsträger.

Aufkommen der EDV:

- Mit der EDV begann die Ära der massenhaften Datenspeicherung, -verknüpfung und -auswertung.
- 1977 trat das erste Bundesdatenschutzgesetz in Kraft.
- Das Volkszählungsurteil von 1983 etablierte das "Recht auf informationelle Selbstbestimmung" als Teil des allgemeinen Persönlichkeitsrechts.
- Die EU-Datenschutzrichtlinie von 1995 führte zur Anpassung des Bundesdatenschutzgesetzes.
- 2016 wurde die EU-Datenschutz-Grundverordnung (DSGVO) eingeführt, die in der gesamten EU direkt anwendbar ist.

Das Recht auf **informationelle Selbstbestimmung** ermöglicht die Kontrolle über die Preisgabe und Nutzung persönlicher Daten. Die **EU-Charta der Grundrechte** schützt personenbezogene Daten und setzt deren Verarbeitung unter strikte Bedingungen.

Praktische Anwendung der Datenschutzgrundlagen

Die DSGVO legt fest, unter welchen Bedingungen die Verarbeitung personenbezogener Daten erlaubt ist:

- betroffene Person hat ihre Einwilligung gegeben
- zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich
- zur Erfüllung einer rechtlichen Verpflichtung erforderlich
- zum Schutz lebenswichtiger Interessen erforderlich
- zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich
- zur Wahrung von berechtigen Interessen des für die Datenverarbeitung Verantwortlichen erforderlich, sofern nicht die Interessen oder Grundrechte der betroffenen Person Vorrang haben

Die Einwilligung der betroffenen Person spielt eine zentrale Rolle und muss **freiwillig**, **informiert** und **eindeutig** erfolgen. "**Berechtigte Interessen**" können die Verarbeitung personenbezogener Daten rechtfertigen, sofern sie die Rechte der betroffenen Personen nicht überwiegen.

Besondere Kategorien wie genetische, biometrische und Gesundheitsdaten genießen zusätzlichen Schutz. Ihre Verarbeitung ist unter strengen Bedingungen und nur in Ausnahmefällen erlaubt.

Allgemeine Datenschutzgrundsätze und-techniken

Datenschutzgrundsätze wie Zweckbindung, Datenminimierung, begrenzte Speicherfristen, Datenqualität und Datensicherheit sind essenziell. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sind verpflichtend.

Technikgestaltung: geeignete technische und organisatorische Maßnahmen, um Datenschutzgrundsätze wirksam umzusetzen, z.B. Pseudonymisierung oder Sicherheit von Vertraulichkeit und Integrität unter Berücksichtigung von Stand der Technik, Implementierungskosten und Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

Die **Datenschutz-Folgenabschätzung** ist die Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten, vor der Implementierung der vorgesehenen Verarbeitungsvorgänge. Durchzuführen, wenn die Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Die Datenschutz-Folgeabschätzung bewertet Notwendigkeit, Verhältnismäßigkeit und Risiken.

Datenschutz und Ambient Intelligence

Die Herausforderung den Datenschutz in AmI-Systemen zu wahren, sind, dass der Nutzer explizit der Verarbeitung personenbezogener Daten einwilligen muss, und wie geht man mit mehreren Personen in einem System um?

Der Informationsfluss von der betroffenen Person zum Datensammler muss verringert werden und der Informationsfluss vom Datensammler zur betroffenen Person soll gesteigert werden.

Beispiel Smart-Grid

Smart Meter melden alle 15min Leistungsmesswerte, um Einspeise- und Lastregelung zu ermöglichen, der Datenkonzentrator summiert alle zu gleicher Zeit erhobenen Messwerte aus einem Teilnetz, um sie zu anonymisieren. Bedrohung durch Ausforschung von Abweichungen vom „Normalverbrauch“ und Änderung der Messwerte durch Unbefugte. Das Sicherheitsziel ist das Schützen der Vertraulichkeit und Integrität der Smart-Meter-Messwerte im gesamten Verarbeitungsprozess.

Schutzprofil definiert Sicherheitsanforderungen an eine Kategorie von Produkten, Smart Meter Gateway Protection Profile: für Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen und Security Module Protection Profile: für Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen.

Beispiel Digitaler Sprachassistent

Software, die gesprochene Sprache erkennen, verstehen und sprachgesteuerte Fragen beantworten, Dialoge führen und Assistenzdienste erbringen kann. Verarbeitet im Bereitschaftsmodus aufgenommene Sprache geräteintern und wartet auf Aufwachbefehl wie „Alexa“, „Hey Siri“, „Ok, Google“ und sendet nach Aufwachbefehl Sprachdaten zur Verarbeitung in die Cloud (auch von Personen, die nicht wissen, dass sie mitgehört werden), eine geräteinterne Verarbeitung ist aufwendig.

Empfehlungen zum Verbraucher- und Datenschutz

Siehe VL-Foliensatz 13-Datenschutz, Folie 37-45.

Editors Note: Ich vermute das dieser Abschnitt nicht Klausurrelevant ist (keine Garantie)

Identifikation

Identifikation ermöglicht die Erkennung eines Benutzers. Dies ermöglicht personalisierte Dienste in einem Mehrnutzersystem, sollte die Benutzbarkeit nicht beeinträchtigen und sollte ausreichend zuverlässig sein.

RFID (Radio Frequency Identification)

Nutztiere bekommen zum Zwecke der Identifikation Glasröhrchen mit eingebettetem Transponder (Mikrochip mit Koppelelement) implantiert. Der Mikrochip speichert ID-Nummer, die kontaktlos gelesen werden kann (meist über induktive Kopplung).

Menschen können Transponder z.B. in Form von Schlüsselanhänger, Armband oder Chipkarte tragen oder implantieren lassen.

Biometrische Erkennung

Biometrie ist die automatische Erkennung von Individuen anhand ihrer biologischen und verhaltensbezogenen Charakteristika.

Biometrische Eigenschaften müssen **universal** (möglichst bei allen Personen vorhanden), **einmalig** und **unterscheidbar** (möglichst für alle Personen unterschiedlich), **beständig** (möglichst über lange Zeit unveränderlich) und **messbar** (geeignete Sensoren verfügbar) sein.

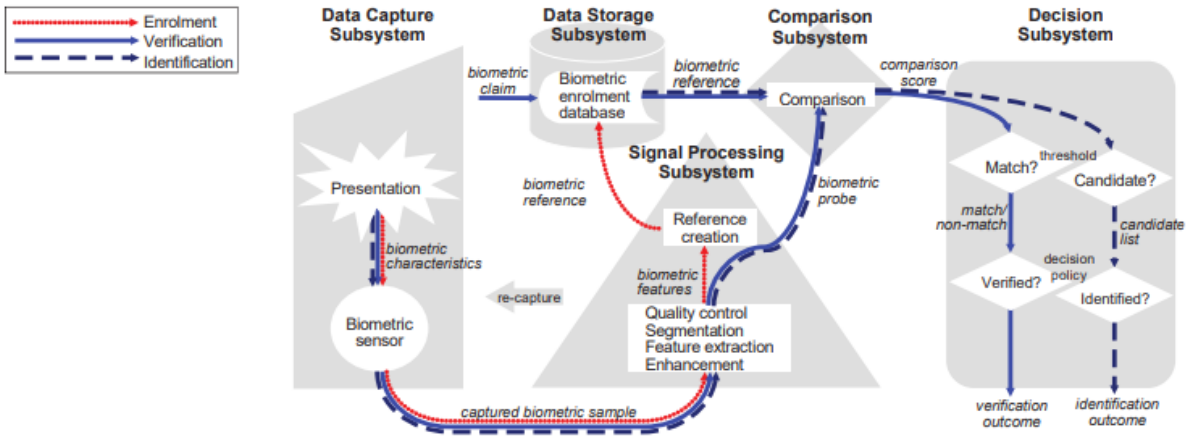
Biometrische Systeme müssen **performant** (mit verfügbaren Ressourcen ausreichende Erkennungsgenauigkeit und -geschwindigkeit erreichbar), **akzeptiert** (möglichst viele Personen zur Nutzung bereit) und **unumgehbar** (nicht leicht mit betrügerischen Methoden vorzutäuschen) sein.

Biometrische Charakteristika können entstehen durch **genotypische Anteile** (durch Vererbung weitergegeben, bei eineiigen Zwillingen gleich), **randotypische Anteile** (durch Zufallsprozesse in der embryonalen Entwicklung entstanden, selbst bei eineiigen Zwillingen verschieden) oder **konditionierte Anteile** (durch Training erworben).

Funktionsweise biometrischer Systeme

Biometrische Identifikation: Hierbei sind biometrische Daten einer zu identifizierenden Person gegeben und die biometrischen Referenzdaten von n Personen. Gesucht wird, welche Referenzdaten zu der zu identifizierenden Person gehören.

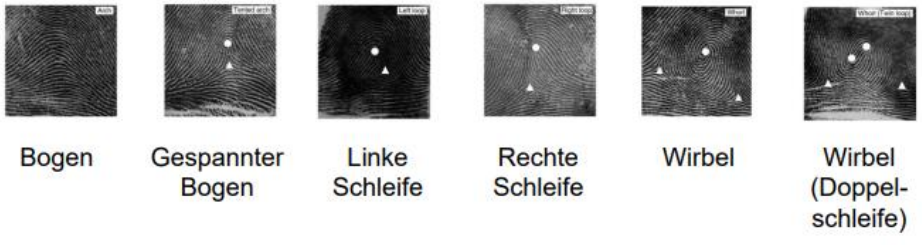
Biometrische Verifikation: Hierbei sind biometrische Daten einer zu verifizierenden Person gegeben und die biometrische Referenzdaten der Person, die die zu verifizierende Person zu sein vorgibt bzw. für die sie gehalten wird. Gesucht wird, ob die biometrischen Daten von derselben Person stammen.



Aufgenommene Daten (captured biometric sample) sind nicht für den direkten rechnergestützen vergleich geeignet aber die Grundlage für die Extraktion von Merkmalsdaten.

Merkmalsdaten (biometric features) sind für den direkten rechnergestützen Vergleich geeignet, sie benötigen weniger Speicherplatzbedarf als aufgenommene biometrische Daten und sind schneller übertragbar.

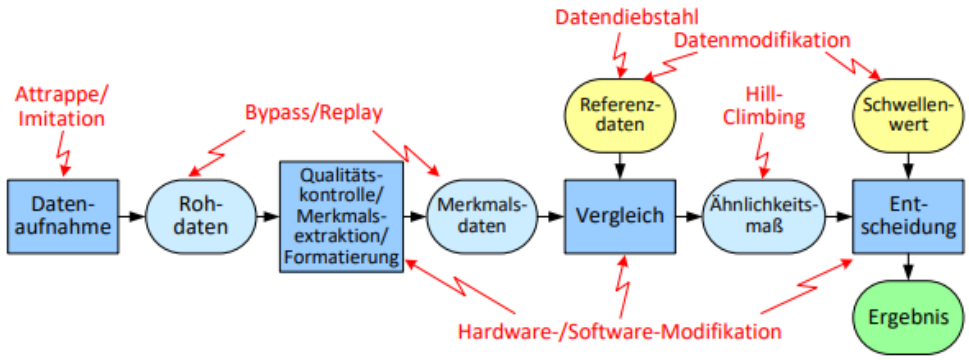
Merkmalsdatenbeispiel Finger: Anordnung der Fingerminutien. Fingerabdrücke sind unterschiedlich klassifiziert.



Wenn Merkmale verglichen werden, gibt es einen **Comparison Score**, der entweder das **Ähnlichkeitsmaß** (je ähnlciher, desto größer) oder das **Abstandsmaß** (je ähnlicher, desto kleiner) beschreibt.

Bei der Identifikation wird entweder immer ein **Eins-zu-Eins-Vergleich** vorgenommen oder die Referenzdaten werden vorgefiltert.

Mögliche Schwachstellen und Sicherheitsmaßnahmen



Biometriespezifische potenzielle **Schwachstellen** sind Erkennungsfehler, Attrappen, und erzwungene biometrische Authentisierung.

Erkennungsfehler

Auch bei ordnungsgemäßer Nutzung können Fehler auftreten.

Type-I-Fehler (fälschlicherweise nicht erkannt): Ursachen können Variabilität der biometrischen Merkmale oder Störsignale, mögliche Folgen sind beeinträchtigte Benutzbarkeit.

Type-II-Fehler (fälschlicherweise erkannt): Ursachen können Ähnlichkeit der biometrischen Merkmale verschiedener Personen oder ineffektive Vergleichsalgorithmen sein, mögliche Folgen sind beeinträchtigte Sicherheit!

Performantmetriken

Verifikation:

- **FMR** (False Match Rate): Anteil der Vergleiche nicht zusammenpassender biometrischer Daten, bei denen diese fälschlicherweise als zusammenpassend angesehen werden
- **FNMR** (False Non-Match Rate): Anteil der Vergleiche zusammenpassender biometrischer Daten, bei denen diese fälschlicherweise als nicht zusammenpassend angesehen werden
- Sinkt die FMR, steigt die FNMR und umgekehrt

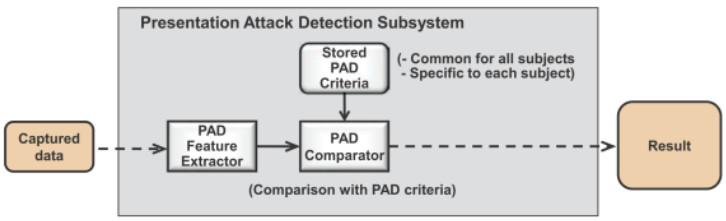
Identifikation:

- **FPIR** (False Positive Identification Rate): Anteil der Recherchen anhand von biometrischen Proben von nicht registrierten Personen, bei denen das Ähnlichkeitsmaß des ähnlichsten Kandidaten einen Schwellwert übersteigt
- **Rang-k-FNIR** (Rang-k-False Negative Identification Rate): Anteil der Recherchen anhand von biometrischen Proben von registrierten Personen, bei denen unter den ähnlichsten k Kandidaten kein Treffer ist
- hängen von der Größe der Referenzdatenbank ab, je größer die Referenzdatenbank, desto höher werden die Fehlerraten
- Sinkt die FPIR, steigt die FNIR und umgekehrt

DET (Detection Error Trade-Off)-Kurve: Geordnete Paare aus Falsch-Positiv-Rate (FMR oder FPIR) und zugehöriger Falsch-Negativ-Rate (FNMR oder Rang-1-FNIR) bei gleicher Schwellwerteinstellung

Präsentationsangriffe

Präsentation nachgemachter oder natürlicher biometrischer Charakteristika am biometrischen Aufnahmegerät in einer Weise, die die beabsichtigte Funktion des biometrischen Systems beeinträchtigen kann. Zum Beispiel Fingerabdruckattrappen, ausgedruckte Gesichtsbilder, auf einem Bildschirm abgespielte Aufnahmen oder Silikonmasken, Kontaktlinsen mit aufgedrucktem Irismuster. Biometrische Merkmale können nicht wie Passwörter beliebig ersetzt werden, falls Angriffe erfolgreich sind.



Multibiometrische Fusion

Zusammenfassung der Vergleichsergebnisse für verschiedene biometrische Charakteristika der gleichen Person, für verschiedene Aufnahmen der gleichen biometrischen Charakteristika oder von verschiedenen Algorithmen. Dies kann Erkennungsleistung und Benutzbarkeit erhöhen und biometrische Präsentationsangriffe erschweren.

Rechenbeispiele

I²C Beispiel

Wie viele Sensorwerte können maximal pro Sekunde von allen Sensoren mit sequentiellen Messungen abgefragt werden?

Wir haben gegeben:

- Datenrate: 100 kbit/s
- Eine Nachricht zum Starten der Messung (Datenlänge 1 Byte)
- Wartezeit für die Messung: 10ms
- Eine Nachricht zum Abholen der Messung (Datenlänge 4 Bytes)
- Anzahl an Slaves im Bus: 12 Sensoren

$T_{Bit} = \frac{1}{f} = \frac{1}{100kbit/s} = 10us$

$$T_{Message} = T_{Bit} + 7\,T_{Bit} + T_{Bit} + T_{Bit} + \left(\sum_{i=1}^{k} 8\,T_{Bit} + T_{Bit}\right) + T_{Bit} = 11T_{Bit} + \sum_{i=1}^{k} 9\,T_{Bit}$$

Start Adresse R/W ACK Data Bytes + ACK Stopp

$T_{Message,Start} = 20T_{Bit} = 20 \cdot 10us = 0{,}2ms$

$T_{Measurement} = 10ms$ Wartezeit für die Messung

$T_{Message,ReturnMesurementData} = 11T_{bit} \sum_{i=1}^{4} 9T_{Bit} = 47T_{Bit} = 0{,}47ms$ Messwert für 4 Bytes

$T_{Cycle} = T_{Message,Start} + T_{Measurement} + T_{Message,ReturnMesurementData} = 10{,}67\ ms$

$f_{Cycle,1} = \frac{1}{T_{Cycle} \cdot N} = 93{,}72Hz$ Für N = 1 Sensor

$f_{Cycle,1} = \frac{1}{T_{Cycle} \cdot N} = 7{,}81Hz$ Für N = 12 Sensoren

Antwort: Man erhält maximal 7,81 Werte pro Sekunde und Sensor. Darauf basierend werden 7,81 neue Handpositionen pro Sekunde errechnet.

Kernkompetenzen für die Klausur

Sie …

Sensoren und Aktoren

- können definieren was ein Sensor/Aktor ist,
- können die Funktionsweise von kapazitiven Sensoren erläutern,
- können Beispiele geben für verschiedene Arten von Sensoren

Mikrocontroller

- können Mikrocontroller zu anderen Rechnersystemen abgrenzen und die Hauptkomponenten erklären (Steuerwerk, Rechenwerk, Speicherwerk, Eingabe-/Ausgabewerk).
- können die Funktionsweise des Rechen- und Steuerwerks anhand von Pseudo-Code beschreiben.
- kennen die Eigenschaften der Von-Neumann- und Harvard-Architektur.
- wissen, was Interrupts sind, und können diese einordnen.
- können die Funktionsweise verschiedener ADCs und typische Wandlungsfehler an Beispielen beschreiben

Kommunikation

- können (syntaktische/semantische) Interoperabilität definieren
- können Beispiele für verschiedene Topologien von Netzwerktechnologien benennen
- können erklären, was ein Bus ist
- können I²C/SPI-Beispielsysteme und andere Bussysteme entwerfen und skizzieren
- können I²C-Kommunikation interpretieren
- können die Grundlagen von drahtlosen Systemen vermitteln

Smart Home und Smart Building

- kennen die Begriffe Smart Home und Smart Building und können sie beschreiben
- können Anwendungsbereiche zu den Bereichen Smart Home und Smart Building zuordnen
- können Gebäudeebenen erklären
- können Schritte zur Sanierung eines Smart Home nennen
- kennen verschiedene individuelle Anpassungen und wissen über deren Zukunftsfähigkeit bescheid
- können Hauptanwendungsbereiche im Smart Building nennen
- kennen die Digitalisierung der Energiewende in Form des Messstellenbetriebsgesetzes und der Heizkostenverordnung
- können Beispiele von Chancen und Herausforderungen nennen.

Smart City

- können die typischen Handlungsfelder einer Smart City nennen
- können Beispiele von Smart City Anwendungen geben
- können beschreiben wie Anomaly Detection mit Autoencodern funktioniert
- können Konflikte beschreiben, die aus Technik resultieren

Benutzerinteraktion

- Konzepte nennen können, die zu einem guten konzeptionellen Modell beitragen
- die Definition von impliziter und expliziter Interaktion erklären und entsprechende Beispiele nennen können
- Regeln für gutes Design verstehen und mögliche Verletzungen erkennen können
- die Modalitäten in HCI kennen und nennen können
- erklären können, was multimodale Interaktion bedeutet
- zwei aktuelle Forschungsbeispiele im Bereich HCI nennen können

Context-Awareness

- kennen die Begriffe Kontext und Context-Awareness und können sie beschreiben.
- können Kontextkategorien nennen, beschreiben und Kontexte zuordnen.
- kennen die Eigenschaften von Kontext und können sie erklären.

- können die Komponenten einer kontextabhängigen Datenverwaltung erklären.
- kennen verschiedene Ansätze zur Kontextmodellierung und Wissen über deren Vorteile und Nachteile Bescheid.
- können Methoden zum Schutz der Privatsphäre nennen und deren Schritte und Zusammenhänge benennen.
- kennen Typen von Reasonern.

Sicherheit

- kennen die Bedrohungen, dehnen AmI-Systeme ausgesetzt sind.
- kennen die IT-Sicherheitsziele.
- kennen die IT-Sicherheitsmaßnahmen in AmI-Systemen.
- wissen, wie geeignete IT-Sicherheitsmaßnahmen ausgewählt werden.

Datenschutz

- wissen, was personenbezogene Daten sind und unter welchen Bedingungen diese verarbeitet werden dürfen
- können Datenschutzprobleme von AmI-Systemen aufzeigen und bewerten

Identifikation

- kennen die Vorteile von Benutzeridentifikation in AmI-Systemen.
- Wissen, was biometrische Merkmale sind und was diese auszeichnet.
- Kennen den Unterschied zwischen biometrischer Identifikation und Verifikation.
- Wissen, wie man die Erkennungsgenauigkeit biometrischer Systeme bewertet.
- Kennen die möglichen Schwachstellen biometrischer Systeme und Sicherheitsmaßnahmen.

Nicht-Lernziele

Sie …

Mikrocontroller

- können einen Mikrocontroller elektronisch korrekt skizzieren.
- kennen sämtliche Registerschaltungen und FlipFlop-Varianten.
- 30 verschiedene Anwendungsgebiete für ADCs aufzählen.
- kennen sich perfekt mit Schaltnetzen und allen Logikgattern aus