



Unternehmen für Bildung.

Cyber-physische Systeme ergänzen

Modul: **ITG / H**

Version: 1.0
September 2022

Erstellt von: IT-Abteilung

Modul: **ITG / H - Cyber-physische Systeme ergänzen**

Version, Datum: 1.0, September 2022

Erstellt von: IT-Abteilung

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie oder einem anderen Verfahren) ohne Genehmigung des Herausgebers reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Die Modulunterlage und alle ihre Bestandteile wurden mit großer Sorgfalt erstellt und geprüft. Dennoch können Fehler nicht vollkommen ausgeschlossen werden. Der Herausgeber und die Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Literaturhinweis

Titel: IT-Berufe Grundstufe

ISBN: 978-3-14-220000-2

Verlag: Westermann Gruppe

Inhalt

TAG 1 – Grundlagen von cyberphysischen Systemen erarbeiten	6
LE 1 - Eine Einführung in das Internet of Things erarbeiten.....	8
LE 2 - Einflussfaktoren auf die technologische Entwicklung von cyber-physischen Systemen beschreiben.....	10
Lernzielkontrolle TAG 1	11
TAG 2 - Anwendungsfelder von cyber-physischen Systemen im Internet of Things unterscheiden	12
LE 1 - Smart Home - Energie- und Gebäudetechnik.....	12
LE 2 - Intelligente Fertigung und das Industrial Internet of Things (IIoT)	13
LE 3 - Automotive-Bereich	15
LE 4 - Smart Health – Gesundheitswesen.....	17
LE 5 - Smart Cities - intelligente Städte	17
LE 6 - Consumer-Bereich	18
Lernzielkontrolle TAG 2	20
TAG 3 - Den strukturellen Aufbau von cyber-physischen Systemen definieren	21
LE 1 – Sensorik.....	22
LE 2 - Regelung mittels intelligenter Sensorik	25
LE 3 - Einplatinencomputer als Basis für cyber-physische Systeme.....	25
LE 4 - Mikrocontrollerboards als Basis für cyber-physische Systeme.....	26
LE 5 - Unterscheidung von Einplatinencomputer und Mikrocontroller	27
LE 6 - Mikrocontroller und das Internet of Things.....	27
Lernzielkontrolle TAG 3	28
TAG 4 - Kommunikation zwischen cyber-physischen Systemen präsentieren	29
LE 1 - IoT-Protokolle und Industrial-Internet-Protokolle unterscheiden.....	29
LE 2 - Die Anbindung von cyber-physischen Systemen mit dem MQTT-Protokoll beschreiben	33
LE 3 - Client-Server-(Broker)-Prinzip	34
LE 4 - Quality of Service und Last Will Testament	36
LE 5 - Message Persistence - Beharrlichkeit einer Nachricht	37
LE 6 - Eigenschaften von MQTT.....	38
LE 7 – Machine-to-Machine-Kommunikation mit dem Standard „OPC UA“ untersuchen	38
Lernzielkontrolle TAG 4	40
TAG 5 - Ein bestehendes cyber-physisches System im Unternehmen analysieren.....	41
LE 1 - Den Datenfluss an CPS-Schnittstellen und innerhalb eines Netzwerks vergleichen	43
LE 2 - Energie-, Stoff- und Informationsflüsse eines exemplarischen cyber-physischen Systems erläutern	46
Lernzielkontrolle TAG 5	49
TAG 6 - Erweiterungen für ein cyber-physisches System planen.....	50
LE 1 - Ein Projekt zur CPS-Erweiterung initiieren und die Anforderungen des Auftraggebers abstimmen.....	51
LE 2 - Requirements Engineering.....	51
LE 3 – Stakeholder	53
LE 4 – Akzeptanzkriterien	54
Lernzielkontrolle TAG 6	55
TAG 7 - Eine Projektplanung durchführen	56

LE 1 - DevOps-Ziele	56
LE 2 - DevOps-Konzept und DevOps-Ansatz.....	56
LE 3 - DevOps-Kultur	57
LE 4 - DevOps-Phasen	58
LE 5 - Versionsverwaltung mit Git	59
Lernzielkontrolle TAG 7	61
TAG 8 - Ein cyber-physisches System in Betrieb nehmen	62
LE 1 - Sie sollen einen Prototyp aufbauen	62
LE 2 - Software des erweiterten cyber-physischen Systems programmieren	63
LE 3 - MQTT-Broker und Client verbinden	64
LE 4 - Die Funktionalität der CPS-Erweiterung prüfen und protokollieren	65
LE 5 - Im Review Projektergebnisse und -erkenntnisse erfassen	66
Lernzielkontrolle TAG 8	67
TAG 9 - Ein cyber-physisches System optimieren	69
LE 1 - Bestehende Gefahren für die Betriebs- und Datensicherheit durch den Einsatz des cyber-physischen Systems erkennen	69
LE 2 - CPS-Systemausfälle mittels FMEA minimieren	70
LE 3 - Verbesserungsvorschläge dem Auftraggeber vorstellen	74
LE 4 - Betriebliches Vorschlagswesen (BVW).....	74
LE 5 - Elevator Pitch	75
Lernzielkontrolle TAG 9	76
TAG 10 - Vertiefung des Wissens und Modulprüfung	77
LE 1- Einleitung.....	77
LE 2 - Modulprüfung	77

In diesem Modul wird die wachsende Bedeutung des Internet of Things (IoT) verdeutlicht. Der dynamisch wachsende Einsatz von sogenannten cyber-physischen Systemen vernetzt alle Bereiche des täglichen Lebens und auch die industrielle Produktion. Sprachassistenten, Sensoren aller Art, Fitnessarmbänder, Autos, Maschinen und Anlagen - das Internet of Things verbindet bereits Milliarden von Endgeräten miteinander. Des Weiteren steht Industrie 4.0 für die intelligente, sensorgestützte und nahezu selbststeuernde Produktion über miteinander vernetzte Produktionssysteme, in denen die meisten Prozesse automatisiert ablaufen. Um die Funktion von cyber-physischen Systemen darzulegen, werden in diesem Modul die Grundlagen, die Analyse von Kundenanforderungen und die Implementierung von cyberphysischen Systemen detailliert erarbeitet.

TAG 1 – Grundlagen von cyberphysischen Systemen erarbeiten

Entsprechend dem Ausbildungsplan kommen Sie in der zweiten Hälfte Ihrer Ausbildung als Fachinformatikerin oder Fachinformatiker in die Entwicklungsabteilung des IT-Systemhauses JIKU IT-Solutions. Ein Team der Entwicklungsabteilung beschäftigt sich momentan mit der Erweiterung des Smart-Home- und Smart-Factory-Produktportfolios. Es wird gezielt nach neuen Einsatzgebieten von cyber-physischen Systemen gesucht. Die Auszubildenden sollen sich in kleinen Teams die Grundlagen von cyber-physischen Systemen erarbeiten.



Ausbildungsplan für den Unternehmensbereich „Entwicklung“

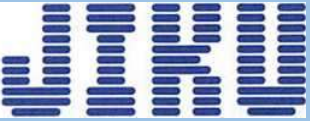
Schwerpunktthema „Industrial Internet of Things“ und „Digital Workplace Solutions“

Zeitraum: zweite Hälfte des 2. Ausbildungsjahres

In unserer Entwicklungsabteilung werden die Auszubildenden folgende Schwerpunkte kennenlernen und bearbeiten:

- Einsatz von cyber-physischen Systemen in der Industrie (Smart Factories)
- Anwendungsbereiche des Internet of Things am Arbeitsplatz (Digital Workplace Solutions)

In einer ersten Besprechung verdeutlicht die Abteilungsleitung, warum die Weiterentwicklung von IT-Lösungen im Bereich von Industrial-A-O-IT-Solutions und im Bereich der Digital Workplace Solutions von sehr hoher Priorität für das Unternehmen JIKU IT-Solutions ist (siehe Leistungsportfolio). Beide Bereiche verzeichnen ein hohes Marktwachstum und sind daher von strategischer Bedeutung für das Unternehmen.



Systemhaus
Ausbildung
Portfolio
Social Responsibility

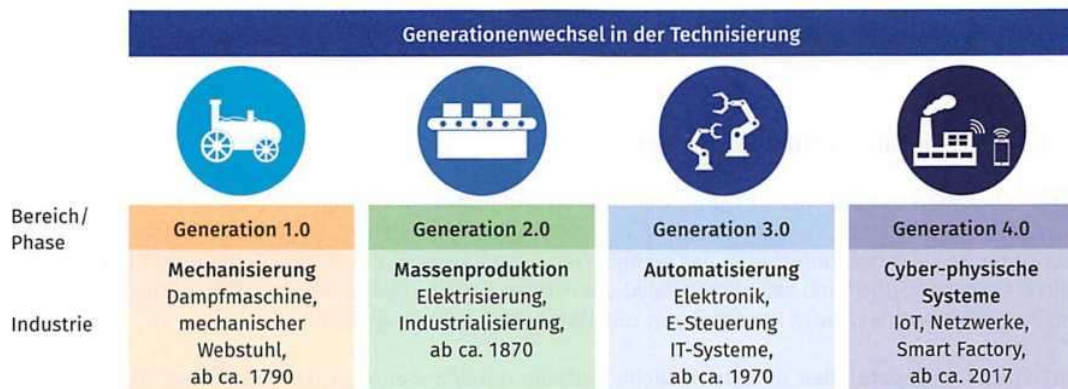
IT-Solutions und Expertise in der Systemhausgruppe

Unser Produkt- und Dienstleistungsportfolio im Bereich des Industrial Internet of Things und Digital Workplace Solutions

Wir bieten Ihnen ein umfassendes Portfolio an Produkten und Dienstleistungen, um Ihr Unternehmen fit für die neuesten Veränderungen durch die Digitalisierung zu machen.

- **Reifegradanalyse**
 - Ist-Analyse Ihrer bestehenden Infrastruktur in Büro und Produktionsbereich
 - Darstellung des Potenzials aus technologischer, ökonomischer und ökologischer Sicht
- **Installation und Vernetzung von cyber-physischen Systemen**
 - Integration von IoT-Devices in allen Arbeitsbereichen
 - Nach- und Umrüsten (Retrofitting) von bestehenden Maschinen und Anlagen
- **Datenanalyse und Reporting der CPS-Informationen**
 - Datenerfassung und -analyse in der Cloud
 - Big Data Analytics mittels künstlicher Intelligenz (KI)
 - Umfassendes Echtzeit-Reporting
- **Schulung und Betreuung der IT-Solutions**
 - Trainingsangebot für Ihr Personal aus allen Unternehmensbereichen

Das starke Wachstum ist getrieben durch die fortschreitende Digitalisierung in allen Bereichen des Lebens. Die vierte industrielle Revolution kennzeichnet den Übergang von der reinen Automatisierung in eine neue technologische Generation 4.0, die durch den Einsatz von cyber-physischen Systemen im Internet of Things gekennzeichnet.



Im industriellen Umfeld steht die sogenannte Smart Factory im Mittelpunkt der Industrie 4.0 und beschreibt eine Produktionsumgebung, die sich selbst organisiert und optimiert. Zu diesem Produktionsumfeld gehören neben Maschinen und Anlagen auch die Intralogistik und natürlich auch der Mensch, der in zukünftige Produktionsprozesse wesentlich weniger eingreifen soll. Basis solcher Smart Factories sind die sogenannten cyber-physischen Systeme, die die intelligente Vernetzung von Maschinen untereinander aber auch die Vernetzung der Wertschöpfungskette von den Lieferanten bis hin zu den Kunden ermöglichen. Es ist wichtig zu unterscheiden, dass die reine Automatisierung von Prozessen oder der Einsatz von IT in den Bereichen der Produktion nicht bereits das Konzept der Industrie 4.0 umfasst. Die

Unterscheidung liegt vielmehr im Einsatz von netzwerkfähigen, modularen Produktionseinheiten, die intelligent und autonom agieren können.

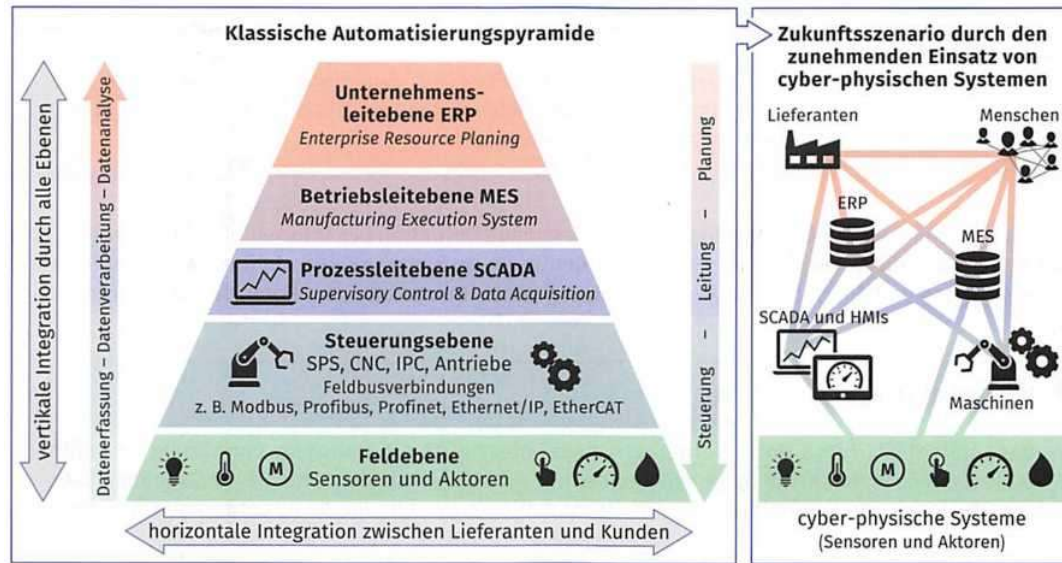
Im Bereich des Gebäudemanagements steht der Begriff des Smart Home im Vordergrund. Dieser dient als Oberbegriff für den technischen Einsatz von cyber-physischen Systemen in Wohnräumen, Häusern und Bürogebäuden. Im Mittelpunkt stehen Energieüberwachung und Energiemanagement sowie die Erhöhung von Wohn- und Lebensqualität. Smart Home beschreibt die Vernetzung von Haushaltsgeräten, Unterhaltungselektronik und Elementen der Energie- und Gebäudetechnik eines Hauses. Komponenten des Smart Homes können über das Internet angesprochen werden und lassen sich über mobile Apps überwachen und steuern.

Grundbegriffe der Industrie 4.0	
Cyber-physische Systeme (CPS)	CPS sind ein Verbund aus informatischen und softwaretechnischen Komponenten mit mechanischen wie auch elektrischen Teilen, die mit IT-Systemen vernetzt kommunizieren.
Cyber-physische Produktionssysteme (CPPC)	CPPC sind entsprechende cyber-physische Systeme, die im industriellen Umfeld in modernen Produktionsmaschinen und -anlagen zum Einsatz kommen.
Internet of Things (IoT)	Das IoT ist ein Sammelbegriff für die unterschiedlichsten Technologien einer global vernetzten Infrastruktur, die sowohl physische als auch virtuelle Objekte über das Internet verbindet.
Industrial Internet of Things IIoT)	Das IIoT beschreibt industrielle Anwendungen im Internet of Things. Hierbei steht besonders die Vernetzung mit Maschinen und Anlagen mittels intelligenter Sensorik im Vordergrund.
Smart Factory	Die Smart Factory bezeichnet eine sich selbst organisierende und optimierende Produktionsumgebung, in der mittels cyberphysischen Systemen Maschinen und Anlagen miteinander vernetzt sind.
Smart Home	Smart Home ist der Oberbegriff für den Einsatz von cyber-physischen Systemen in Wohn- und Bürogebäuden zur Erhöhung der Wohn- und Lebensqualität und zum intelligenten Energiemanagement.

LE 1 - Eine Einführung in das Internet of Things erarbeiten

Das Internet of Things liefert eine der technischen Grundlagen, in der Gegenstände untereinander und mit Menschen zeitlich und räumlich nahezu unbegrenzt kommunizieren können. Jeder Haushaltsgegenstand, jede Maschine, jedes Produkt kann zum Datenproduzenten werden.

IoT-Plattformen verbinden unterschiedliche Systeme miteinander. Dies bedeutet, dass sie mit unterschiedlichen Standards, Formaten und Schnittstellen zurechtkommen müssen. Die unterschiedlichen Systeme können zum einen Business-Anwendungen wie CRM oder ERP sein, mobile Apps, aber auch Daten aus der Fertigung (MES, SCADA, HMI, SPS, siehe Schaubild). Daher sind offene Schnittstellen (API, Application Programming Interface) unerlässlich.



In der folgenden Auflistung werden die wesentlichen Grundlagen für ein modulares IoT - Ecosystem aufgezeigt. Die ganzheitliche Betrachtung aller Anforderungen ist notwendig, um für die weitere technologische Entwicklung gut gerüstet zu sein.

Anforderungen und technische Grundlagen für das Internet of Things

Konnektivität

Auf einer IoT-Plattform laufen die unterschiedlichsten Daten von zahlreichen Geräten und cyber-physischen Systemen zusammen. Dies können unter anderem Informationen von Maschinen, Anlagen, der Energieversorgung von Gebäuden und Produktionsbereichen oder des Fuhrparks sein. Daher müssen IoT-Plattformen mit den zahlreichen Funktechnologien und Industrie-Standardprotokollen zurechtkommen. Hierzu sind exemplarisch die Funktechniken 4G/5G, Bluetooth, WLAN, ZigBee, Z-Wave und Industrieprotokolle wie OPC UA oder Modbus zu nennen.

Offene Schnittstellen

Nicht zuletzt sind in Bezug zur Konnektivität offene Anwendungsprogrammierschnittstellen erforderlich. Diese Schnittstellen werden Application Programming Interface (API) genannt und ermöglichen den Entwicklern den universellen Zugriff auf den Dienst.

Management

Für ein optimales Management der IoT-Plattformen sind eine zentrale Steuerung und Überwachung von Vorteil, die wiederum die Fernwartung in Bezug auf Software-Updates, Tests oder Fehlerbehebung ermöglichen.

Datenanalyse

IoT-Plattformen können Datenanalyse in Echtzeit durchführen. Diese Daten werden unter anderem auf Muster und Abweichungen hin untersucht und die daraus abgeleiteten Ergebnisse zur Prozessoptimierung eingesetzt. Die Themen der künstlichen Intelligenz und vor allem des maschinellen Lernens sind hierbei von sehr großer Bedeutung.

Reporting

Die Visualisierung der Daten und Analyseergebnisse können sehr übersichtlich auf Dashboards dargestellt werden. Diese Berichtsfunktion ist schon bei kleinen Projekten mit cyber-physischen Systemen leicht zu bewerkstelligen.

Sicherheit

Sicherheit ist im Internet of Things von sehr großer Relevanz. Funktionen wie Authentifizierung, Verschlüsselung oder geschützter Datentransfer müssen gewährleistet sein, um vor möglichen Angriffen und unberechtigtem Zugriff zu schützen.

Generell sind drei Grundvoraussetzungen für eine genaue Definition des Internet of Things von sehr großer Bedeutung: die Verbindung von Gegenständen in einem Netzwerk, die eindeutige Adressierbarkeit eines Objektes und die Nutzung von einheitlichen Standardprotokollen zur Kommunikation untereinander.

Internet of Things

Das Internet of Things (IoT, Internet der Dinge) beschreibt die weltweite Vernetzung von unterschiedlichen Objekten, die durch eine eindeutige Adresse erreichbar sind. Bei der Kommunikation der Objekte werden einheitliche Standardprotokolle eingesetzt, um die Interoperabilität sicherzustellen.

LE 2 - Einflussfaktoren auf die technologische Entwicklung von cyber-physischen Systemen beschreiben

Statistische Daten belegen den Trend der internetfähigen Geräte als Massenprodukte, der im Kontext der digitalen Transformation die Zukunftstechnologien antreibt.

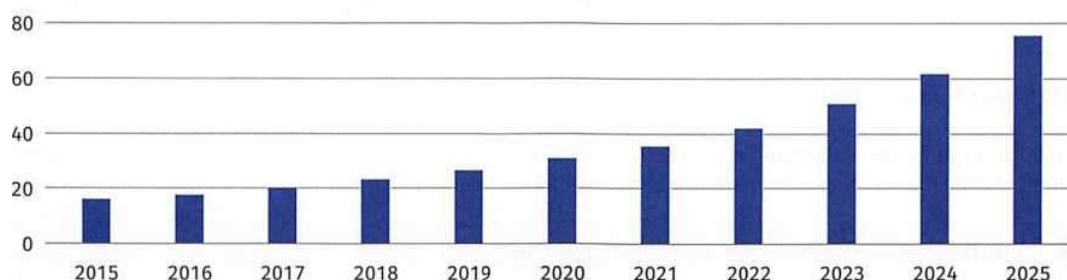
Einflussfaktoren auf das Internet of Things

Rechenleistung steigt stetig	Konnektivität wird flächendeckender	Kosten und Größe der Hardware sinken
- Trotz steigender Rechenleistung sinken die Kosten für Rechenleistung und zur Speicherung von Daten. - Der Energiebedarf für den Betrieb einzelner IoT-Komponenten wird trotz höherer Rechenleistung geringer.	- Die Kosten zur Übertragung von Daten sind deutlich gefallen. - Die Netzabdeckung durch unterschiedliche Funktechnologien hat sich deutlich verbessert.	- Sensoren werden immer kleiner bei permanentsinkenden Kosten. - Neue Einplatinencomputer und Mikrocontroller ermöglichen neue IoT-Anwendungen.

Wenn man die wesentlichen Einflussfaktoren auf das Internet of Things (IoT) betrachtet, wird deutlich, dass die technologischen Entwicklungen im Bereich der Rechenleistung von Prozessoren, der flächendeckenden Konnektivität und der Miniaturisierung von Sensoren die Entwicklung stark vorantreiben. Des Weiteren sinken die Kosten und der Energiebedarf einzelner Komponenten.

Was sich im ersten Moment positiv in Bezug auf die Nachhaltigkeit anhört, wird leider durch die Gesamtfolgen der weltweit vernetzten cyber-physischen Systeme überkompensiert. Die einzelnen Einheiten benötigen zwar weniger Energie, doch die Gesamtzahl an global eingesetzten cyber-physischen Systemen steigt sehr stark an. Das folgende Diagramm zeigt die weltweite Entwicklung von vernetzten IoT-Devices zwischen 2015 und 2025. Diese Überkompensation wird als Rebound-Effekt bezeichnet, durch den ein mögliches Einsparpotenzial durch das Verhalten der Verbraucher wieder teilweise oder sogar komplett eliminiert wird.

Entwicklung der IoT-Devices in Milliarden von 2015 bis 2025



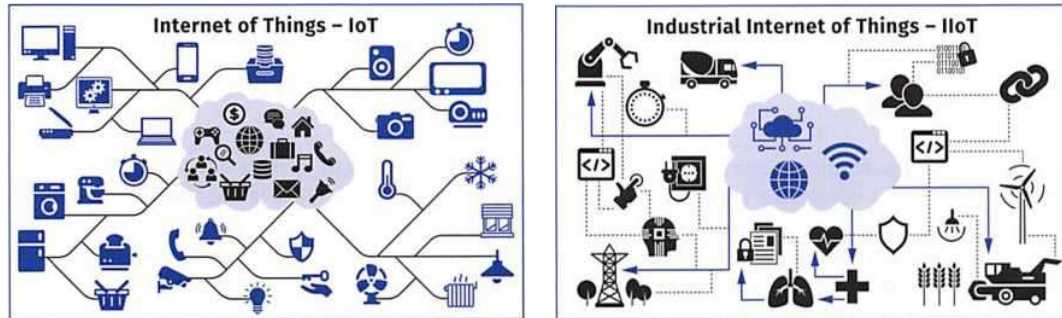
Es wird prognostiziert, dass sich von 2015 bis 2025 die Anzahl der IoT-Devices verfünffachen wird.

Lernzielkontrolle TAG 1

1. Nennen Sie wesentlichen Unterschiede zwischen den Zielsetzungen von Smart Factories und Smart Homes.
2. Beschreiben Sie die unterschiedlichen Anforderungen an eine IoT-Plattform und stellen diese in einer strukturierten Mindmap dar.
3. Führen Sie im Internet weitere Recherchen zum Begriff "Rebound-Effekt" durch und erläutern Sie diesen zusammen mit der steigenden Anzahl von cyber-physischen Systemen an einem Beispiel Ihrer Wahl.

TAG 2 - Anwendungsfelder von cyber-physischen Systemen im Internet of Things unterscheiden

Cyber-physische Systeme spielen heute in vielen Alltagsbereichen eine wichtige Rolle. Sei es im privaten Umfeld, bei der Arbeit im Büro, in den Fertigungen von Industrieunternehmen, der Landwirtschaft oder im Gesundheitswesen. Jeder Lebensbereich wird heute durch den Einsatz von cyber-physischen Systemen verändert.



Im Folgenden werden Anwendungsfelder von cyber-physischen Systemen in sechs Einsatzbereichen näher beschrieben. Allein diese decken bereits ein beachtliches Spektrum an möglichen Funktionen ab. In Kombination mit Dienstleistungen oder neuen Geschäftsmodellen ist die weitere Entwicklung nicht vorhersehbar.

LE 1 - Smart Home - Energie- und Gebäudetechnik

Nicht nur Computer, Smartphone und Fernseher sind in der Zwischenzeit mit der Haustechnik vernetzt. Immer mehr Haushaltsgeräte werden integriert, die das Wohnen sicherer und komfortabler machen.

Einsatzgebiete in der Energie- und Gebäudetechnik

Haushaltsgeräte und Komfort

Moderne Kühlschränke sind nicht mehr nur dazu da, um Lebensmittel frisch zu halten. Viel mehr sorgt innovative Smart-Home-Technik für ein komfortableres und effizienteres Haushalten. Bei einem Modell mit Kamera kann der Besitzer beispielsweise während des Einkaufs überprüfen, was sich noch im Kühlschrank befindet und was noch besorgt werden muss. Multimedia-Anlagen können so eingestellt werden, dass während des Einschaltens bereits das Licht im Raum gedimmt wird und Jalousien automatisch bei Sonneneinstrahlung nach unten fahren.

Energieversorgung

Das Smart Home hilft, Energiekosten einzusparen. Es kann beispielsweise die Heizung automatisch ausschalten, wenn Fenster und Türen geöffnet sind oder das Licht wird ausgeschaltet, sobald niemand mehr im Raum ist. Im Bereich der Energieversorgung steht die Einsparung von Heizenergie im Vordergrund. Neben dem Einsatz von Smart-Home-Anwendungen im Neubau können auch bestehende Gebäude nachgerüstet werden. Viele Funktionen werden per App gesteuert. Ist man im Urlaub, so kann man z.B. die Beleuchtung nach Belieben so einstellen, dass abends das Licht zu unterschiedlichen Zeiten angeht oder sich die Rollläden automatisch schließen.

Sicherheit

Wenn ein Haus dunkel ist, signalisiert es Einbrechern, dass niemand zu Hause ist. Smart-Home-Steuerungen können die Anwesenheit von Bewohnern auf geschickte Weise simulieren. Das Smart Home schaltet automatisch das Licht ein. Ob zu einer bestimmten Zeit oder in der Abenddämmerung. Zusätzlich fährt die Jalousiesteuerung die Rollläden herunter. Gekippte Fenster laden die Täter ein, in das Gebäude einzubrechen. Intelligente Sensoren können Gefahren erkennen, die Anwohner benachrichtigen und sogar Fenster aus der Ferne schließen lassen. Wenn jemand versucht in das Haus einzubrechen, kann eine App sofort die Anwohner oder einen Sicherheitsdienst benachrichtigen.

LE 2 - Intelligente Fertigung und das Industrial Internet of Things (IIoT)

Für die Smart Factory hat sich im industriellen Umfeld der Begriff "Industrial Internet of Things" durchgesetzt. Im Gegensatz zum Internet of Things konzentriert sich IIoT auf die Umsetzung von industriellen Einsatzgebieten. Höhere Variantenvielfalt, kurze Lieferfristen, schnelle Prozessanpassungen, sehr kleine Losgrößen und viele mehr, sind alles Indikatoren, dass die Anforderungen an die Produkte, die Geschäftsprozesse und an die Produktion ständig wachsen. Des Weiteren wird die Kommunikation zwischen den Maschinen untereinander (M2M = Machine-to-Machine) immer wichtiger. All dies führt zu einer enorm gestiegenen Komplexität in der Planung und Ausführung. Die folgende Auflistung beschreibt vier wesentliche Handlungsfelder für Einsatzgebiete von cyber-physischen Systemen in der industriellen Fertigung.

Handlungsfelder für Einsatzgebiet von cyber-physischen Systemen in der Smart Factory

Produktionsplanung

Cyber-physische Systeme unterstützen die Planung durch Echtzeitmeldungen der momentanen Ressourcenbelegungen und dem aktuellen Personaleinsatz. Neben der Reihenfolgeplanung von Kundenaufträgen und Arbeitsgängen kann auch der Einsatz von Material und Energie dem aktuellen Bedarf entsprechend optimiert werden und somit Kosten durch verbesserten Maschinen- und Personaleinsatz eingespart werden.

Produktionssteuerung

Alle Prozesse können in Echtzeit mittels cyber-physischen Systemen online überwacht werden. Die durchgängige Überprüfung der Produkt- und Prozessqualität ermöglicht die Früherkennung von Abweichungen und ist daher ein wertvolles Hilfsmittel zur Fertigungssteuerung.

Vorhersage

Durch die erfassten Daten lassen sich unterschiedliche Vorhersagen treffen. Dies sind beispielsweise die Materialreichweite, Produktions-, Versand- und Liefertermine, die zu erwartende Qualität oder bevorstehende Instandhaltungsmaßnahmen.

Analyse

Die Analyse der Daten ermöglicht die Bereitstellung von Kennzahlen und Key Performance Indicators (KPI) online. Durch maschinelles Lernen aus sehr großen Datenmengen (Big Data) können Langzeitanalysen durchgeführt werden, die unter anderem Optimierungspotenziale identifizieren können, was ohne den Einsatz von künstlicher Intelligenz (KI) nicht möglich gewesen wäre.

Für alle vier Handlungsfelder lassen sich konkrete Anwendungsgebiete für die Industrie 4.0 ableiten. Die folgende Tabelle beschreibt Optimierungsziele und die möglichen Anwendungsgebiete in der Smart Factory.

Anwendungsgebiete in der Industrie 4.0	
Unternehmensziele	Möglicher Ansatz, mittels cyber-physischen Systemen realisierbar
Maschinenverfügbarkeit in der Produktion erhöhen	Die vorausschauende Instandhaltung (Predictive Maintenance) erfasst mittels intelligenter Sensorik den Zustand von Maschinenelementen in Echtzeit. Anhand dieser Daten können Maschinenstörungen vorausberechnet werden. Dies ermöglicht den gezielten Einsatz von Servicetechnikern, um Produktionsstillstände zu minimieren. Somit kann die Maschinenverfügbarkeit erhöht werden.

Anwendungsgebiete in der Industrie 4.0	
Unternehmensziele	Möglicher Ansatz, mittels cyber-physischen Systemen realisierbar
Produktionsprozess maschinenübergreifend koordinieren	Über eine Plattform, z. B. MES (Manufacturing Execution System), werden alle Rückmeldungen zum momentanen Stand der Fertigung erfasst, notwendige Planänderungen ermittelt und an die Maschinen zurück übermittelt.
Energieverbrauch von Maschinen und Anlagen reduzieren	Maschinen und Anlagen erfassen und überwachen ihren Energieverbrauch eigenständig. Sie koordinieren ihn unter Berücksichtigung von definierten Rahmenbedingungen mit den anderen Maschinen und reduzieren somit Lastspitzen, was zu einem ausgeglichenen Gesamtverbrauch führt.
Werkzeugmanagement optimieren	CPS erfassen automatisch Betriebsdaten von Werkzeugen und ermöglichen somit eine genaue Lebenszyklusüberwachung der Werkzeuge. Auf dieser Basis können Instandhaltungsmaßnahmen effizienter gesteuert werden.
Informationsaustausch zwischen Maschine und Mensch vereinfachen	Maschinenführer und Werker erhalten über geeignete Schnittstellen Echtzeitinformationen der Maschine sowie papierlose Anweisungen, welche viel schneller erlernt werden können und somit den Einsatz des Personals flexibilisieren.
Flexibilität und Effizienz von Montageprozessen erhöhen	Bauteile und Maschinenelemente werden an den Montagearbeitsplätzen ergonomisch ideal platziert, der Montagereihenfolge entsprechend eindeutig identifiziert und beim Einbau automatisch überwacht. Die gesamte Montage wird informationstechnisch mit visualisierten Anweisungen unterstützt, das Arbeitsergebnis protokolliert und dokumentiert.
Feinplanung an den Fertigungslinien optimieren	Entscheider wie Schichtführer oder Produktionsleiterin können über Dashboards (Informationssystem zur Visualisierung von Produktions- und Prozessdaten) auf ihren mobilen Endgeräten Feinplanungen simulieren und bei Bedarf entsprechend anpassen. Werden Anpassungen in der Produktion vorgenommen, informiert das System automatisch alle anderen Mitarbeiter über geeignete Endgeräte.
Identifikation von Produktionsaufträgen und Produktdaten im gesamten Fertigungsprozess ermöglichen	Alle Bauteile können beim Transport und an den Maschinen automatisch identifiziert und Produktionsaufträgen zugeordnet werden. Der momentane Bearbeitungsstatus kann permanent mit dem MES-System (und auch ERP) abgeglichen werden. Die gesamte Überwachung aller Produktionsaufträge ist sehr detailliert möglich.
Durchgängige Qualitätskontrolle in der gesamten Fertigung gewährleisten	CPS-Sensoren in und an den Maschinen, Anlagen und auch an anderen Arbeitsplätzen erfassen automatisch alle relevanten Qualitätsmerkmale. Abweichungen werden sofort erkannt und können unmittelbar behoben werden. Die Produktqualität kann durch den Einsatz von Inline-Qualitätsüberwachung (direkt in der Fertigungslinie) mittels Kameras (Vision Control) verbessert werden. Hundert Prozent der produzierten Teile können somit im Takt der Produktion geprüft werden.
Wertschöpfende Zusatzleistungen für den Kunden generieren	Produkte oder Maschinen, die bereits beim Kunden im Einsatz sind, erfassen mithilfe von cyber-physischen Systemen Nutzungs- und Umgebungsdaten. Dadurch lassen sich gezielt Produktverbesserungen und Weiterentwicklungen realisieren und neue, wertschöpfende Dienstleistungen anbieten.

Auf Basis dieser Möglichkeiten können Unternehmen viele Chancen durch den Einsatz von cyber-physischen Systemen realisieren, müssen sich aber auch über die entstehenden Risiken im Klaren sein.

Einsatz von cyber-physischen Systemen

Chancen

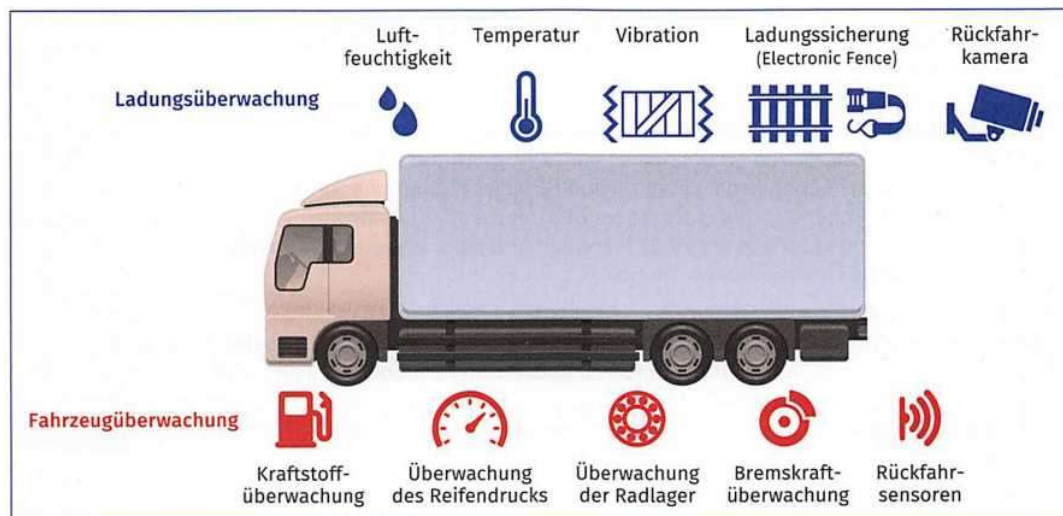
- Effizienzsteigerungen in der Produktion
- Erhöhung der Flexibilität in der Planung und im laufenden Fertigungsprozess
- Entlastung und informationstechnische Unterstützung des Personals
- Wettbewerbsvorteile

Risiken

- Erhöhte Komplexität der gesamten IT-Infrastruktur im Unternehmen
- Erheblicher Veränderungsprozess für ein Unternehmen, was die Akzeptanz der neuen Technologien stark beeinflusst
- Datensicherheit in Bezug auf Angriffe von außen
- Hohe Anforderungen an die IT-Kompetenzen im Unternehmen

LE 3 - Automotive-Bereich

Die Implementierung des Internet of Things im Automotive-Sektor brachte ebenfalls sehr große Entwicklungen mit sich. Das Konzept von untereinander kommunizierenden Fahrzeugen ist vielversprechend. Die Fahrzeuge werden über ein IoT-Netzwerk miteinander verbunden. Dies ermöglicht zum einen die Kommunikation zwischen den Fahrzeugen untereinander und die Interaktion der Fahrzeuge mit der Umgebung (z. B. die Verbindung zu den Fußgängern und die Vernetzung zu den städtischen Verkehrsleitsystemen).



Sensorik an einem Lkw

Einsatzgebiete im Automotive-Bereich

Vehicle-to-Vehicle (V2V)

Die Kommunikation zwischen Fahrzeugen ermöglicht den Austausch von Daten, wenn sich die Fahrzeuge annähern. Diese Daten sind primär Geschwindigkeit, die Dynamik der Fahrt (Bremsen/Beschleunigen) oder die exakte Position der Fahrzeuge. Dies soll zur Vermeidung von Unfällen führen und Feuerwehr, Ambulanz oder Polizei schneller durch den Verkehr leiten.

Vehicle-to-Infrastructure (V2I)

Vehicle-to-Infrastructure-Verbindungen beziehen sich hauptsächlich auf die Vernetzung von Fahrzeugen mit der Infrastruktur der Straßen. Dies sind beispielsweise Ampeln, Spurmarkierungen, Verkehrsleitsysteme oder Maut-Stationen. Primäres Ziel ist die Optimierung des Verkehrsflusses.

Vehicle-to-Pedestrians (V2P)

Mittels mobiler Applikationen und dem Smartphone kann sich auch der Fußgänger mit Fahrzeugen und Verkehrsinfrastruktur verbinden. Dadurch lassen sich nahegelegene Taxis lokalisieren oder es lässt sich die zu erwartende Ankunftszeit von öffentlichen Verkehrsmitteln vorhersagen.

Vehicle-to-Network (V2N)

Verkehrsleitsysteme und Wettervorhersagen können den Fahrer übersieh verändernde Wetter und Straßenbedingungen oder bestehende Verkehrsunfälle auf der geplanten Route informieren und Alternativen vorschlagen.

Flottenmanagement

Lkws besitzen heutzutage integrierte Sensoren zur Überwachung des Gewichts oder zur Lokalisierung der Position eines Lkw. Diese und weitere Daten von Sensoren einer großen Lkw-Flotte werden in Cloud-Applikationen gespeichert, analysiert und visualisiert. Dies sind beispielsweise Echtzeit-Location-Monitoring der Lkw-Flotte, die Überwachung von Volumen und Gewicht der Ladungen, Leistungsdaten zu Kraftstoffverbrauch oder Verkehrsinformationen, um Fahrerinnen und Fahreraktiv beim Routenmanagement zu unterstützen.

Autonomes Fahren

Autonomes Fahren wird bereits in Pilotprojekten umgesetzt, z.B. sind in Städten autonom fahrende Taxis mit sicherer Fußgängererkennung unterwegs. Mögliche Chancen für unsere Gesellschaft sind der Einsatz von automatisiertem ÖPNV, der unter anderem auch den ländlichen Raum besser erschließen kann. Verkehr kann flüssiger fließen und Gütertransporte können somit umweltschonender transportiert werden. Ältere oder leistungseingeschränkte Menschen können an der individuellen Mobilität teilhaben und jeder einzelne kann die Zeit in fahrerlosen Taxen und Bussen produktiver nutzen.

Automotive Maintenance System

Vorausschauende Wartung und Instandhaltung wird auch im Automotive-Bereich von immer größerer Bedeutung. Eingebettete Sensoren in den unterschiedlichen Fahrzeugkomponenten sammeln Daten und speichern diese auf den IoT-Plattformen der Hersteller. Auch in diesem Szenario wird mittels KI-unterstützter Datenanalyse frühzeitig sichtbar, welche Teile gewartet oder präventiv ausgetauscht werden müssen.

Infotainment and Telematik

Durch WLAN im Auto eröffnen sich neue Möglichkeiten im Bereich des Car-Infotainments und der Telematik. Die eigene Lieblingsmusik kann ohne Unterbrechung, von zu Hause, auf dem Weg zum Auto und beim Fahren angehört werden. Informationen und Dienstleistungen in der nahen Umgebung können angezeigt und direkt angesteuert werden, all dies auch mit Unterstützung intelligenter Sprachassistenten. Des Weiteren lassen sich in Kombination mit dem Smartphone Sicherheits- und Überwachungsfunktionen für das Fahrzeug realisieren. Beispielsweise kann bei einem Unfall automatisch der Notruf angewählt und die Position übermittelt werden oder der Besitzer wird bei einem Einbruchversuch direkt alarmiert.

LE 4 - Smart Health – Gesundheitswesen

Der Einsatz von Gesundheits-Apps findet auch heute schon große Anwendung. Fitness-Tracker sammeln Daten wie Puls, Anzahl der Schritte und sportliche Aktivitäten. Geprüfte und zertifizierte Funktionen wie die Messung der Sauerstoffsättigung oder die Überwachung des Herzrhythmus ergänzen den Funktionsumfang von Fitness-Armbändern oder Smart-watches. Diese Geräte sind cyber-physische Systeme, die zusammen mit ihren Apps die Aufzeichnung von Gesundheitsdaten übernehmen sowie die Körperfunktionen über



wachen und mögliche Krankheitssymptome identifizieren. Letztlich erinnern sie den Benutzer an die Einnahme von Medikamenten, steuern automatisiert die Verabreichung eines Medikaments oder unterstützen ihn mit einem persönlichen Gesundheits- und Fitnessprogramm. Diese Daten können auch mit dem Arzt, einem Krankenhaus, der Krankenkasse oder in anonymisierter Form mit Forschungseinrichtungen ausgetauscht werden, was allerdings unter den Gesichtspunkten des Datenschutzes und der Datensicherheit sehr kritisch betrachtet werden sollte.

LE 5 - Smart Cities - intelligente Städte



Der Begriff „Smart City“ beschreibt intelligente Ideen und Konzepte für Städte. Diese sollen durch modernste Technik effizienter, klimafreundlicher und damit lebenswerter gemacht werden. Um diese Ziele zu verwirklichen, sind nicht nur Produkte, sondern auch Dienstleistungen, Prozesse und Infrastrukturen erforderlich, die durch hochintegrierte und vernetzte Informations- und Kommunikationstechnologien unterstützt werden.

Ziele, Handlungsfelder und Gefahren der intelligenten Stadt

Ziele

Das zentrale Thema einer Smart City ist die Verbesserung der Effizienz, Effektivität und Flexibilität des gesamten Systems. Beim demografischen Wandel und um die wachsende Herausforderung des Klimaschutzes zu bewältigen, spielen Städte eine große Rolle. Mithilfe von Informations- und Kommunikationstechnologien und weiteren neuen Technologien können alle Seiten der Gesellschaft, egal ob Bürgerinnen und Bürger, Unternehmen oder Verwaltungen in Smart Cities, diesen Herausforderungen begegnen. Ziel ist es, das größtmögliche Potenzial für ökologische und soziale Verbesserungen auszuschöpfen.

Herangehensweise

In einer Smart City können Sensoren für die gesamte städtische Umgebung bereitgestellt werden. Das Ergebnis ist das Internet of Things und Dienste, mit denen alle aufgezeichneten Daten auf einem virtuellen Computerserver (Cloud Computing) verwendet werden können. Die eingesetzten Technologien der Bevölkerung und die ihrer Umgebung interagieren ständig.

Anwendungsbeispiel

Man kann bereits heute Smartphones verwenden, um bei der Navigation Kraftstoff und damit Emissionen einzusparen. Des Weiteren können Informationen verwendet werden, um Transportmethoden zu kombinieren, die es ermöglichen, schnell, umweltfreundlich und bequem von A nach B zu kommen.

Handlungsfelder

Intelligente Technologien können in vielen Handlungsfeldern von Smart Cities zu massiven Verbesserungen beitragen. Die Verbindung von Smart Cities zieht sich durch Verwaltung und Mobilität mit Energie- und Umweltmanagement. Eine verteilte Energieerzeugung, die Kontrolle von Lastspitzen, Beleuchtung und Smart Homes spielen hierbei eine wichtige Rolle.

Gefahren

Betrachtet man die Möglichkeiten der Gesichtserkennung, so stellt man fest, dass diese Technologie auch sehr schnell zur Gefahr für unsere Demokratie werden kann. Wäre die Technik fehlerfrei, würden ständig Bewegungsprofile erstellt und somit viele tausend Menschen anlasslos überwacht werden.

LE 6 - Consumer-Bereich

Endverbraucher interagieren schon seit vielen Jahren mit dem Internet of Things und Dienstleistungen. Sie sind in Kontakt bzw. nutzen aktiv cyber-physische Systeme, sei es das Smartphone, PC oder Laptop, das Tablet, die Smartwatch oder Gesundheitstracker, den Smart-TV, die Spielekonsole oder die Multimediaanlage mit Sprachsteuerung. Intelligente und vernetzte Geräte sind Bestandteil unseres Lebens geworden. Die folgende Übersicht beschreibt Technologien, die schon heute für weitere Innovationen im industriellen Umfeld und im Privatleben sorgen.

Einsatzgebiete in der Smart Factory

Virtual Reality (virtuelle Realität)

Baumärkte und Möbelgeschäfte bieten VR-Apps zur Planung und Raumgestaltung an, auch Spielkonsolenhersteller erweitern laufend ihr Portfolio an VR-Brillen. Diese interaktiven Erlebnisse sind nicht nur in den privaten Bereichen interessant, sondern auch im beruflichen Umfeld der Industrie, des Handwerks und im Gesundheitswesen. Die virtuelle Realität verknüpft Daten und Bits mit der realen Welt und macht sie greifbar. Heutzutage ist es möglich, 3D-Modelle von Landschaften, Fabrikhallen und Autoinnenräumen zu erstellen und die Ansicht jedes Punkts mithilfe virtueller Stereokameras zu berechnen. VR-Brillen können ein „immersives Erlebnis“ entwickeln, welches dem Benutzer ermöglicht, sich in der virtuellen Welt zu bewegen und dabei ganz natürlich umzusehen. Des Weiteren werden die natürlichen Hände des Benutzers durch Handcontroller in der virtuellen Realität sichtbar, mit denen man Dinge greifen, Knöpfe drücken und virtuelle Türen öffnen kann.



Augmented Reality (erweiterte Realität)

Neben „vollimmersiven“ VR-Brillen, die den Menschen vollständig von der Realität abschirmen, existiert ein breites Spektrum an Anwendungen, welche von „komplett real“ zu „fast komplett real“ reichen. Man spricht dabei von Augmented Reality (AR, erweiterte Realität). Je nach Einsatzgebiet bieten diese Technologien interessante Anwendungsmöglichkeiten.



Sprach-Erkennung und -Steuerung

Sprachgesteuerte Überwachungs- und Steuerungssysteme sollen der Hausautomation zu einem Durchbruch verhelfen. Beleuchtung, Heizung, Jalousien, Fernseher, Waschmaschine, Alarmanlage und vieles mehr können per Sprache bedient werden. Smart Home und Sprachsteuerung ergänzen sich perfekt. Wenn man zuerst eine App öffnen muss, um dann das Menü zu durchsuchen, damit die Temperatur oder das Licht eingestellt werden kann, ist das nicht intuitiv und bedienerfreundlich. Von Smart Home kann man erst sprechen, wenn alles vollautomatisch ist oder die Steuerung vollständig intuitiv funktioniert. Genau das ermöglicht die Sprachsteuerung. Wenn man eine höhere Temperatur im Raum, den Fernseher einschalten oder die Jalousien nach unten fahren möchte, soll das Smart Home dank der Sprachsteuerung die Aktionen einfach ausführen können.



Alle genannten Technologien finden immer mehr Anwendungsfelder in der Industrie. Ein Einsatzgebiet sind Maschinen und Anlagen, deren Anzeigen von Sensoren im Normalfall nur in der Leitstelle sichtbar sind. Durch die Nutzung von AR-Brillen können die Messwerte direkt neben dem realen Sensor angezeigt werden, wenn der Benutzer durch das Werk geht. Leitungen, Ventile, Bau- und Bedienelement werden virtuell beschriftet oder je nach Funktion eingefärbt, damit die Technikerin vor Ort gemeinsam mit dem Spezialisten in seinem Büro ein Problem beheben kann. Hat die Servicetechnikerin beide Hände im Einsatz, können mithilfe von Sprachsteuerung Aktionen gestartet werden, z. B. ein Antrieb ein- oder ausgeschaltet werden.



Gerade diese Verbindung von realer Umwelt und digitalen Daten hat sehr großes Potenzial, unsere Arbeitswelt zu verändern. Durch die meisten Mobilgeräte wie Tablets und Smartphones können wir bereits heute an jedem Ort Daten abrufen, ob direkt beim Kunden oder an einer Maschine. Dadurch ermöglicht AR nicht nur einen wesentlich einfacheren, sondern auch schneller verständlichen Blick auf Daten, Zusammenhänge und Abläufe. IT-Giganten setzen große Hoffnung auf die Sprachsteuerung des vollvernetzten Hauses mithilfe intelligenter Sprachassistenten. Wenn Amazon, Google, Apple und Co. diesen Weg weitergehen, wird bald keine Maus, keine Tastatur, kein Bildschirm und kein Smartphone mehr für den Alltag zu Hause benötigt.

Lernzielkontrolle TAG 2

1. Erstellen Sie in Partnerarbeit eine Mindmap zu den oben behandelten sechs Anwendungsfeldern (Smart Home, Smart Factory, Automotive, Smart Health, Smart City, Consumer). Erweitern Sie Ihre Mindmap mit zusätzlichen Anwendungsbeispielen, die Sie aus Ihrem betrieblichen und privaten Umfeld kennen.
2. Beschreiben Sie ein Anwendungsgebiet, das Sie selbst aktiv nutzen. Welche Vorteile bietet Ihnen das gewählte Anwendungsfeld? Gibt es Gefahren durch den Einsatz dieser Anwendung?

TAG 3 - Den strukturellen Aufbau von cyber-physischen Systemen definieren

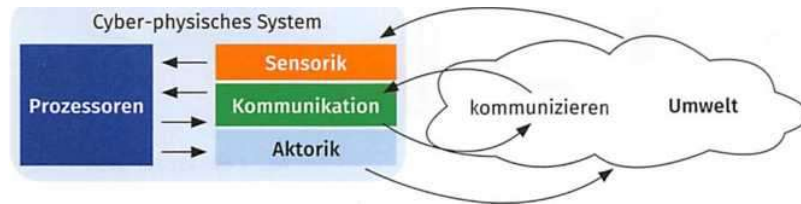
Kontinuierliches Echtzeit-Monitoring zusammen mit zustandserfassenden cyber-physischen Systemen ermöglicht die Überwachung von Prozessen und Systemen. Entscheidungsfindung, Rückverfolgbarkeit, Qualitätssicherheit und Prozesskontrolle können durch den Einsatz von intelligenten Sensoren, z. B. Temperatur, Feuchtigkeit, Infrarot, Ultraschall, Bewegung oder Druck, verbessert werden.

Cyber-physische Systeme (CPS)

Ein cyber-physisches System besteht aus mechanischen, elektrischen und informationstechnischen Komponenten. Das CPS kann über eine Kommunikationsinfrastruktur Daten austauschen, es kann kontrolliert und gesteuert werden. Eine Steuerung des CPS ist über das Internet in Echtzeit möglich. Für die rasanten Entwicklungen in der Industrie 4.0 spielt der Einsatz von cyber-physischen Systemen eine wesentliche Rolle.

In der folgenden Übersicht sind die wesentlichen Funktionen von cyber-physischen Systemen aufgelistet.

Funktionen von cyber-physischen Systemen	
Integration	Ein cyber-physisches System vereint die physische Welt mit der virtuellen Welt in einem Objekt. Eine eindeutige Identifikation des Objektes im Netzwerk zeichnet ebenfalls das integrierte cyber-physische System aus.
Sensorik	Mittels Sensorik (z. B. Sensoren zur Erfassung von Temperatur und Luftfeuchtigkeit) kann ein cyber-physisches System Werte aus seiner Umwelt aufnehmen und verarbeiten.
Verarbeitung	Mikrocontroller (Ein-Chip-Computersysteme) sind ein wesentlicher Bestandteil von cyber-physischen Systemen. Sie sind die technische Voraussetzung, um die erfassten Informationen und Daten zu verarbeiten.
Aktorik	Cyber-physische Systeme können Aktoren (antriebstechnische Baueinheiten wie Motoren, Ventile oder Zylinder) besitzen. Sie interagieren direkt mit der Umwelt. Speziell im Bereich der Robotik ist dies von sehr großer Bedeutung.
Steuerung und Regelung	Cyber-physische Systeme verfügen über eine Intelligenz und können dezentral Entscheidungen zur Steuerung (z. B. das Öffnen und Schließen von Ventilen) oder zur Regelung (z. B. das Heizen oder Kühlen eines Raumes) treffen und physische Prozesse beeinflussen.
Vernetzung	Cyber-physische Systeme können untereinander (z. B. zwischen einer Werkzeugmaschine und dem eingesetzten Werkzeug), innerhalb eines Unternehmens (z. B. zwischen dem Werkzeug und dem SCADA-System), entlang der Wertschöpfungskette (z. B. zwischen dem Werkzeug, das seinen Verschleiß selbstständig überwacht und beim Werkzeuglieferanten eine Bestellung auslöst) und mit den Menschen (z. B. der Maschinenführerin, die den Werkzeugwechsel vorbereitet) kommunizieren.
Adaption	Cyber-physische Systeme können ihre eigene Funktionalität anpassen (z. B. das Intervall der Messwerterfassungen verändern, wenn ein neues Produkt produziert wird), aus Daten lernen und die eigenen Funktionen erweitern (z. B. wenn auf Basis von Datenanalysen neue Fehlermuster identifiziert wurden und somit früher in den Prozess eingegriffen werden kann - Machine Learning, maschinelles Lernen).

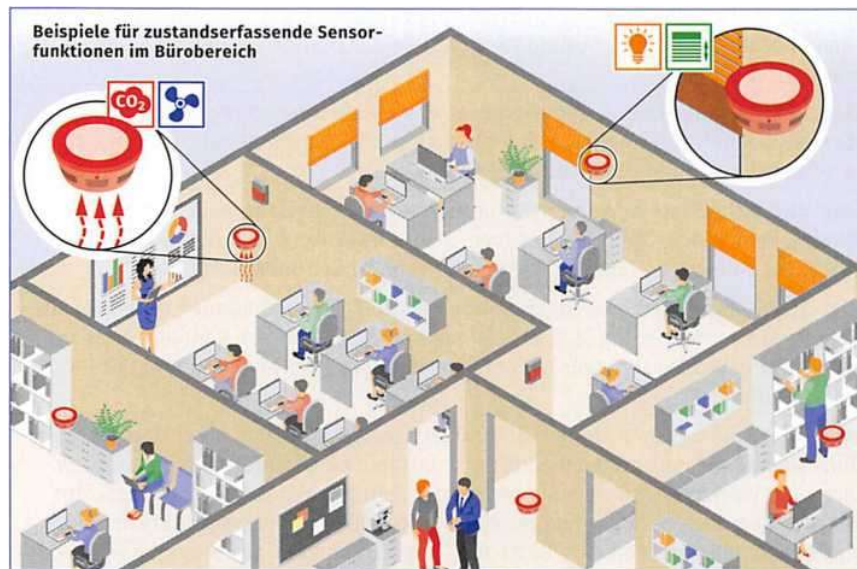


Hauptbestandteile eines cyber-physischen Systems und die Interaktion mit seiner Umwelt

LE 1 – Sensorik

In Gebäuden sowie in der Produktion spielt das Erfassen von Umgebungszuständen eine wesentliche Rolle. Hierdurch ist es möglich, Materialflüsse besser zu steuern, Maschinenparameter in Echtzeit einzustellen und sogar Wartungsprogramme bedarfsgerecht zu verbessern. Daraus folgen optimierte Wartungskosten, minimierte Stillstandszeiten und eine höhere Effizienz.

Eine Herausforderung besteht darin, reale Zustände wie „Luftfeuchtigkeit zu hoch“ oder „Druck zu niedrig“ im gesamten Netzwerk zu erfassen. Hier kommt moderne, verknüpfbare Sensortechnik ins Spiel. Zustände wie Lichtstärke, Luftfeuchtigkeit, Temperatur, Luftdruck oder Bewegungen im Raum können von Sensoren erfasst und dem Netzwerk als Information verfügbar gemacht werden. Mit diesen Daten können Programme intelligente Steuerungen umsetzen, welche beispielsweise eine bedarfsgerechte Betätigung der Klimatisierung oder der Lichtanlage erlauben. Die Sensorik ist damit ein fundamentales Element vieler cyber-physischer Systeme, die in modernen Maschinen und Anlagen von den Herstellern integriert werden. Aber selbst ein bestehender Maschinenpark kann durch die Ergänzung mit moderner Sensorik auf den neuesten Stand der Technik gebracht werden.



Sensorfunktionen im Büro



Wichtige Sensoren und ihre Einsatzbereiche

Übersicht und Einsatzgebiete von modernen Sensoren

Temperatursensoren

Um die Qualität von empfindlichen Waren, z. B. Lebensmittel oder pharmazeutische Produkte, zu gewährleisten, erfordern viele Prozesse wie Lagerung und Transport bestimmte Umgebungs- und/oder Gerätetemperaturen. Daher erhalten Temperatursensoren Einlass in die Raumautomation, um alle Aktoren, z.B. Heiz-/Kühlventile oder Lüftungsklappen, anhand der benötigten Umgebungsbedingungen präzise zu steuern.

Feuchtigkeitssensoren

Kondenswasser kann in Wohn- und Arbeitsräumen gesundheitsgefährdenden Schimmelpilzbefall herbeiführen. Um schon im Vorhinein Maßnahmen dagegen zu ergreifen, können Feuchtigkeitssensoren wichtige Kenntnisse ermitteln. Die wichtigsten Einsatzgebiete sind vor allem Industrie- und Büroumgebungen für die Heizungs-, Lüftungs- und Klimakontrolle.

Infrarot-Thermosensoren

Für Anwendungen, die Oberflächentemperaturen und Objektbewegungen erfassen, sind Infrarot-Thermosensoren eine geeignete Wahl. Hierbei werden Wärmestraahlen von Objekten erfasst und in ein elektrisches Signal umgewandelt. Sie eignen sich als Präsenzmelder in Sicherheitssystemen, für die Patientenerkennung im medizinischen Umfeld oder für die Temperaturmessung in der industriellen Prozesskontrolle.

Ultraschallsensoren

Bei Ultraschallsensoren werden Ultraschallwellen ausgesendet, vom Objekt reflektiert und wieder vom Sensor erfasst. Aufgaben davon können beispielsweise die Füllstanderkennung von flüssigen oder festen Materialien in geschlossenen Behältern oder die Messung der Entfernung von Personen und Objekten sein (vergleichbar Sonar und Radar). Da Ultraschallwellen Objekte unabhängig von Material, Farbe oder Oberfläche erkennen, sind sie eine zuverlässige Lösung für raue und anspruchsvolle Einsatzbedingungen.

Präsenzmelder

Ein Präsenzmelder dient dazu, physische An- oder Abwesenheit zu erkennen. Er überwacht den Erfassungsbereich auf Basis von Infrarot: Wird eine Person erkannt, dann wird eine entsprechende Aktion ausgelöst, z. B. Einschalten der Beleuchtung.

Lichtsensoren

Lichtsensoren messen die Intensität von Tageslicht oder künstlichem Licht. Sie sind sowohl im industriellen als auch kommerziellen Umfeld einsetzbar. Beispielsweise wird durch das Erkennen der Beleuchtungsstärke in einem Raum der Komfort verbessert, indem man das Anheben und Absenken von Jalousien sowie das Ein- und Ausschalten von Beleuchtungen mit den Sensoren verknüpft.

CO₂-Sensoren

Um Veränderungen der Luftqualität zu überwachen und die Konzentration von Kohlenstoffdioxid zu messen, werden CO₂-Sensoren eingesetzt. Gerade in Bürogebäuden, Schulen, Krankenhäusern oder Smart Homes werden sie häufig genutzt, um die Raumluftqualität zu überwachen. Des Weiteren sind CO₂-Sensoren sehr gut für Echtzeitüberwachung von Qualität, Frische und Sicherheit von Agrar- und Lebensmittelprodukten geeignet, da Kohlendioxid zum Schutz vor dem Wachstum von Bakterien und Pilzen eingesetzt werden kann.

Luftdrucksensoren

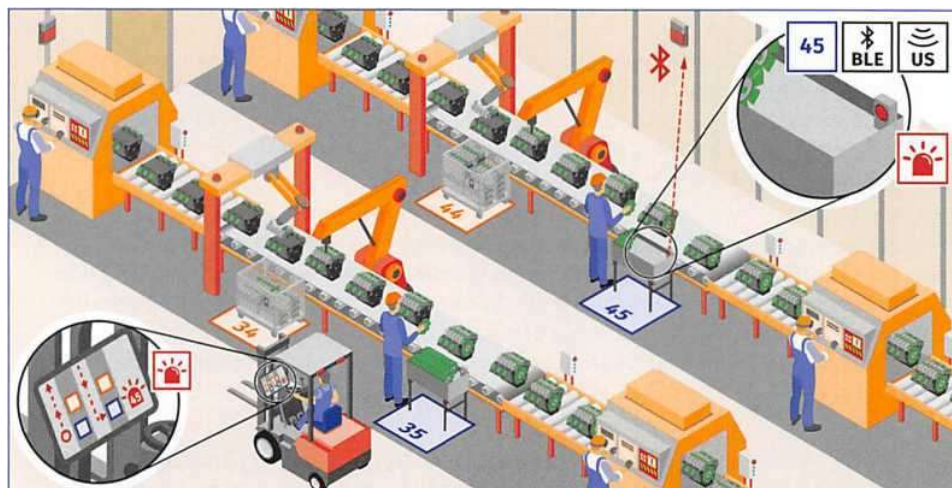
Barometrische Drucksensoren erfassen Druckschwankungen der Atmosphäre und werden bei der Prozess- und Qualitätskontrolle im industriellen Umfeld eingesetzt. Überall, wo eine ständige Überwachung und Regelung des Luftdrucks für die Betriebsabläufe entscheidend ist, z.B. in Reinräumen, Krankenhäusern und Computerräumen, erfassen Luftdrucksensoren die erforderlichen Daten.

Vibrationssensor, Schwingungssensor und Beschleunigungsmesser

Zur Überwachung der Laufruhe von Maschinen und Anlagen werden Vibrationssensoren oder auch Schwingungssensoren eingesetzt. Maschinen können in der Leistung gedrosselt werden, falls Schwingungen in der Anlage zu stark werden. In der Kombination mit einer Regelungseinheit kann die Steuerung von Motoren vollautomatisch erfolgen, sei es, um Drehzahlen zu erhöhen, um Taktzeiten zu verkürzen oder zu reduzieren, um Ausfälle durch zu starke Schwingungen zu verhindern und die damit verbundenen Reparaturkosten zu verringern.

Kraftsensor

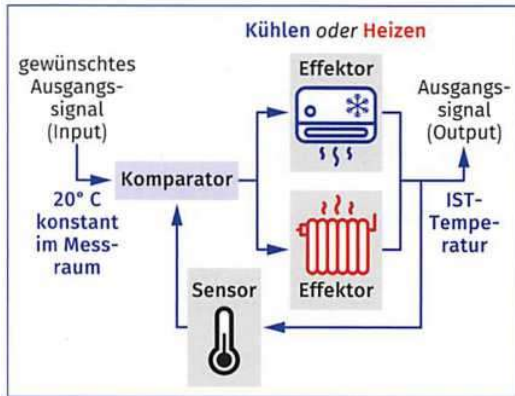
Kraftsensoren werden zur Messung von einwirkenden Kräften auf Maschinen- und Anlagenkomponenten eingesetzt. Mit diesen Sensoren können durch elastische Verformung sowohl Zug- als auch Druckkräfte gemessen werden.



Sensoreinsatz im Behältermanagement in der Fertigung

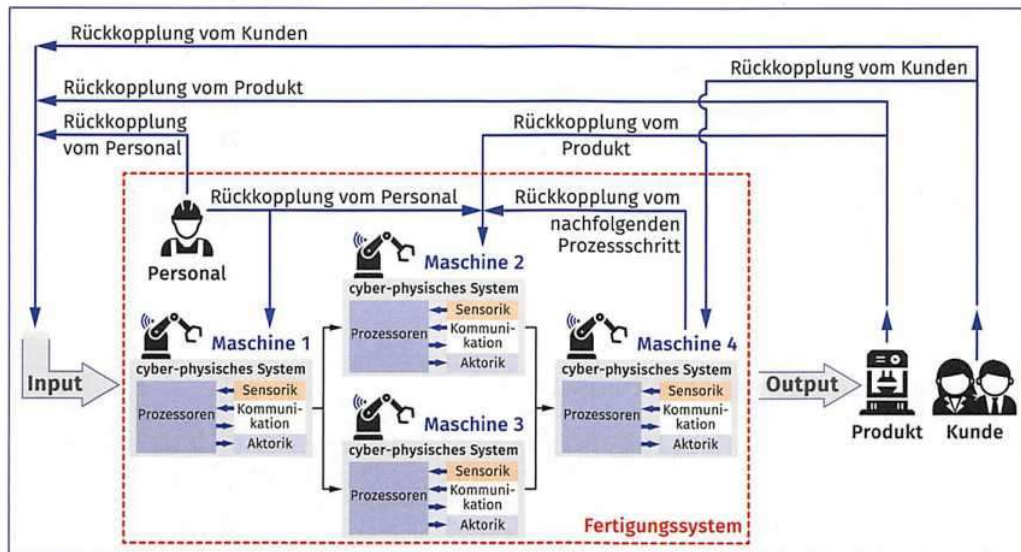
LE 2 - Regelung mittels intelligenter Sensorik

Durch Rückkopplung des kontinuierlichen Echtzeit-Monitorings ist es nun möglich, laufende Prozesse oder Anlagenzustände anzupassen. Das zurückgekoppelte Signal kann auf unterschiedlichste Weise eingreifen. Das Beispiel in folgendem Schaubild stellt eine Temperaturregelung in einem Messraum dar.



Beispiel für einen einfachen Regelkreis

Das grundlegende Prinzip der Regelungstechnik kann durch den Einsatz von cyber-physischen Systemen ganze Produktionsprozesse regeln. Im folgenden Schaubild wird verdeutlicht, dass neben dem Bedien- oder Instandhaltungspersonal auch vernetzte Maschinen und Anlagen, vor- oder nachgelagerte Prozessschritte, das Produkt selbst, aber auch der Kunde die Prozesse in Echtzeit beeinflussen können.



Rückkopplung durch cyber-physische Systeme

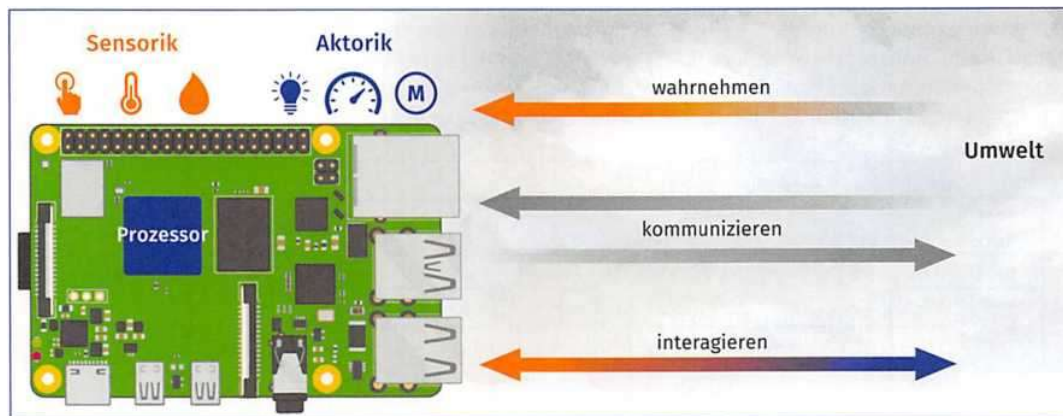
LE 3 - Einplatinencomputer als Basis für cyber-physische Systeme

Viele Funktionen eines Standardcomputers mit den zugehörigen Schnittstellen zu Peripheriegeräten sind bei einem Einplatinencomputer (Single-Board-Computer, SBC) auf einer kleinen Platine integriert. Aufgrund des sehr kleinen Designs arbeiten Einplatinencomputer nicht so schnell wie die größeren Modelle, sind aber für viele Anwendungen absolut ausreichend. Die erforderlichen Erweiterungen wie Festplatten oder Laufwerke können problemlos über eine USB-Verbindung auf einem Einplatinencomputer ermöglicht werden.

Abgesehen von der kompakten Bauform ist die sehr geringe Stromaufnahme ein ausschlaggebender Vorteil. Um einen Mikrocomputer mit Energie zu versorgen, reicht ein einfaches Netzteil eines Smartphones. Die geringe Leistungsaufnahme begrenzt die Erweiterung mit USB-Geräten ohne eigene Stromversorgung. Entwickelt wurden Einplatinencomputer hauptsächlich als Entwicklerboards, für die Ausbildung und den Hochschulbereich, aber auch für den Einsatz in Produktionsmaschinen und für andere begrenzte Einsatzgebiete. Dort ermöglichen sie das Regeln und Steuern, ohne dass ein externer Computer benötigt wird. Inzwischen sind sie in fast jedem technischen Gerät mit einem größeren Funktionsumfang zu finden - etwa in Smartphones, Smart-TVs, Routern, Waschmaschinen oder Kraftfahrzeugen.



In der Aus- und Weiterbildung ist der „Raspberry Pi“ weit verbreitet, was unter anderem an den online verfügbaren Bau- und Programmieranleitungen liegt. Neue Modelle mit anderen Ausstattungsvarianten, weiteren Anschlüssen, immer mehr Leistung und vor allem die ständig wachsende weltweite Community schaffen die Basis für neue Anwendungsgebiete und nachbaubare Projekte.



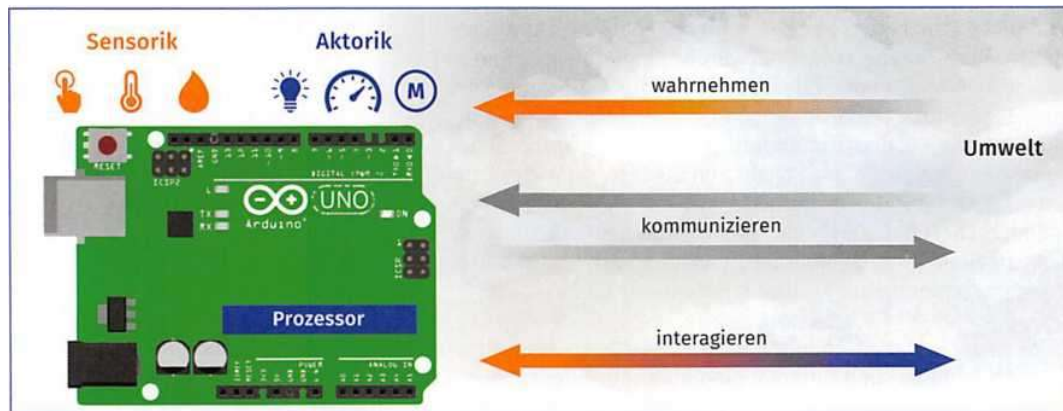
Einplatinencomputer - Single-Board-Computer (SBC)

Wie es der Name schon sagt, handelt es sich bei einem Einplatinencomputer um einen voll funktionsfähigen Computer, der alle wesentlichen Komponenten wie Prozessor und Arbeitsspeicher auf einer Platine vereint. Zusätzlich kann ein Einplatinencomputer Aus- und Eingabe-Schnittstellen besitzen, um Monitor, Tastatur, Maus sowie weitere Sensoren und Aktoren anzuschließen.

LE 4 - Mikrocontrollerboards als Basis für cyber-physische Systeme

Fernbedienungen, Router und Roboter arbeiten mit Mikrocontrollern. Moderne Mikrocontroller sind einfach zu bedienen und zu programmieren. Man benötigt lediglich einen Laptop, ein USB-Kabel und Open-Source-Software. Ein bekanntes Mikrocontrollerboard ist beispielsweise der „Arduino“. Dieses Mikrocontrollerboard ist eine komplette Entwicklungsumgebung, die sowohl aus Software als auch aus Hardware besteht. Beide Komponenten sind frei zugänglich (Open Source). Die Hardware umfasst einen Mikrocontroller sowie analoge und digitale Ein- und Ausgänge.

Prinzipiell wird in einem Mikrocontroller ein Programm in einer Schleife ausgeführt, das so konzipiert ist, dass eine einzelne, spezifische Aufgabe ausgeführt wird. Präzisiert ist ein Mikrocontroller ein Chip, auf den eine grundlegende Firmware oder Software geladen wird, um den Mikrocontroller auf den Empfang von Signalen vorzubereiten und Aktoren anzusteuern.



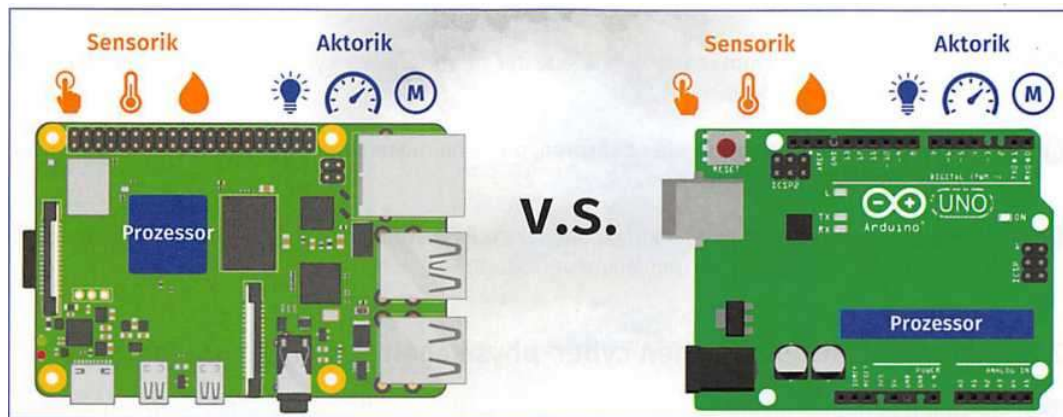
Mikrocontroller als cyber-physische Systeme

Mikrocontroller

Ein Mikrocontroller ist ein Chip, in dem neben dem Prozessor oftmals auch der Arbeitsspeicher integriert ist. Im Chip arbeitet ein einzelnes Programm, das zyklisch ausgeführt wird. Eine solche Mikrocontroller-Einheit eignet sich sehr gut zur Automatisierung von sich wiederholenden Aufgaben. Oftmals findet man auch die Bezeichnungen „Microcontroller Unit“ (MCU) oder „ μ Controller“ (μ C).

LE 5 - Unterscheidung von Einplatinencomputer und Mikrocontroller

Der „Raspberry Pi“ ist im Gegensatz zu einem Mikrocontroller ein ausgereifter Computer mitsamt einem Betriebssystem. Computer verfügen sowohl über Mikroprozessoren als auch über Mikrocontroller, die zusammenarbeiten, um simultan mehrere Aufgaben ausführen zu können. Der Mikroprozessor führt die Anweisungen und Berechnungen aus, mit denen der Computer funktioniert. Mikroprozessoren sind weitaus schneller als Mikrocontroller, erfordern jedoch externe Ressourcen wie RAM oder Eingabe-/Ausgabeports, während Mikrocontroller normalerweise unabhängig sind.



Einplatinencomputer „Raspberry Pi“ (links) vs. Mikrocontroller „Arduino“ (rechts)

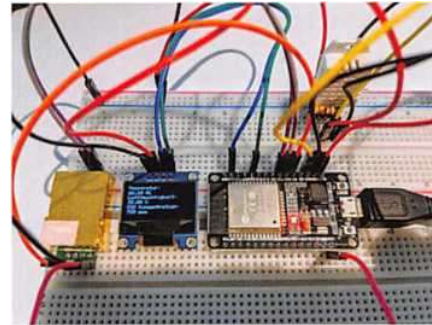
LE 6 - Mikrocontroller und das Internet of Things

Im Bereich der Mikrocontroller ist die Vernetzung von verschiedenen Geräten von großer Bedeutung. In diesem Zusammenhang beschreibt das Internet of Things die Technologie und die Infrastruktur, die diese Vernetzung ermöglicht. Viele Mikrocontroller werden mit entsprechenden Komponenten ausgestattet, damit sie als intelligente Objekte mit anderen Geräten im Netzwerk kommunizieren können.

Beliebte Mikrocontrollerboards mit integrierter Kommunikationseinheit sind der „ESP8266“ oder der „ESP32“. Beide sind kostengünstige Boards mit eingebautem WLAN-Chip und TCP/IP Protocol Stack. Dieser Chip ist kompatibel mit der WLAN-Norm IEEE 802.11 b/g/n, besitzt einen

internen Programm- und Datenspeicher und universell nutzbare Input-Output-Ports. Der „ESP8266“ ist ein Low-Power-Chip und kostet nur wenige Euro. Zusätzlich zum „ESP8266“ hat der Hersteller Espressif Systems den neueren Mikrocontroller „ESP32“ entwickelt. Dabei handelt es sich um eine Aktualisierung und Erweiterung des „ESP8266“, der nicht nur in allen bisherigen „ESP8266“-Projekten verwendet werden kann, sondern auch zusätzliche Eigenschaften wie Bluetooth-Kommunikation, einen größeren SRAM-Datenspeicher und mehr I/O-Schnittstellen bietet.

In der folgenden Abbildung ist ein Versuchsaufbau für ein einfaches cyber-physisches System auf Basis eines „ESP32“-Mikrocontrollers dargestellt. Das Mikrocontrollerboard ist mit unterschiedlichen Sensoren auf einem Breadboard (Steckbrett für Versuchsaufbauten) verbunden. Die Kommunikationseinheit sendet die erfassten Werte an einen zentralen Server, der wiederum die Werte grafisch aufbereitet und diese als Dashboard beispielsweise mobilen Endgeräten zur Verfügung stellen kann.



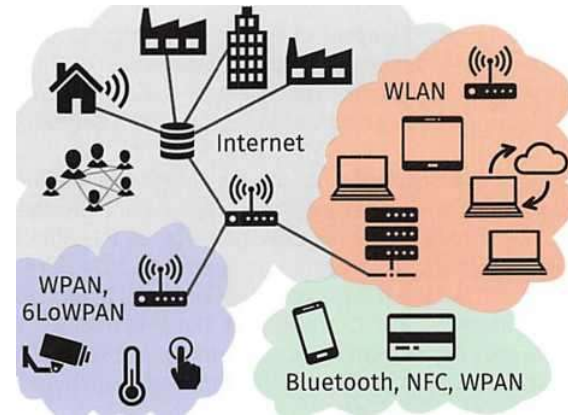
„ESP32“-Versuchsaufbau

Lernzielkontrolle TAG 3

1. Welche der beiden Aussagen ist richtig?
 - a. Ein Mikrocontrollerboard ist ein vollständiger Computer.
 - b. Die englische Abkürzung für einen Einplatinencomputer lautet SBC.
2. Beschreiben Sie mit eigenen Worten die Hauptelemente eines cyber-physischen Systems.
3. Erläutern Sie einen geschlossenen Regelkreis, der mithilfe eines cyber-physischen Systems Ihrer Wahl realisiert werden kann.
4. Informieren Sie sich im Internet über Sensoren, die in heutigen Smartphones integriert sind. Diskutieren Sie Ihre Rechercheergebnisse.

TAG 4 - Kommunikation zwischen cyber-physischen Systemen präsentieren

Ein wichtiges Kriterium für den Erfolg oder Misserfolg einer IoT-Anwendung ist die Auswahl des richtigen Protokolls für die Kommunikation im Netz. Bei der Kommunikation zwischen Geräten in IoT-Netzwerken werden verschiedene IoT Kommunikationsprotokolle verwendet. Es wurden unterschiedliche Protokolle entwickelt, um den verschiedenen Anforderungen von IoT-Produkten und -Dienstleistungen gerecht zu werden. Wenn ein Sensor, z.B. ein Temperatursensor, nur wenig Datenmengen übertragen muss, sollte er auch nur wenig Energie verbrauchen. Andere Sensoren müssen sich an einem festen Ort befinden, da sie mit 230 V Netzspannung versorgt werden müssen. Das Schaubild verdeutlicht, dass innerhalb eines Netzwerks viele unterschiedliche Protokolle zum Einsatz kommen können.



Bei der **Entwicklung von IoT-Produkten und -Dienstleistungen** sind folgende Faktoren zu berücksichtigen:

- die Datenmenge und Datenübertragungsrate, die für den geforderten Anwendungsfall zu übertragen ist,
- die Energieeffizienz bzw. der Energiebedarf des cyber-physischen Systems,
- die Relevanz einer Verzögerung der Datenübertragung.

LE 1 - IoT-Protokolle und Industrial-Internet-Protokolle unterscheiden

Um die zahlreichen unterschiedlichen Protokolle einzuordnen, ist zuerst die Zuordnung zu den entsprechenden OSI-Schichten notwendig. Danach können die unterschiedlichen IoT-Protokolle der Bit-Übertragungsschicht näher betrachtet werden. Speziell für die Anwendungsschicht wird im nächsten Kapitel auf das MQTT-Protokoll eingegangen.

OSI-Schicht	IoT-Protokolle
Anwendungsschicht Die Anwendungsschicht dient als Schnittstelle zwischen Benutzer und IoT-Device.	• MQTT (Message Queue Telemetry Transport): MQTT ist ein Kurznachrichtenprotokoll, das vorrangig für Verbindungen mit geringer Bandbreite mit entlegenen Standorten verwendet wird. MQTT verwendet das Publisher-Subscriber-Prinzip und ist somit ideal für kleine Geräte, die eine effiziente Bandbreiten- und Akkunutzung voraussetzen.
Transportschicht Die Transportschicht schützt und unterstützt die Datenkommunikation.	• TCP (Transmission Control-Protokoll) • UDP (User Datagram-Protokoll)
Vermittlungsschicht Die Vermittlungsschicht ist für die Kommunikation einzelner IoT-Devices mit dem Router verantwortlich.	• IPv4, IPv6 (Internet Protocol) • 6LoWPAN (IPv6 over Low power Wireless Personal Area Network): Dieses IoT-Protokoll eignet sich ideal für Geräte mit niedrigem Energieverbrauch.

OSI-Schicht	IoT-Protokolle
Sicherungsschicht Die Sicherungsschicht identifiziert Fehler auf der physischen Schicht und korrigiert diese.	• LPWAN (Low-Power Wide-Area Network): LPWAN ist für die Kommunikation über Entfernungen von 500 m bis hin zu über 10 km geeignet. Ein LoRaWAN ist beispielsweise ein LPWAN, das für einen geringen Energieverbrauch optimiert wurde.
Bit-Übertragungsschicht Die Bit-Übertragungsschicht beschreibt den eigentlichen Kommunikationskanal.	• Mobilfunk • Wi-Fi/802.11 • Bluetooth, Bluetooth Low Energy (BLE), iBeacon • ZigBee • Z-Wave • NFC (Near Field Communication) • RFID (Radiofrequenz-Identifikation)

Die folgenden Tabellen beschreiben die wesentlichen Technologien der drahtlosen Kommunikation und ihre Eigenschaften und Anwendungsbereiche.

Mobilfunk	
GSM/ GPRS/ EDGE (2G)/ UMTS oder HSPA (3G)/ LTE (4G)	Seit fast zwei Jahrzehnten verwenden wir Mobilfunknetze. Diese bestehen aus Kommunikationsprotokollen GSM/ GPRS/ EDGE (2G)/ UMTS oder HSPA (3G)/ LTE (4G). Solche Protokolle werden generell für die Fernkommunikation genutzt und im Vergleich zu anderen Technologien können große Datenmengen schnell gesendet werden.
5G 	5G ist die fünfte Generation von Mobilfunknetzprotokollen und wurde für die Hochgeschwindigkeitskommunikation zwischen Smartphones und anderen Geräten entwickelt. Dabei sind durchschnittliche Download-Geschwindigkeiten von ca. 1 Gbit/s ohne Probleme zu erreichen. 5G wird ein enormes Wachstum der IoT-Anwendungsbereiche bewirken. Die Technologie wurde 2019 eingeführt.
LTE-M	LTE-M wird auch als LTE-Cat-M1-Protokoll (Long Term Evolution) bezeichnet. Diese Technologie wird verwendet, um IoT-Geräte ohne Zugriff über Zwischen-Gateways direkt mit dem 4G-Netzwerk zu verbinden. Es bietet eine Datenrate von etwa 100 Kbit/s und der Chip ist billig. Da weniger Daten übertragen werden, kann das Gerät eine längere Akkulaufzeit haben.

Drahtlose Kommunikation mit geringer Reichweite	
Wi-Fi (Wireless Fidelity) 	Bei der Benutzung des Wi-Fi-Protokolls für IoT-Anwendungen müssen seine Vor- und Nachteile berücksichtigt werden. Zum einen sind die Kosten der Wi-Fi-Infrastruktur und auch der Wi-Fi-Ausrüstung niedrig und einfach bereitzustellen. Jedoch ist der Stromverbrauch hoch und die Reichweite recht moderat. Daher ist Wi-Fi nicht in allen Bereichen von IoT-Anwendungen die beste Wahl. Bei Anwendungen in der Heimautomation kommt Wi-Fi sehr häufig zum Einsatz. Wi-Fi verwendet den IEEE 802.11-Standard für 2,4-GHz-UHF- und 5-GHz-ISM-Frequenzen. Im Freien und bei unverstellter Sicht sind Reichweiten bis zu 100 m möglich. Die maximale Datenrate beträgt je nach Kanalfrequenz und Anzahl der verwendeten Antennen bis zu 600 Mbit/s.

Drahtlose Kommunikation mit geringer Reichweite	
Bluetooth 	Mit einer Reichweite zwischen 50 m und 150 m kann Bluetooth vielseitig angewendet werden, z.B. in Telefonen, Tablets oder Robotersystemen. Der Datenaustausch ist dabei begrenzt auf 1 Mbit/s.
BLE 	BLE (Bluetooth 4.0, Bluetooth Low Energy) hat als Hauptunterschied zu Bluetooth einen deutlich geringeren Stromverbrauch. Daher kann das Produkt billiger beworben und länger genutzt werden als Bluetooth. Durch die Einführung des BLE-Protokolls konnten mithilfe der Bluetooth-Technologie viele neue Anwendungen im IoT-Bereich entwickelt werden. Sie gehören zur Kategorie der kostengünstigen Konsumgüter und Smart-Building-Anwendungen.
ZigBee 	Die Eigenschaften von ZigBee sind vergleichbar mit denen der Bluetooth-Technologie. Es folgt jedoch dem IEEE 802.15.4-Standard und ist ein erweitertes Kommunikationsprotokoll. Der geringe Stromverbrauch, die Robustheit, hohe Sicherheit und hohe Skalierbarkeit sind analoge Vorteile. Die Reichweite beträgt etwa 10 m bis max. 100 m und die Datenübertragungsrate ist auf etwa 250 Kbit/s beschränkt. Durch die Nachteile in der Reichweite und Datenrate und die Einschränkung hinsichtlich des Stromverbrauchs ist es nur für kleine drahtlose Anwendungen geeignet. Obwohl es diese Einschränkungen aufweist, bietet es seine 128-Bit-AES-Verschlüsselung und leistet einen wichtigen Beitrag zur sicheren Kommunikation sowohl in der Hausautomation als auch in kleinen industriellen Anwendungen.
Z-Wave	Z-Wave ist ein Kommunikationsprotokoll, das speziell für Hausautomationsprodukte entwickelt wurde und zusätzlich als HF-Kommunikationstechnologie mit niedrigem Stromverbrauch bekannt ist. Datenpakete können mit einer maximalen Datenrate von 100 Kbit/s ausgetauscht werden. Das Protokoll arbeitet mit 900 MHz im ISM-Band. Die maximale Reichweite beträgt 30 m. Es unterstützt die Steuerung von bis zu 232 Geräten.

Für den Einsatz von einigen der oben genannten Wi-Fi-IoT-Protokollen gibt es zahlreiche Erweiterungsmodule für den Einplatinencomputer „Raspberry Pi“ und auch für Mikrocontroller auf „Arduino“-Basis.

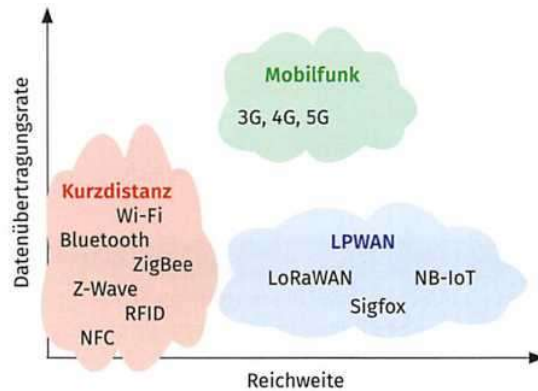
- Wi-Fi/Bluetooth-HC-05-Modul kann für Do-it-yourself-Projekte mit Entwicklungsboards wie „Arduino“ oder „Raspberry Pi“ verbunden werden.
- Für Echtzeitanwendungen werden andere Module benötigt, die Hochgeschwindigkeits- und Mesh-Netz- Werk-IoT-Protokolle unterstützen.
- Zigbee hat die DIY-Modul XBee und XBee Pro, die an ein „Arduino“- oder „Raspberry Pi“-Board angeschlossen werden können, um einfache Projekte oder Anwendungsprototypen zu erstellen.
- Z-Wave verfügt über das ZIY-Modul (Z-Wave Itself), ein „Arduino“- und „Raspberry Pi“-kompatibles Board, das für Hausautomationsanwendungen verwendet werden kann.
- Das 6LoWPAN-IoT-Protokoll verfügt über das 6LoWPAN L-Tek Arduino Shield. Es kann an die „Arduino“- Entwicklungsplatine angeschlossen werden, um eine BLoWPAN-Verbindung im 900-MHz-Frequenzband zu erhalten.

	Nahfeldkommunikation
RFID 	Radio Frequency Identification (RFID) ist eine Technologie, die mithilfe elektromagnetischer Felder Objekte oder Tags identifiziert, die bestimmte gespeicherte Informationen enthalten. Die Reichweite von RFID reicht von ungefähr 10 cm bis max. 200 m. Aufgrund des großen Bereichsunterschieds ist die Arbeitsfrequenz der RFID-Technologie sehr unterschiedlich.
NFC 	Near Field Communication (NFC) ist ein Protokoll für einfache und sichere Wechselseitige Interaktion zwischen elektronischen Geräten. Die generellen Anwendungen findet NFC vor allem bei Smartphones. Beispielsweise das Ermöglichen von kontaktlosen Zahlungsvorgängen, Zugreifen auf digitale Inhalte und das Anschließen verschiedener elektronischer Geräte. Es arbeitet mit einer Frequenz von 13,56 MHz im ISM-Band mit einem maximalen Entfernungsbereich von ungefähr 10 cm. Die Datenrate reicht von 100 bis 420 Kbit/s.

	Low Power Wide Area Networks (LPWAN)
LoRaWAN	Long Range Wide Area Network (LoRaWAN) verfügt über Fernanwendungen und zielt darauf ab, Kommunikation in IoT- und M2M-Anwendungen mit geringem Stromverbrauch zu erreichen. Es kann mit Datenraten zwischen 0,3 Kbit/s und 50 Kbit/s eine Verbindung zu Millionen von Geräten herstellen. Die Entfernung der LoRaWAN-Anwendung kann in einer städtischen Umgebung 2 km bis 5 km und in der vorstädtischen Umgebung 15 km erreichen.
NB-IoT	NB-IoT steht für Narrowband Internet of Things. Es handelt sich um eine Art LPWAN (Low Power Wide Area Network). Diese Technologie ist eine WAN-Technologie und kann in Anwendungen eingesetzt werden, die einen sehr geringen Stromverbrauch, Fernkommunikation und lange Zeiträume (lange Akkulaufzeit) erfordern. Das Signal kann durch die Wand übertragen werden oder in den unterirdischen Bereich gelangen, der mit normalen Mobiltelefonsignalen nicht erreicht werden kann. Die maximale Reichweite beträgt 10 km.

	Low Power Wide Area Networks (LPWAN)
Sigfox	Sigfox ist ein LPWAN, welches im Unterschied zu Mobilfunknetzen nicht für die Kommunikation zwischen einzelnen Personen, sondern für die Device-to-Cloud Kommunikation gedacht ist. Der Energieverbrauch von Sigfox verhält sich deutlich geringer, da sich die Geräte anders als ein Mobiltelefon dauerhaft mit dem Netz verbinden, sondern nur bei Bedarf ihre Nachrichten funken.
4G LTE IoT	Durch hohe Kapazität und geringe Latenzzeiten eignen sich diese Netzwerke hervorragend für IoT-Szenarien, die Informationen oder Updates in Echtzeit erfordern.
5G IoT	5G-IoT-Netzwerke versprechen weitere Innovationen im IoT-Bereich. Vor allem da deutlich schnellere Downloadgeschwindigkeiten und Verbindungen mit erheblich mehr Geräten in bestimmten Bereichen möglich sind.

Um die unterschiedlichen Protokolle in Bezug auf Reichweite und Datenrate besser einzuordnen, verdeutlicht die folgende Grafik diese Einordnung.



LE 2 - Die Anbindung von cyber-physischen Systemen mit dem MQTT-Protokoll beschreiben

MQTT (Message Queue Telemetry Transport) ist ein schlankes Messaging-Protokoll, welches auf das Internet of Things zugeschnitten ist. MQTT gewinnt gerade in Bereichen der Hausautomation und bei Open-Source-Projekten an Beliebtheit. Entwickelt wurde MQTT 1999 in den USA, um eine Öl-Pipeline in der Wüste zu überwachen. Im Jahr 2014 wurde MQTT ein offiziell anerkannter OASIS-Standard.

Die **OASIS** (Organization for the Advancement of Structured Information Standards) ist eine internationale, nicht-gewinnorientierte Organisation, die sich mit der Weiterentwicklung von E-Business- und Webservice-Standards beschäftigt.

2019 ratifizierte die OASIS die neue Spezifikation MQTT 5. Mit dieser neuen MQTT-Version wurden neue Funktionen in MQTT eingeführt, die für IoT-Anwendungen erforderlich sind. Neben Zuverlässigkeit sollte vor allem der sparsame Umgang mit Bandbreite sowie Ressourcen als Ziel der Entwicklung stehen. Das MQTT-Protokoll ist einfach und leichtgewichtig. Für eine Umsetzung des Protokolls ist nur geringfügig Code notwendig, wie beispielsweise die Client-Bibliothek für den „Arduino“-Mikrokontroller zeigt.

MQTT eignet sich für die Kommunikation mit mobilen Geräten, z.B. Smartphones oder IoT-Geräte, bei denen Bandbreite und Energie knapp sind. Dank des kompakten Binärprotokolls können Übertragungen so gut wie in Echtzeit erfolgen. Über den Inhalt einer Nachricht macht MQTT keine Annahmen. Text-, Binär- oder Objektnachrichten sind möglich.

MQTT-Protokoll

Das MQTT-Protokoll (Message Queue Telemetry Transport) ist ein sehr schlankes Übertragungsprotokoll für die Machine-to-Machine-Kommunikation, das Datenpakete trotz hoher Verzögerung in Form von Nachrichten zwischen Geräten ermöglicht. MQTT nutzt ein Publisher-Subscriber-Muster (Daten veröffentlichen und abonnieren) und ist daher für die einfache Kommunikation zwischen kleinen IoT-Geräten geeignet. MQTT besitzt keinen Sicherheitsmechanismus. Deshalb sollte es nicht unabhängig für die automatisierte Steuerung von Maschinen genutzt werden.

LE 3 - Client-Server-(Broker)-Prinzip

Das von MQTT unterstützte Message Exchange Pattern besitzt das im Folgenden beschriebene Publish/Subscribe-Muster. Bei Publish/Subscribe wird nicht direkt mit dem Empfänger kommuniziert. Der Sender übermittelt seine Nachricht zuerst an einen Broker. Dieser übernimmt dann die Zustellung der Nachricht an die Empfänger. Der Broker entkoppelt somit den Sender und die Empfänger. Der Sender kann auch dann eine Nachricht senden, wenn kein Empfänger online ist. Der Sender weiß jedoch nicht, ob es keinen, einen oder mehrere Empfänger gibt, die sich für seine Nachrichten interessieren. Für Empfänger und Sender ist der Broker gleichermaßen der Server. Empfänger und Sender sind Clients, die sich mit dem Broker verbinden. Oftmals sind Empfänger nur an bestimmten Nachrichten interessiert, die von einem Broker verteilt werden. Empfänger können Topics abonnieren (subscribe), die zuvor eingereicht werden müssen. In der folgenden

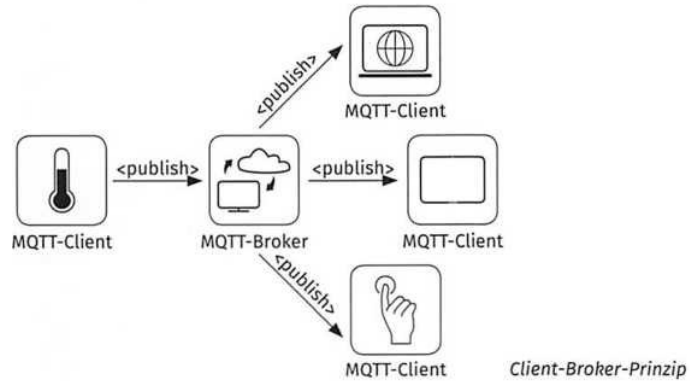
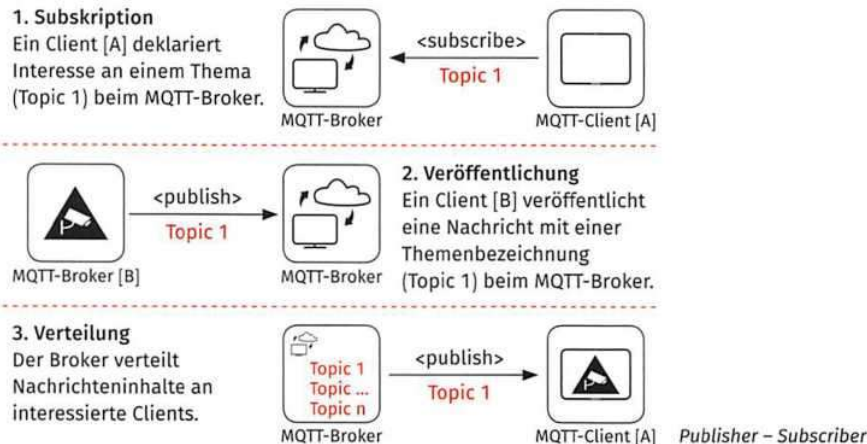


Abbildung haben drei Empfänger eine Subskription auf das Topic Temperatur. Wird jetzt eine Nachricht vom Temperatursensor gesendet (published), übermittelt der Broker jeweils eine Kopie der Nachricht an die drei Subscriber.

Anders als die Client/Server-Protokolle, z. B. Beispiel HKP, arbeitet Publish/Subscribe ereignisorientiert. Hier informiert der Broker den Client, sobald neue Daten eines abonnierten Topics vorliegen. Daher kann es sich der Client sparen, beim Server neue Daten anzufragen.



Begriffe des MQTT-Protokolls

MQK-Broker

Ein Broker erhält Nachrichten von Sendern und leitet diese an die Empfänger weiter. MQK-Broker können in zwei Gruppen aufgeteilt werden: nativen Broker, d. h. eigens für MQK entwickelte Broker, und Broker, die MQK über einen Konnektor unterstützen. Die nativen Broker sind im Vergleich zu Brokern, bei denen MQK nur ein Protokoll von vielen ist, deutlich kleiner. Einige davon, z. B. "Mosquitto", eignen sich deshalb ideal für den Betrieb auf einem Mikrocontroller oder dem „Raspberry Pi“.

MQTT-Client

Ein MQK-Client kann beides sein, ein Publisher und ein Subscriber, je nachdem, ob der Client gerade Nachrichten sendet oder empfängt. Ein MQK-Client kann ein beliebiges Gerät (von einem Mikrocontroller bis hin zu einem vollwertigen Server) sein, auf dem eine MQK-Bibliothek läuft und das sich über ein Netzwerk mit einem MQK-Broker verbindet.

MQK-Topic

Das Topic (Thema) wird vom Broker genutzt, um Nachrichten der Clients zu filtern. Es kann aus einer oder mehreren Themenebenen bestehen, die alle durch Schrägstriche (/) getrennt werden. Beim Erstellen der Topics muss auf die Groß- und Kleinschreibung geachtet werden. Zum Beispiel sind Serverraum/Temperatur und Serverraum/temperatur zwei unterschiedliche Topics. Das Dollarzeichen (\$) darf nicht am Anfang eines Topics verwendet werden, da es für interne Statistiken vom Broker verwendet wird.

Es gibt einige Grundregeln, um eine ordentliche Topic-Struktur zu erstellen:

- **Keinen Schrägstrich (/) am Beginn eines Topics verwenden:** Es verstößt zwar gegen keine Regel, jedoch erzeugt man dabei ein weiteres Topic-Level, das nur mit einem Zero-Zeichen gefüllt wird und nichts Weiteres einbringt.
Beispiel: /haus/obergeschoss/schlafzimmer
- **Leerzeichen in den Topics vermeiden:** Ein Leerzeichen ist schwer zu lesen und sollte vermieden werden, um Fehler zu vermeiden.
- **Kurze Topics verwenden:** In jeder Nachricht wird das Topic mitgesendet. Um nicht unnötig Ressourcen zu verschwenden, sollten Topics möglichst kurzgehalten werden.
- **Keine Sonderzeichen verwenden:** Weil Sonderzeichen nicht ASCII-UTF-8 konform sind und oft inkorrekt dargestellt werden, ist die Verwendung von Umlauten oder Sonderzeichen nicht zu empfehlen.

Topic Wildcard - einstufig

Wenn ein Client ein Topic abonniert, hat er zwei Optionen. Zum einen kann er genau das Topic einer veröffentlichten Nachricht abonnieren und zum anderen kann er Platzhalter verwenden und damit mehrere Topics gleichzeitig abonnieren. Allerdings kann ein Platzhalter nur zum Abonnieren von Topics verwendet werden, nicht zum Versenden von Nachrichten. Es gibt sowohl einstufige als auch mehrstufige Platzhalter.

Mit dem +-Zeichen kann man ein oder mehrere Topic-Level ersetzen.

Beispiel: Nehmen wir an, dass wir alle Temperaturen im Erdgeschoss ansehen wollen. Die Wildcard wird für die verschiedenen Räume im Erdgeschoss verwendet.

Topic: Buerogebaeude/Erdgeschoss/+ /Temperatur

Als Ergebnis werden folgende Topics abonniert:

- Buerogebaeude/Erdgeschoss/Serverraum/Temperatur
- Buerogebaeude/Erdgeschoss/Besprechungszimmer/Temperatur
- Buerogebaeude/Erdgeschoss/BueroChef/Temperatur

Topic Wildcard - mehrstufig

Mit dem #-Zeichen werden immer die nachfolgenden Topic-Level ersetzt, unabhängig davon, wie tief sie verschachtelt sind. Es steht damit immer an letzter Stelle. Wenn nur das #-Symbol verwendet wird, so werden alle Nachrichten, die über MQTT gesendet werden, abonniert. Das folgende Beispiel dient zur Verdeutlichung.

Topic: it (die sogenannte Root-Wildcard abonniert alle Topics)

Beispiel: Topic: Buerogebaeude/Erdgeschoss/#

Als Ergebnis werden folgende Topics abonniert:

- Buerogebaeude/Erdgeschoss/Serverraum/Temperatur
- Buerogebaeude/Erdgeschoss/Serverraum/Luftfeuchtigkeit
- Buerogebaeude/Erdgeschoss/Besprechungszimmer/Temperatur
- Buerogebaeude/Erdgeschoss/Besprechungszimmer/CO₂
- Buerogebaeude/Erdgeschoss/BueroChef/Temperatur
- Buerogebaeude/Erdgeschoss/BueroChef/CO₂

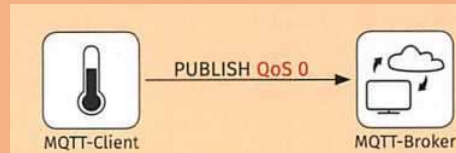
LE 4 - Quality of Service und Last Will Testament

Quality of Service (QoS) steht für den Grad der Zuverlässigkeit, mit der Nachrichten zugestellt werden. MQTT ist in drei QoS-Stufen eingeteilt: 0, 1 und 2. Dabei steht jede Stufe für eine definierte Verbindlichkeit, auf deren Einhaltung sich ein Empfänger verlassen kann. Jede Stufe berücksichtigt dabei eine Abwägung zwischen der Zuverlässigkeit der Nachrichtenübermittlung und dem Ressourcenverbrauch.

Quality of Service (QoS) - Stufenmodell

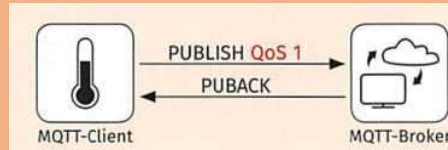
QoS 0: At most once - höchstens einmal

QoS der Stufe 0 garantiert, dass eine Nachricht höchstens einmal ankommt. Das bedeutet nicht, dass eine Nachricht überhaupt ankommt. Der Sender übermittelt eine PUBLISH-Nachricht, welche mit der Stufe „QoS 0“ gekennzeichnet ist und befasst sich damit nicht weiter. Dieses Message Exchange Pattern wird darum auch „Fire and Forget“ genannt. Die Vorteile von „Fire and Forget“ sind eine schnelle Kommunikation und ein geringer Ressourcenverbrauch.



QoS 1: At least once - mindestens einmal

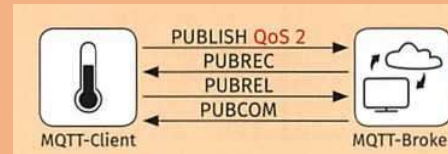
QoS 1 garantiert, dass eine Nachricht mindestens einmal beim Empfänger eintrifft. Sie kann aber auch mehrere Male beim Empfänger eintreffen. Dies kann je nach Anwendungsfall problematisch sein. Bei einer automatisierten Bestellung könnten Duplikate einer Nachricht zu mehreren Bestellungen und somit zu mehrfachen Auslieferungen führen. Bei Messwerten, z. B. der Raumtemperatur, ist es weniger problematisch, da hier Duplikate meistens nicht kritisch sind. Der Sender kann eine Nachricht vor dem Versenden im Speicher ablegen. So steht sie immer noch für eine erneute Übertragung zur Verfügung, sollte es einen Systemausfall geben. Der Sender übermittelt mit dem PUBLISH-Paket einen Packet Identifier zum Empfänger. Der Empfänger quittiert daraufhin den Empfang mit einem PUBACK-Paket, das denselben Packet Identifier enthält. PUBACK steht dabei für PUBLISH-Paket quittiert (acknowledged). Vor dem Empfangen des PUBACK-Paketes kann der Sender die Nachricht mit dem Packet Identifier und dem ursprünglichen Inhalt so oft er möchte an den Empfänger senden. Sobald das PUBACK empfangen wurde, wird eine erneute Nachricht mit demselben Packet Identifier als neue Nachricht ausgelegt. Sollte sich ein erneuter Sendeversuch (Retry) mit dem PUBACK-Paket zeitlich überschneiden, kann es dabei zu einer Duplizierung der Nachricht kommen. Bei QoS 1 sollte der Empfänger wissen, wie man mit Duplikaten umgeht. Mit dem Empfang von PUBACK beim Sender geht die Verantwortung für die Nachricht auf den Empfänger über.



Quality of Service (QoS) - Stufenmodell

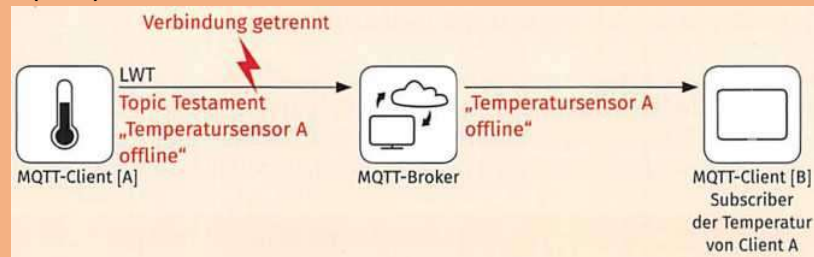
QoS 2: Exactly once - genau einmal

Die höchste Stufe „QoS 2“ garantiert, dass Nachrichten weder verloren gehen noch Duplikate entstehen. Eine Nachricht kommt exakt einmal beim Empfänger an. Um das zu garantieren, braucht es einen zweistufigen Bestätigungsablauf. Durch die hinzukommenden Nachrichten verzögert sich die Zustellung und wertvolle Bandbreite wird beansprucht. Nach dem Empfang einer Nachricht antwortet der Empfänger mit einem PUBREC-Paket (erhalten = received). Darauf folgt ein PUBREL-Paket (freigeben = released) des Senders, auf das der Empfänger wieder mit einem PUBCOMP (alles erhalten = complete) antwortet. Den genauen Ablauf zeigt das Schaubild.



Last Will Testament (LWT)

Wurde die Verbindung zwischen Sender und Broker unterbrochen, kann der Broker stellvertretend für einen Publisher eine Nachricht als dessen „letzten Willen“ versenden. So kann ein Publisher auch nach dessen Verbindungstrennung bestimmen, welchen Wert oder welches Kommando seine Subscriber bekommen. Das Testament ist besonders nützlich, da die Subscriber informiert werden können, wenn ein Verbindungsproblem zwischen Publisher und Broker besteht.



LE 5 - Message Persistence - Beharrlichkeit einer Nachricht

Wird die Verbindung zu einem Client unterbrochen, so kann der Server neue Nachrichten für diesen Client für eine spätere Zustellung Zwischenspeichern.

Verbindungsmanagement zwischen Client und Server

Retained Messages - eine zurückgehaltene Nachricht

Wenn ein Empfänger das erste Mal einen Topic abonniert, erhält er grundsätzlich erst eine Nachricht, wenn ein Publisher eine neue Nachricht an das Topic sendet. Nimmt man als Beispiel eine Temperaturanzeige, so würde nach der Verbindung mit einem Topic so lange kein Wert angezeigt werden, bis ein Temperaturfühler einen neuen Wert an das Topic sendet. Mit Retained Messages bekommt ein Subscriber den Wert, der vor der Subscription als letztes an das Topic gesendet wurde, sofort zugestellt. Anstatt keinen Wert anzuzeigen, kann immerhin ein älterer Wert angezeigt werden. Dieses Konzept wird auch Last Valve Queue genannt.

Verbindungsmanagement zwischen Client und Server

Persistent Sessions - eine dauerhafte Verbindung

Zwischen Client und Server ist es möglich, eine Sitzung aufzubauen, die länger als eine physikalische Netzwerkverbindung lebt. Ein Empfänger kann sowohl angehalten als auch neu gestartet werden und im Anschluss die bestehende Session wieder aufnehmen. Sollte der Empfänger in dieser Zeit Nachrichten verpasst haben, kann der Server diese an ihn ausliefern. Eine Session wird über einen Client Identifier eindeutig identifiziert.

Keep Alive

Clients können dem Server über Keep Alive eine Zeitvorgabe übermitteln, wie lange eine inaktive Verbindung aufrechterhalten werden soll. Sobald diese Zeit überschritten wird, trennt der Server die Verbindung automatisch. Sendet der Client vor Ablauf der Keep-Alive-Vorgabe ein PINGREQ-Paket, beginnt eine neue Zeitmessung. Der Server muss den PINGREQ mit PINGRESP bestätigen. Folglich überprüft PINGREQ den Status der Netzwerkverbindung zum Server.

Web Sockets Transport

Um eine Push-Nachricht von einem Broker an einen beliebigen Browser zu schicken, benötigt es sogenannte MQTT over Web Sockets. Damit können Webbrowser direkt mit einem Broker eine Verbindung aufbauen.

LE 6 - Eigenschaften von MQTT

- **Performance:** MQTT wurde für Netzwerke mit großer Verzögerungszeit und kleiner Bandbreite entwickelt. Sehr kleine Nachrichten können sehr schnell und in großen Mengen ausgetauscht werden. Die notwendigen Header-Felder wie QoS oder Flags werden ressourcenschonend als Binärwerte gespeichert. Selbst definierte Header werden nicht unterstützt. Ideal eignet sich MQTT für kleinste Nachrichten, beispielsweise einzelne Messwerte von Sensoren. Eine Komprimierung auf Protokollebene ist nicht verfügbar. Bei etwas größeren Nachrichten ab wenigen Kilobyte, kann es effizienter sein, die Nachricht über HTTP mit Komprimierung zu transportieren.
- **Skalierbarkeit:** MQTT wurde dafür entwickelt, die wachsende Anzahl von Sensoren und Geräten mit nur einem Server zu vernetzen. Gerade der Transport von vielen kleinen Nachrichten zwischen vielen Geräten ist eine ideale Anwendung von MQTT.
- **Sicherheit:** MQTT selbst unterstützt nur eine Absicherung über Benutzername und Passwort. Mit SSL bzw. TLS kann die Kommunikation auf Transportebene verschlüsselt werden. Für zusätzliche Sicherheit können Broker/Client-Zertifikate für die Authentifizierung verwendet werden oder beispielsweise durch die Überprüfung der IP den Zugriff über Access Control Lists einschränken.

LE 7 – Machine-to-Machine-Kommunikation mit dem Standard „OPC UA“ untersuchen

Nicht angeschlossene Maschinen und Anlagen sollen in ein IP-basiertes Netzwerk mittels IoT-Technologien eingebunden werden. Dabei steht die Standardisierung der Machine-to-Machine-Kommunikation im Mittelpunkt. Dieses Ziel zu erreichen, bemühen sich Firmen und Konsortien auf der ganzen Welt, z. B. die OPC Foundation mit OPC UA.

Machine-to-Machine (M2M)

Der automatisierte Informationsaustausch zwischen Maschinen, Anlagen, Automaten, Fahrzeugen und Containern wird als M2M bezeichnet. Das bedeutet, dass einzelne Maschinensteuerungen untereinander und mit einer zentralen Leitstelle kommunizieren können. Bestehende Maschinen und Anlagen können mit cyber-physischen Systemen nachgerüstet werden, um diesen M2M-Informationsaustausch zu ermöglichen.

Eine von vielen zentralen Herausforderungen der Industrie 4.0 sowie dem industriellen Internet der Dinge (IIoT) ist ein sicherer, standardisierter Daten- und Informationsaustausch zwischen Maschinen, Anlagen, cyber-physischen Systemen und auch Diensten verschiedener Branchen. Grundvoraussetzung für den Einsatz des Industriestandards OPC UA zur Kommunikation im IIoT ist ein auf dem Internetprotokoll (IP) basierendes Netzwerk. Nur wenn die Vernetzung der zentralen Komponenten auf einem einheitlichen und globalen Kommunikationsstandard beruht, der die komplexer werdenden Anforderungen erfüllen kann, lässt sich die IIoT-Vision erfüllen. Des Weiteren ist neben einem Publish/Subscriber-Modell wie MQTT ein sicheres und verbindungsorientiertes Client/Server-Kommunikationsmodell notwendig, um eine bidirektionale Kommunikation mit steuernden Eingriffen auf Akteure zu ermöglichen. Zusätzliche Voraussetzungen sind zum einen die Skalierbarkeit und Integrationsfähigkeit über allen Ebenen sowie die Hersteller- und Plattformunabhängigkeit.

OPC UA

OPC UA (Open Platform Communications Unified Architecture) ist ein Industriestandard für die Kommunikation zwischen Maschinen untereinander bzw. zwischen Maschinen

und Computersystemen. Es handelt sich dabei um einen offenen Schnittstellenstandard. Der Standard ist herstellerunabhängig und kann mit zahlreichen Entwicklungsumgebungen programmiert werden.



Die folgenden Anforderungen der Industrie 4.0 werden mit dem Standard „OPC UA“ erfüllt.

- **Unabhängigkeit der Kommunikationstechnologie:** Die OPC Foundation ist eine herstellerunabhängige Non-Profit-Organisation. Weder für den Einsatz noch die Erstellung von OPC-UA-Produkten und -Technologien benötigt man eine Mitgliedschaft. OPC hat die größte Verbreitung im Bereich der Automatisierung, ist aber technologisch branchenneutral. OPC UA ist sowohl auf allen Betriebssystemen als auch auf Chip-Ebene ohne Betriebssystem lauffähig. OPC UA ist in vielen Programmiersprachen umsetzbar.
- **Skalierbarkeit:** Skalierbarkeit zur durchgängigen Vernetzung vom kleinsten Sensor über eingebettete (embedded) Geräte und SPS-Steuerungen bis PC und Smartphone sowie Großrechner und Cloudanwendungen; horizontale und vertikale Kommunikation über alle Ebenen
- **Sicherheit:** Sicherheit der Übertragung sowie Authentifizierung auf Anwender- und Anwendungsebene
- **Serviceorientierte Architektur (SOA):** SOA-Transport über etablierte Standards wie TCP/IP für den Austausch von Echtzeitdaten, historischen Daten, Kommandos und Ereignissen
- **Prüfbarkeit der Konformität zum definierten Standard:** OPC UA bereits IEC-Standard (IEC 62541)

Das Grundprinzip der OPC UA-Architektur besteht aus vier zentralen Komponenten: der Bereitstellung einfacher Schnittstellen, eines einheitlichen Nachrichtenformats, flexibler Erweiterungsmöglichkeiten und der Implementierung hoher Sicherheitsstandards. Damit bietet die OPC UA eine anpassungsfähige Architektur, die sich schnell an die fortlaufend weiterentwickelte Industrieautomation anpassen kann. Egal ob Sensor oder Cloud, OPC UA kann auf jedem beliebigen Betriebssystem genutzt werden. Durch den herstellerunabhängigen Austausch an Informationen ist OPC UA zu einem wesentlichen Baustein für die Entwicklung der Industrie 4.0 geworden.

OPC-UA-Architektur

Topologie

OPC UA verwendet ein TCP-basiertes Protokoll, dem der Port 4840 zugewiesen wird. Da der binäre Datenaustausch von der OPC-UA-Spezifikation vorgeschrieben wird, kann er von jeder OPC-UA-Anwendung unterstützt werden. Darüber hinaus wird das Webservice-Protokoll verwendet, welches das Transportprotokoll HTTP oder HTTPS unterstützt. Auch in diesem Fall werden gegebenenfalls vorgeschriebene Ports zugewiesen (Port 80 und Port 443).

Client-Server-Prinzip

OPC UA geht nach dem Client-Server-Prinzip vor. Das bedeutet, dass der OPC-UA-Server sowohl Daten als auch Informationen bereitstellt, auf die OPC-UA-Clients zugreifen können. Ein Gerät kann Server und Client gleichzeitig sein.

Konfiguration

OPC UA nutzt IP-Adresse oder Gerätenamen zur genauen Adressierung. Der Local-Discovery-Server kann von dem Netzwerk verwendet werden, um nach verfügbaren OPC-UA-Servern zu suchen. Dabei ist die Verbindungssicherung ein zentrales Element bei der Verbindungskonfiguration. Je nachdem, welche Sicherheitsstufe angefordert wird, kann zusätzlich eine authentifizierte, signierte und verschlüsselte Verbindung aufgebaut werden. Die Konfiguration des OPC-Clients erfolgt weitestgehend automatisch.

Sicherheit

OPC UA nutzt in Bezug auf Cybersicherheit die neuesten Technologien, was für Datenübertragungen über das Internet von großem Vorteil ist. Das Sicherheitskonzept umfasst folgende Punkte:

- Sicherstellung der Informationssicherheit hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit
- Zugriffskontrolle mit Authentifizierung, Autorisierung und Auditierbarkeit
- Verschlüsselte und signierte Nachrichtenübertragung

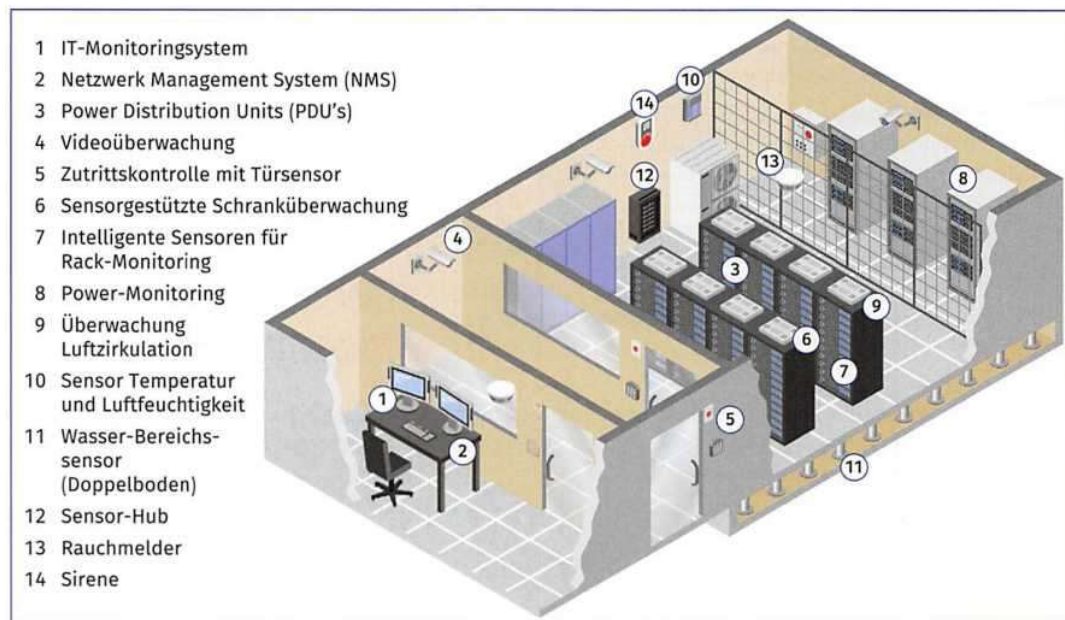
Die meisten SPS-, MES- und Visualisierungshersteller unterstützen diesen Standard. Außerdem ermöglicht OPC UA eine umfangreiche Skalierung von IoT-Anwendungen, welche von den kleinsten Geräten bis hin zu großen IT-Ebenen reicht.

Lernzielkontrolle TAG 4

1. Beschreiben Sie in eigenen Worten das Publisher/Subscriber-Prinzip, dass bei MQTT eingesetzt wird.
2. Diskutieren Sie in Arbeitsgruppen die unterschiedlichen QoS-Level und sammeln Sie Einsatzfelder für QoS 0, QoS 1 und QoS 2.
3. Geben Sie den passenden Begriff an.
 - a. Die Kommunikation zwischen unterschiedlichen Maschinen
 - b. Abkürzung für das Internet der Dinge im industriellen Umfeld
 - c. Weltweit etablierter Datenaustauschstandard zur herstellerunabhängigen Kommunikation zwischen Maschinen
4. Beschreiben Sie mit eigenen Worten die Machine-Lo-Machine-Kommunikation und finden Sie Beispiele von Informationen, die Maschinen untereinander teilen können.
5. Erläutern Sie wesentliche Unterschiede zwischen MQTT und OPC UA und diskutieren Sie diese im Plenum.

TAG 5 - Ein bestehendes cyber-physisches System im Unternehmen analysieren

Nachdem Sie sich mit den anderen Auszubildenden in die Grundlagen von cyber-physischen Systemen und IoT eingearbeitet haben, möchte der Ausbildungsbeauftragte der Entwicklungsabteilung den Auszubildenden eine herausfordernde Projektaufgabe übergeben. Das Verwaltungsgebäude von JIKU IT-Solutions soll mit zusätzlichen Sensoren die Raumtemperatur, die Luftfeuchtigkeit und die CO₂-Konzentration in den unterschiedlichen Räumen erfassen und automatisiert das Raumklima und die Belüftung steuern. Für eine erste Bestandsaufnahme wird gemeinsam der Serverraum begutachtet, in dem schon zahlreiche Sensoren im Einsatz sind. Der Raum verfügt bereits über eine digitale Zutrittskontrolle mit Türsensor (5), Videoüberwachung (4), Sensoren zur Überwachung der Luftzirkulation (9), der Temperatur und der Luftfeuchtigkeit (10), einen Wasser-Bereichssensor (11) sowie einen Rauchmelder (13).



Die Serverraumüberwachung soll die geschäftskritische IT-Ausrüstung vor potenziellen Schäden durch technische Probleme schützen. Des Weiteren kann die Überwachung vor Schäden durch menschliches Versagen, Cyber-Attacken, Diebstahl und Sachbeschädigung warnen.

Potenzielle Gefahren im Serverraum

Zu hohe Temperatur

Eine permanente Überwachung der Temperatur, sowohl des Raums als auch aller Server-Racks, ist notwendig, um den IT-Administrator vor Leistungsminderungen zu warnen und die Raumtemperatur automatisiert zu senken.

Zu hohe Luftfeuchtigkeit

Elektronische Komponenten sind für einen definierten Luftfeuchtigkeitsbereich ausgelegt. Bei zu hoher Luftfeuchtigkeit können Datenträger beschädigt werden und bei zu geringer Luftfeuchtigkeit steigt die Gefahr von elektrostatischen Entladungen, was zu Beschädigungen von Elektronikbauteilen führen kann.

Einbruch, Diebstahl und Sachbeschädigung (Sabotage)

Die Zutrittskontrolle in den Serverraum sollte überwacht und protokolliert werden. Zusätzlich können Überwachungskameras Ereignisse wie das Betreten des Serverraums aufzeichnen oder direkt an Mobiltelefone von verantwortlichen IT-Mitarbeitern gestreamt werden.

Schmorbrände und Feuer

Rauchmelder stellen sicher, dass sowohl Feuerwehr als auch die verantwortlichen IT-Mitarbeiter schnellstmöglich informiert werden. Diese können unmittelbar mit der Implementierung des Disaster-Recovery-Plans beginnen, um weitere Ausfallzeiten zu minimieren, die Datenwiederherstellung zu starten und die Betriebssicherheit der verbleibenden IT-Infrastruktur sicherzustellen.

Netzausfall

Die Netzspannung muss stetig überwacht werden, um Stromausfälle schnellstmöglich zu beheben. Defekte USV-Geräte (USV = unterbrechungsfreie Stromversorgung) müssen sofort ausgetauscht werden.

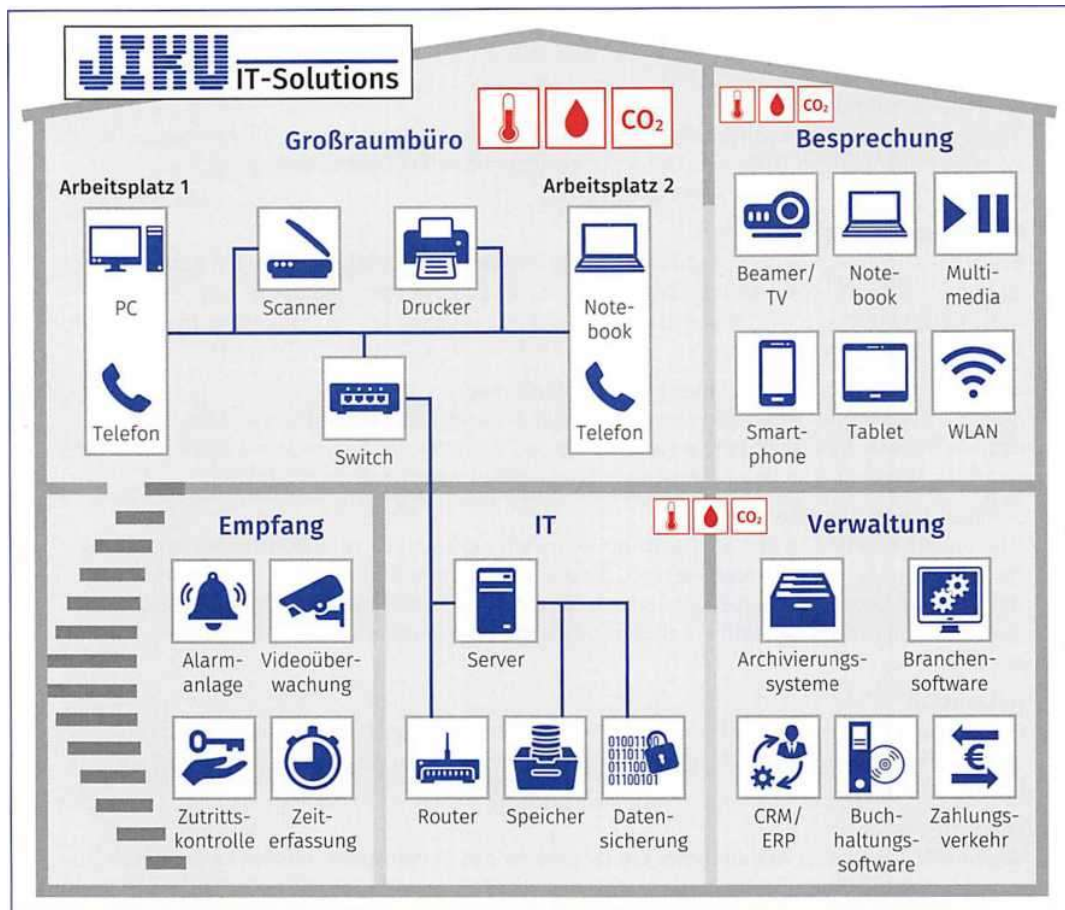
Wasserleckagen

Bei Eintritt von Wasser in den Doppelbodenbereich des Serverraums müssen sofort die IT-Mitarbeiter und die Gebäudeverwaltung informiert werden, um den Schaden schnellstmöglich zu beheben und kritische IT-Geräte zu schützen.

Die erfassten Daten aller Sensoren können den Mitarbeitern mittels Datenvisualisierung auf einem Dashboard angezeigt werden. So haben die IT-Mitarbeiter ein Echtzeitmonitoring des Serverraums auf ihren Mobilgeräten, auf dem auch alle Fehler- und Alarmmeldungen angezeigt werden.

Analog zu den Beispielen des Serverraums können sowohl Smart Homes als auch industrielle Maschinen und Anlagen überwacht und geschützt werden. Speziell in der Industrie ermöglichen cyber-physische Systeme die Nachrüstung von bestehenden Maschinenparks.





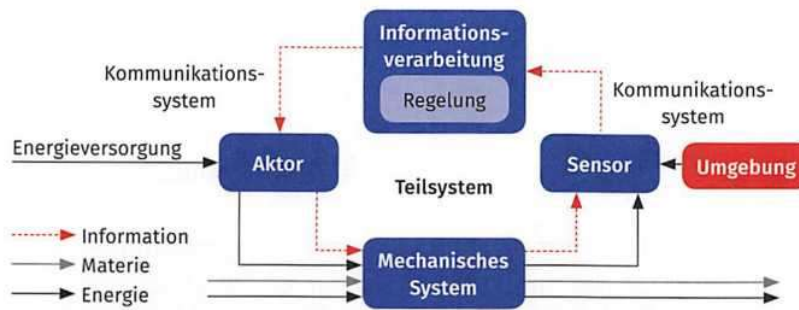
Wie eingangs beschrieben, sollen die Auszubildenden die Büro-, Besprechungs- und Verwaltungsräume mit vernetzten Sensoren ausstatten, die somit eine Regelung des Raumklimas und der CO₂-Konzentration ermöglichen.

Zur Auswahl geeigneter Sensoren und Mikrocontroller ist es notwendig, eine Systembetrachtung des geplanten cyber-physischen Systems vorzunehmen. In einem technischen System müssen die Informations-, Material- und Energieflüsse in das System und aus dem System heraus betrachtet werden. Dieser Ansatz ermöglicht die Schnittstellenauswahl für die Kommunikation und Energieversorgung eines cyberphysischen Systems.

LE 1 - Den Datenfluss an CPS-Schnittstellen und innerhalb eines Netzwerks vergleichen

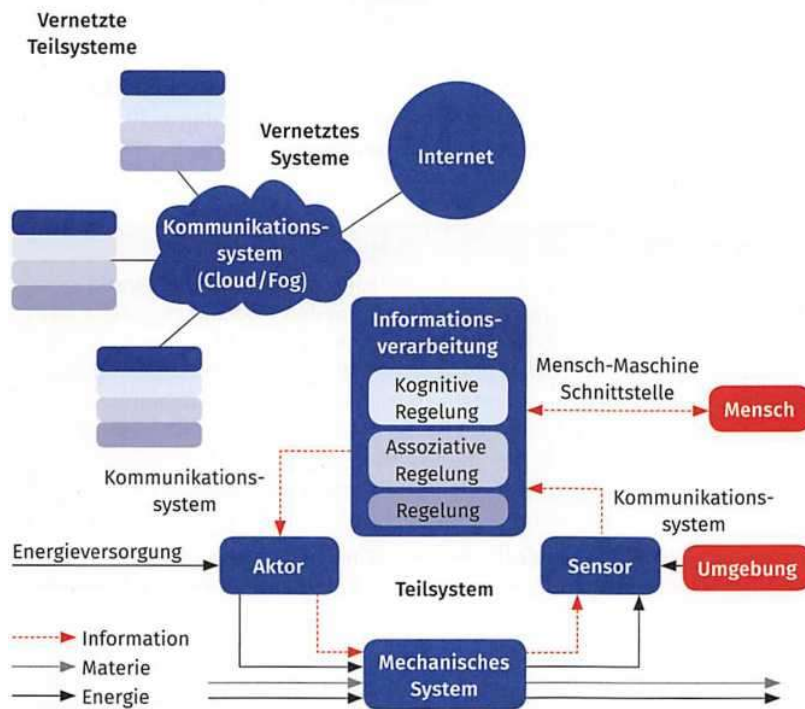
Ein reines mechatronisches System besteht im Wesentlichen aus den abgebildeten Komponenten (siehe folgende Abbildung). Es ist in sich geschlossen und arbeitet einseitig mit den definierten Informations-, Material- und Energieflüssen. Auch aus Sicht des Teilsystemausgangs sind die Informationen, die Material- und Energieflüsse lokal zu betrachten.

Mechatronisches System mit integrierter Regelung



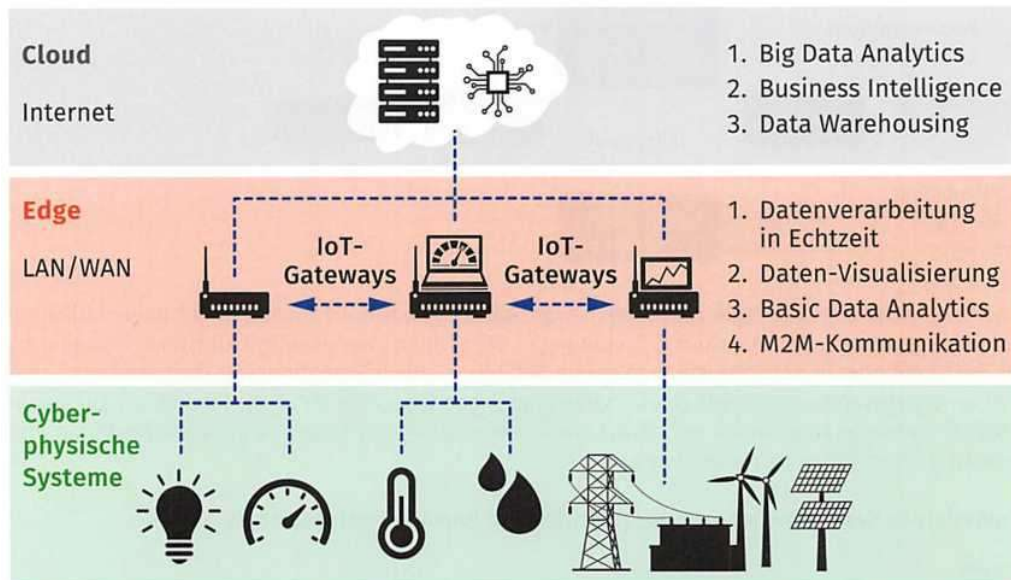
Ein cyber-physisches System ergänzt ein mechatronisches System mit Funktionen zur Kommunikation und Vernetzung mit anderen Maschinen, Steuerungen, Menschen, aber auch mit künstlicher Intelligenz (KI) aus der Cloud oder in der Edge (siehe folgende Abbildung). Die Informationsverarbeitung kann somit durch KI erweitert werden und stellt einem cyber-physischen System mehr „Eigenintelligenz“ zur Verfügung, was bestehende Regelungen mit assoziativen (vernetzten) und kognitiven (wahrnehmenden und „denkenden“) Algorithmen weiter optimiert.

Cyber-physisches System mit integrierter Regelung und Kommunikationseinheit



Die notwendigen Schnittstellen hängen von zahlreichen Faktoren ab (siehe auch Kapitel 7.2). Es ist zu klären, ob beispielsweise zwei cyber-physische Systeme lokal über einen MQTT-Broker Nachrichten sicher austauschen dürfen oder ob die Daten sicher über das Internet weltweit bereitgestellt werden sollen. Im industriellen Umfeld werden die Daten häufig an ein IoT-Gateway geschickt, welches in der Edge erste Datenverarbeitungen, -analysen und -Visualisierungen durchführen kann. Alternativ können die Sensoren an einer Speicherprogrammierbaren Steuerung (SPS) angeschlossen werden. Moderne Speicherprogrammierbare Steuerungen besitzen integrierte OPC-UA-Server, die eine sichere Vernetzung mit anderen Maschinen, Anlagen und Mensch-Maschine-Schnittstellen (HMI = Human Machine Interface) ermöglichen. Die folgende Abbildung zeigt die wesentlichen

Schichten von der Sensorebene über das Edge-Computing mit den IoT-Gateways bis hin zum Cloud Computing.



Darüber hinaus muss genau betrachtet werden, unter welchen Bedingungen das cyber-physische System betrieben wird. Die folgende Übersicht zeigt Beispiele von Arbeitsplatztypen und den Einfluss auf die ganzheitliche Betrachtung des cyber-physischen Systems mit all seinen Informations-, Material- und Energieflüssen.

Arbeitsplatztypen und Einsatzgebiete

Sensorüberwachung von Restfeuchtigkeit nach einem Wasserschaden (Einsatz im Handwerk)

Es können Feuchtigkeitssensoren in einer Wand angebracht werden, um den Trocknungszustand nach einem Wasserschaden zu messen. Sobald die Wand trocken genug für eine Renovierung ist, meldet der Sensor automatisiert die Restfeuchtigkeit an den Handwerksbetrieb. Ein weiterer Sensor überwacht den Flüssigkeitsfüllstand des verwendeten Luftentfeuchters. Wenn der Wasserbehälter voll ist, informiert das Gerät die Eigentümer der Wohnung oder des Hauses, z. B. per SMS, damit diese den Behälter leeren können. Diese Lösung verkürzt nicht nur die Trocknungszeit, sondern eliminiert auch unnötige Betriebsunterbrechungen des Luftentfeuchters. Der Handwerksbetrieb muss für diese Aktivitäten nicht zur Baustelle fahren, was Zeit und Kosten einspart.

Verstopfte Regenrinne ruft automatisch den Dachdeckerbetrieb (Einsatz im Handwerk)

Über Gewichtssensoren können verstopfte Regenrinnen identifiziert werden, wenn ein sich definierter Wasserstand (entspricht einem definierten Gewicht) in einer bestimmten Zeit nicht verändert. Somit können im Notfall sowohl der Handwerksbetrieb als auch die Eigentümer per Kurznachricht informiert werden.

Intelligente, elektronisch gesteuerte Fenster (Einsatz in der Bauindustrie und im Handwerk)

Mittels Temperatur- und Feuchtigkeitssensoren lässt sich eine intelligente Fensterschaltung realisieren. Ein Kombisensor misst gleichzeitig die Werte im Raum und im Freien. Ein Algorithmus mit Wenn- Dann-Funktion entscheidet, ob die automatische Lüftung aktiviert wird und die Fenster geöffnet werden sollen. Wenn beispielsweise die Luftfeuchtigkeit im Raum höher ist als die Luftfeuchtigkeit im Freien, öffnen sich die Fenster. In diesem Fall werden Service und Produkt als Komplettpaket verkauft. Durch intelligente Belüftung erhalten Kunden nicht nur elektronisch gesteuerte Fenster, sondern auch ein gesundes Raumklima. Dieser Ansatz wird auch als Produkt-Service-System bezeichnet.

Arbeitsplatztypen und Einsatzgebiete

Moderner Denkmalschutz durch nachträglich integrierte Sensorik

An alten Bauwerken und Statuen angebrachte Sensoren erfassen Luft- und Fugenfeuchtigkeit sowie die Material- und Umgebungstemperatur. Die erfassten Daten werden drahtlos an die Firma übermittelt, die die Daten auswertet und entsprechende Aktionen einleitet. Dies ermöglicht eine permanente Kontrolle aus der Ferne und eliminiert die Häufigkeit von Vor-Ort-Analysen der schützenswerten Denkmäler.

Überwachung der Wasserqualität von Badeseen

Die laufende Überwachung der Wasserqualität an Badeseen ist mittels Fernüberwachung vergleichbar zu realisieren, wie das zuvor beschriebene Beispiel mit dem Denkmalschutz. Es kommen lediglich unterschiedliche Sensoren zum Einsatz.

Direkte Messung der Temperatur und zentrale Überwachung aller Produkte entlang der

Kühlkette im Lebensmittelhandel

Kleinste Sensoren können direkt an Lebensmittelverpackungen angebracht werden und somit die Temperatur über die gesamte Kühlkette von der Verpackung über den Transport bis hin zur Lagerung im Supermarkt aufzeichnen. Die erfassten Daten könnten über Nahfeldkommunikation an IoT-Gateways übertragen werden und die Betriebe des Lebensmittelhandels könnten die Temperatur von einzelnen Verpackungen lückenlos überwachen und dokumentieren.

Energiemanagement, vorausschauende Instandhaltung und Identifikation von Anomalien in der Industrie

Dieser Bereich ist zentrales Element der technologischen Entwicklung in der Industrie 4.0. Daher ist nachvollziehbar, dass im industriellen Umfeld die Arbeitsplätze und Einsatzgebiete von cyber-physischen Systemen sehr vielfältig sind. Wärme, Kälte, Schmutz, ölhaltige Luft, starke Vibrationen oder hohe Kräfte sind nur einige Rahmenbedingungen, die bei der Konzeption berücksichtigt werden müssen.

Optimierung von Raumklima und Lichtsteuerung

Neben der Funktionalität tritt beim Einsatz von Smart-Home-Devices auch die Ästhetik und somit das Design des cyber-physischen Geräts in den Vordergrund. Ein sichtbarer Sensor soll optisch und haptisch mit der restlichen Raumausstattung harmonisieren.

LE 2 - Energie-, Stoff- und Informationsflüsse eines exemplarischen cyber-physischen Systems erläutern

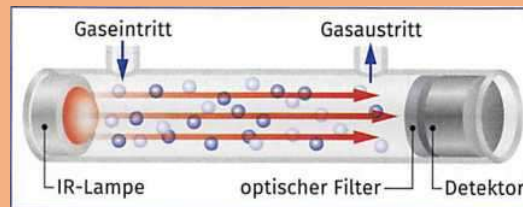
Die Luftqualität in Arbeits- und Wohnräumen ist von großer Bedeutung. Viren und Bakterien können auf verschiedenen Wegen übertragen werden, so auch über die ausgeatmete Luft. In Form von Tröpfchen oder Aerosolen gelangen sie in die Raumluft und verbreiten sich mühelos. Aerosole sind Kleinstpartikel, die über einen langen Zeitraum in der Raumluft verweilen können. So kann der CO₂-Anteil, der durch die ausgeatmete Luft in den Raum gelangt, als Referenz für die Luftqualität genutzt werden. Je höher der Anteil der ausgeatmeten Luft ist, desto höher ist auch der CO₂-Anteil.

Klassifizierung der Raumlufthqualität nach DIN EN 13779: 2007-09 (DIN 2007-09)/IDA (= In-Door Air)	
Raumlufthkategorie	Eigenschaften
IDA 1	Hohe Raumlufthqualität Erhöhung der CO ₂ -Konzentration gegenüber der Außenluft in ppm: < 400 Absolute CO ₂ -Konzentration in der Innenraumlufth in ppm: < 800
IDA 2	Mittlere Raumlufthqualität Erhöhung der CO ₂ -Konzentration gegenüber der Außenluft in ppm: > 400-600 Absolute CO ₂ -Konzentration in der Innenraumlufth in ppm: > 800-1000
IDA 3	Mäßige Raumlufthqualität Erhöhung der CO ₂ -Konzentration gegenüber der Außenluft in ppm: > 600-1000 Absolute CO ₂ -Konzentration in der Innenraumlufth in ppm: > 1000-1400
IDAA	Niedrige Raumlufthqualität Erhöhung der CO ₂ -Konzentration gegenüber der Außenluft in ppm: > 1000 Absolute CO ₂ -Konzentration in der Innenraumlufth in ppm: > 1400

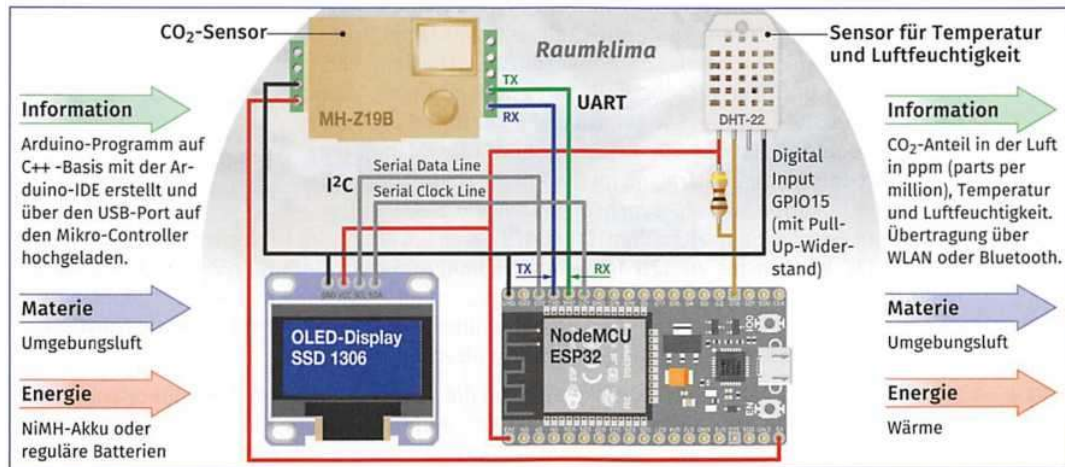
Ein cyber-physisches System, das neben Temperatur und Luftfeuchtigkeit auch die Kohlendioxid-Konzentration in der Umgebungsluft erfasst und den CO₂-Anteil in ppm über WLAN oder Bluetooth übertragen kann, ist in der folgenden Abbildung dargestellt. Der CO₂-Sensor (MH-Z19B) misst den Kohlendioxid-Gehalt der Umgebungsluft nach dem NDIR-Prinzip.

NDIR-Sensor

In einem NDIR-Sensor (nicht dispersiver Infrarotsensor) wird, wie in der nebenstehenden Abbildung dargestellt, ein Infrarotstrahl durch ein Gasgemisch, z.B. die Umgebungsluft, geschickt. Jedes Gas der Umgebungsluft absorbiert Infrarotlicht einer bestimmten Wellenlänge. Die CO₂-Konzentration wird elektro-optisch über das Ausmaß der Absorption der spezifischen Wellenlänge bestimmt.



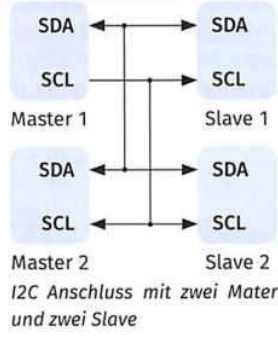
Bei einem cyber-physischen System sind für Fachinformatikerinnen und Fachinformatiker die Informationsflüsse von höchster Relevanz. Neben den exemplarisch dargestellten Informationen am Eingang und am Ausgang des Systems sind auch die internen Informationsflüsse von großer Bedeutung. Um beispielsweise Sensoren und Aktoren mit dem Mikrocontrollerboard zu verbinden, stehen im Wesentlichen die Varianten zur Anbindung zur Verfügung, die in der nächsten Tabelle aufgeführt sind.



EVA-Prinzip - Eingabe, (interne) Verarbeitung, Ausgabe

In der oberen Abbildung sind die Verbindungen der verwendeten Sensoren mit GPIO, UART und I2C gekennzeichnet. Dies sind Abkürzungen für wichtige Schnittstellen bei Mikrocontrollern und Einplatinencomputern. In der folgenden Tabelle sind die Eigenschaften der genannten Schnittstellen beschrieben.

Anbindung von Sensoren und Aktoren auf Mikrocontrollerboards und Einplatinencomputern	
GPID	GPID (General Purpose Input/Output) bezeichnet universelle Ein- und Ausgänge, die durch die Programmierung frei bestimmbar sind. In den meisten Fällen sind die GPIO-Pins als Stiftleiste oder als Lötunkte auf den Einplatinencomputern und Mikrocontrollerboards angebracht und dienen als Schnittstelle für digitale und analoge Signale von außen (Input) oder für Signale nach außen (Output)
UART	UART (Universal Asynchronous Receiver and Transmitter) ist eine recht einfache Schnittstelle, weswegen man nur zwei Datenleitungen benötigt. Eine Leitung sendet Daten (Transmit Data – TX) an ein zweites Gerät. Die Leitung wird am zweiten Gerät an dessen „Empfangs-Pin“ angeschlossen (Receive Data – RX). In der Umkehrung verbindet sich der TX-Pin des zweiten Geräts mit dem RX-Pin des ersten Geräts. UART verwendet keinen Clock (Takt) zum Takte des Signals, sondern benutzt Start- und Stop-Bits. Der Empfänger beginnt mit dem Lesen der Daten, sobald er ein Start-Bit erhalten hat und macht dies so lange, bis er das Stop-Bit empfängt. Die sogenannte BAUD-Rate legt fest, mit welcher Geschwindigkeit die Daten gesendet werden. Die Einheit BAUD wurde nach dem Franzosen Émile Baudot benannt und steht für die Einheit der seriellen Übertragungsgeschwindigkeit (1 BAUD = 1 Bit/s) Gerät 1 Gerät 2 UART Anschluss mit zwei Geräten

Anbindung von Sensoren und Aktoren auf Mikrocontrollerboards und Einplatinencomputern	
I2C	I2C steht für Inter-Integrated-Circuit. Die beiden I aus Inter- Integrated werden zusammengefasst und als I²C oder I2C geschrieben. Gesprochen wird die Abkürzung als „I-Quadrat-C“ oder im Englischen „I-Squared-C“. Seinen Ursprung hat dieses Bus-System in den frühen 1980er-Jahren. Es wurde vom Unternehmen Philips mit dem Ziel entwickelt, eine einfache Kommunikation zwischen zwei Komponenten zu schaffen. Vergleichbar mit UART hat I2C ebenfalls nur zwei Leitungen. Eine davon ist die SDA-Leitung (Serial Data Line), um Daten zu übertragen. Die andere ist die SCL-Leitung (Serial Clock Line), um einen Takt-Impuls zu übertragen. Im Gegensatz zu UART erfolgt die Kommunikation bei I2C synchron durch die SCL-Leitung. Daher sind Geschwindigkeiten von 100 Kbit/s bis zu 3,4 Mbit/s im Highspeed-Modus erreichbar. Bei I2C können bis zu 128 Teilnehmer kommunizieren (bei einer 7-bit-Adressierung). Jeder davon hat eine eindeutige Adresse. Insgesamt 112 Adressen können frei genutzt werden, die restlichen sind fest reserviert. Die Datenübertragungsgeschwindigkeit wird bestimmt, indem während jedes Takt-Zyklus ein Datenbit übertragen wird.  I2C Anschluss mit zwei Master und zwei Slave
SPI	SPI wurde 1987 von Motorola entwickelt und ist die Abkürzung für Serial Peripheral Interface. Anders als bei I2C und UART werden für die Kommunikation über die SPI-Schnittstelle vier Leitungen benötigt. • SCL - Serial Clock Leitung: Clock (Takt) wird vom Master ausgegeben • MOSI - Master Output/Slave Input: Leitung für Daten vom Master zum Slave • MISO - Master Input/Slave Output: Leitung für Daten vom Slave zum Master • CS - Chip Select: Auf dieser Leitung gibt der Master ein LOW-Signal aus, um mit dem entsprechenden Slave, der an dieser CS-Leitung angeschlossen ist, zu kommunizieren. Wenn der Master die CS-Leitung wieder auf HIGH setzt, ist die Kommunikation mit dem Slave abgeschlossen. SPI ist voll duplexfähig. Mit den beiden Datenleitungen (MOSI und MISO) können Daten mit bis zu 20 Mbit/s ausgetauscht werden. Im Unterschied zu I2C kann man bei SPI nur einen Master im Netzwerk einsetzen und die Anzahl der Slaves ist nur von der Verfügbarkeit der Pins (für die CS-Leitungen) vom Mikrocontroller abhängig.

Lernzielkontrolle TAG 5

1. Diskutieren Sie in der Gruppe, welche Maßnahmen Zur Gefahrenabwehr in Ihrem Ausbildungsbetrieb in den Serverräumen zum Einsatz kommen.
2. Geben Sie die passenden Fachbegriffe an.
 - a. Bereich, in dem Datenanalysen, Business Intelligence und Data-Warehousing-Anwendungen außerhalb des eigenen Rechenzentrums durchgeführt werden
 - b. Bereich im firmeneigenen LAN/WAN, in dem grundlegende Datenanalysen in unmittelbarer Nähe zu Maschinen und Anlagen durchgeführt werden
 - c. Bauteile, die physische Daten, wie z. B. Temperatur, Druck, Helligkeit erfassen
 - d. Schnittstelle zwischen Maschine und Mensch
3. Beschreiben Sie ein cyber-physisches System Ihrer Wahl als Blackbox und definieren Sie die Schnittstellen des Netzwerks, in dem das CPS eingesetzt werden soll.
4. Sammeln und diskutieren Sie im Team die Schutzmaßnahmen der Serverräume in Ihren Ausbildungsbetrieben.
 - a. Geben Sie die korrekte Schnittstelle zu den folgenden Aussagen an.
 - b. Es können mehrere Master bei dieser Schnittstelle zum Einsatz kommen.
 - c. Dieser Typ ist voll duplexfähig.
 - d. Jeder Pin kann individuell durch das Programm als Eingang oder als Ausgang genutzt werden.
 - e. Für jeden Slave wird eine separate CS-Leitung benötigt.
5. Die Kommunikation bei diesem Typ funktioniert durch die Zuordnung einer dedizierten Sende-/Empfangsleitung in die eine Richtung und einer zweiten Leitung mit entsprechend umgekehrter Richtung.

TAG 6 - Erweiterungen für ein cyber-physisches System planen

Zur Umsetzung des Projekts sollen Arbeitsräume des Verwaltungsgebäudes von JIKU IT-Solutions mit zusätzlichen Sensoren ausgestattet werden (siehe auch Kapitel 7.3). Die Sensoren müssen die Raumtemperatur, Luftfeuchtigkeit und CO₂-Konzentration in den unterschiedlichen Räumen erfassen und automatisiert das Raumklima und die Belüftung steuern. Ein erster wesentlicher Schritt bei der Projektplanung ist die Erfassung aller Anforderungen an das zu entwickelnde CPS mit den notwendigen Sensoren, der Darstellung der Informationen auf einem Dashboard und der Einbindung der CPS-Devices in das Firmennetzwerk. Der Ausbildungsbeauftragte erklärt auch, dass die genauen Anforderungen noch nicht komplett definiert sind und dass die Auszubildenden selbstständig im Team definieren sollen, wie sie die komplexe Projektaufgabe bewerkstelligen wollen.

Die Herausforderung für die Auszubildenden entspricht der heutigen Realität, in der Unternehmen flexibel agieren müssen, um sich an neue Veränderungen anzupassen. Die immer schneller werdenden technologischen Entwicklungen lassen sich durch das Kunstwort „VUCA“ charakterisieren.

Was bedeutet VUCA?



Wir leben in einer volatilen Welt, in der neue Technologien eine immer kürzere Halbwertszeit haben. Die Unternehmen sind durch den digitalen Wandel sehr vielen und dynamischen Veränderungen ausgesetzt. Die Kommunikationssysteme der Informationstechnologie (IT) und der Fertigung (Operational Technology, OT) verschmelzen dank intelligenter Automatisierungseinrichtungen, Cloud Computing und Edge Computing miteinander. Die Maschinen und Anlagen können heute wesentlich mehr nützliche Informationen bereitstellen als jemals zuvor. In vielen Fällen erfolgt die Erfassung, Nutzung und Bereitstellung via OPC UA und MQTT. Daten werden an IT-Domains übertragen, neue CPS-Devices und IoT-Gateways werden mit bestehenden Industrial-Ethernet-Netzwerken kombiniert, die sich ebenfalls permanent weiterentwickeln. Immer mehr Funktionen und Echtzeitfähigkeiten halten Einzug in heutige Smart Factories. Dies bedeutet, dass eine viel größere Datenvielfalt in den Fabrikhallen bereitgestellt und von lokalen IT-Funktionen gesammelt, vor Ort gespeichert und in die externe Cloud übertragen wird, um den Unternehmen neue Wettbewerbsvorteile zu verleihen.

Die IT/OT-Konvergenz ermöglicht eine neue Art der Vernetzung, die den Maschinen und Anlagen im Shopfloor (Fertigung) einen höheren oder gar komplett neuen Mehrwert verleiht. Der erweiterte Datenaustausch kann viele Vorteile bieten, vor allem im Bereich der Produktionsauslastung, des Qualitätsmanagements und der Prozessoptimierung. Gleichzeitig verfügen die industriellen Prozesse dadurch über viel bessere Möglichkeiten für die vorausschauende Wartung und Vorhersageanalyse. Das Energiemanagement sollte für ein produzierendes Unternehmen ganzheitliche betrachtet werden, da sowohl der Energiebedarf der Fertigung, aber auch der Verbrauch im Verwaltungsbereich durch intelligentes Energiemanagement optimiert werden kann.



LE 1 - Ein Projekt zur CPS-Erweiterung initiieren und die Anforderungen des Auftraggebers abstimmen

Einstmals große und bedeutende Firmen wie Kodak (ehemals weltweit bedeutendster Hersteller für fotografische Ausrüstung und Filmmaterial) oder Nokia (ehemals Weltmarktführer in Sachen Handy) spielen heute keine wesentliche Rolle mehr. Disruptionen kommen überall vor, so auch in der Industrie. Sie verändern, zerstören oder bilden Märkte. Betrachtet man beispielsweise unterschiedliche



Musikmedien, so gab es Plattenspieler, Kassettenrekorder, Walkman-, Disc man- und MP3-Player. Heutzutage sind Schallplatten und CDs meistens an einen emotionalen Wert gebunden, da der Tonträger selbst nicht mehr von weiterem Nutzen ist. Musik wird einfach gestreamt. Man muss die Anforderungen des Marktes permanent hinterfragen und neue technische Möglichkeiten sollten bezüglich Kundenmehrwertfortlaufend untersucht werden.

Für Hersteller ist es wichtig, bereits im Voraus diese Situationen zu erkennen. Essenzielle Fragen helfen ihnen, die Bedürfnisse von zukünftigen Benutzern und Kunden zu verstehen. Der Prozess dieser Anforderungsanalyse umfasst das Lastenheft, welches von Seiten des Auftraggebers die Fragestellung nach dem Was und Wofür beantworten soll, und das Pflichtenheft, welches vom Auftragnehmer das Wie und Womit spezifiziert. Für neue Technologien und sich schnell verändernde Rahmenbedingungen ist eine erweiterte Betrachtung von Anforderungen notwendig.

LE 2 - Requirements Engineering

Requirements Engineering beinhaltet das systematische Vorgehen beim Spezifizieren und Verwalten von Anforderungen an ein System, ein Produkt oder eine Software. Was sind die Gründe für Requirements Engineering, warum sind Anforderungen wichtig, was sind wichtige Begriffe und welche Fragen gilt es bei der Anforderungsanalyse zu beantworten? Diese Fragestellungen werden in diesem Kapitel schrittweise vorgestellt.

Requirements Engineering	
Fragestellungen	Aktivitäten
Was sind die Anforderungen an das Produkt und/oder die Dienstleistung? • Funktionen • Bedürfnisse • Fähigkeiten • Eigenschaften	Genaue Ermittlung der Anforderungen inklusive notwendiger Detaillierung mittels Marktanalysen, Fokusgruppen (Gruppengespräche mit möglichen Kundengruppen) und Kundengesprächen
Wie können die Kundenanforderungen genau spezifiziert werden? • Datenerfassung • Analyse • Validierung • Dokumentation	Prüfung und Abstimmung der Anforderungen mit den definierten Zielen im Qualitätsmanagement; genaue Dokumentation aller erfassten Anforderungen mit den entsprechenden Analyse- und Validierungsergebnissen
Wie sollen identifizierte Anforderungen verwaltet werden? • Freigabe der Anforderungen • Veränderung von bereits definierten Anforderungen • Rückverfolgbarkeit der vorgenommenen Veränderungen	Strukturiertes Verwalten der Anforderungen (Requirements Management)

Es ist nicht nur von großer Bedeutung, dass alle Anforderungen an das Produkt oder die Dienstleistung bestmöglich erfasst werden. Vielmehr gibt es Anforderungen, die nicht durch das neue Produkt selbst definiert werden. Dies können produktunabhängige Ziele des eigenen Unternehmens oder des Kunden sein oder auch Anforderungen von Interessensgruppen oder gesetzlichen Vorgaben. Daher lassen sich Anforderungen in vier Kategorien einteilen.

Kategorisierung von Anforderungen

Business Requirements

Sie beschreiben die Ziele, Ergebnisse und Merkmale eines neuen Produkts oder einer neuen Dienstleistung für den Endbenutzer und das Unternehmen.

Stakeholder Requirements

Die Bedürfnisse aller Stakeholder, welche berücksichtigt werden müssen, um die Business Requirements zu erfüllen, werden von den Stakeholder Requirements zusammengefasst.

Solution Requirements

Sie legen die Leistungsfähigkeit und Qualität einer Lösung dar, die das Ziel hat, die Stakeholder Requirements zu erfüllen. Sie werden unterteilt in funktionale und nichtfunktionale Anforderungen.

Transition Requirements

Sie beschreiben die Leistungsfähigkeit einer Lösung, um die Transition vom Ist-Zustand zum Soll-Zustand zu ermöglichen.

In der folgenden Übersicht werden wichtige Begriffe des Requirements Engineering erläutert. Diese Begriffe kommen heutzutage in vielen Produktentwicklungsumgebungen vor. Nicht nur in der reinen Softwareentwicklung, sondern auch bei der Entwicklung von Consumer Produkten oder im Maschinen- und Anlagenbau.

Wichtige Begriffe des Requirements Engineering

Anforderungskatalog

Ein Anforderungskatalog ist eine Auflistung von Anforderungen. Es handelt sich idealerweise um eine priorisierte Liste von Anforderungen an das Produkt oder die Dienstleistung. In vielen Fällen werden die Begriffe „Anforderungskatalog“ und „Lastenheft“ als bedeutungsgleich gesehen. Präziser ist es jedoch, den Anforderungskatalog als Bestandteil oder auch als Input des Lastenhefts zu verstehen.

Anforderungsliste

Die Anforderungsliste ist ein wesentlicher Bestandteil des Pflichtenhefts und unterstützt die Bewertung von Lösungsalternativen, mit denen Anforderungen erfüllt werden können. In der Praxis werden der Anforderungskatalog und die Anforderungsliste oftmals synonym verwendet. Beide beinhalten Anforderungen, aber der Anforderungskatalog des Kunden fließt als Input in ein Lastenheft ein und die Anforderungsliste ist ein Element des Pflichtenhefts. Wesentliche Unterschiede sind somit der Zeitpunkt und der Ersteller.

Anwendungsfall (Use Case)

Anwendungsfälle beschreiben das Verhalten eines Produkts oder einer Software aus Anwendersicht. Aus der Anforderung aus Anwendersicht ergibt sich normalerweise der Name des Anwendungsfalls, z. B. „CO₂-Konzentration erfassen“ oder „Raumklima auf Dashboard anzeigen“. Mit einem Anwendungsfall ist die Erwartung des Anwenders konkret und einfach beschrieben.

Anwendungsfälle haben eine lange Historie. Schon 1990 werden sie in der Softwareentwicklung, bei der Systemerstellung und auch in der Produktentwicklung verwendet. Durch einfache Modelle dokumentieren sie die Funktionalität eines bestehenden oder geplanten Systems. Diese können dann wiederum in konkrete Testfälle abgeleitet werden.

Systemkontext

Bei der Entwicklung eines neuen Systems ist es essenziell, den Systemkontext genauestens zu betrachten, denn er beschreibt die allumfassende Interaktion eines Systems mit seiner Umgebung. Die zu beachtenden Rahmenbedingungen werden festgelegt, indem man das System selbst, dessen Systemgrenze, sowie die relevante und irrelevante Systemumgebung definiert. Auch Gesetze, Normen und Richtlinien werden bei dieser Systembetrachtung berücksichtigt.

LE 3 – Stakeholder

Stakeholder können Personen, Gruppen und Organisationen sein, die von Produkten, Dienstleistungen und Aktivitäten eines Unternehmens entweder direkt oder indirekt betroffen sind. Jeder

Stakeholder kann ein eigenständiges Interesse an bestimmten Produkten, Dienstleistungen oder Aktivitäten haben und sollte daher bei der Anforderungsanalyse nicht vernachlässigt werden. Stakeholder müssen keine natürlichen Personen sein, die Definition gilt ebenfalls für juristische Personen. Der Begriff besteht aus den Wörtern „stake“, was so viel wie Anteil oder Anspruch bedeutet, und „holder“, was Besitzer oder Eigentümer bedeutet. Daher werden Stakeholder mitunter auch als Anspruchsgruppen bezeichnet, die ein berechtigtes Interesse an den Aktivitäten eines Unternehmens haben.



Typische Stakeholder

Endkunden

Die eigentlichen Endkunden, aber auch Kunden innerhalb der Wertschöpfungskette

Mitarbeiter

Die Mitarbeiter im Unternehmen, die direkt (z. B. Werker, die das Produkt montieren oder Softwareentwickler aber auch indirekt (z. B. Mitarbeiter in der Buchhaltung) durch das Produkt betroffen sind

Beispiele

- Gewerkschaften, Verbände, Verbraucherorganisationen, Vereine und Bürgerinitiativen
- Kapitalgeber wie Eigentümer, stille Teilhaber, Aktionäre oder Banken
- Wettbewerber, Patenteigentümer, Lizenzgeber
- Institutionen, Behörden und der Gesetzgeber

Stakeholder können die Erreichung von Unternehmenszielen maßgeblich beeinflussen. Daher sichert das **Stakeholder-Management** die kontinuierliche Auseinandersetzung eines Unternehmens mit seinen Stakeholders. Die **Stakeholder-Identifikation** ist der erste Schritt. Alle Personen und Organisationen, die direkt oder auch indirekt von Aktivitäten des Unternehmens betroffen sind oder ein konkretes Interesse an diesen Aktivitäten haben, werden bei der Identifikation erfasst. Danach werden durch die **Stakeholder-Analyse** die Ziele, Motive und Einstellungen der verschiedenen Stakeholder sowie die potenziellen Risiken durch die identifizierten Personen und Gruppen ermittelt. Die Analyseergebnisse bilden nun die Grundlage der **Stakeholder-Kommunikation**. Sie bezeichnet den regelmäßigen Austausch des Unternehmens mit den Stakeholdern, um geänderte Meinungen und daraus abgeleitet neue Ziele und Prioritäten zu identifizieren. Durch die Stakeholder-Kommunikation erhält man frühzeitig Feedback und Meinungen, die unter anderem Konflikte proaktiv vermeiden können.

LE 4 – Akzeptanzkriterien

Alle Stakeholder formulieren ihre Erwartungen an Produkte und Dienstleistungen, explizit oder implizit, als Anforderungen. Im Idealfall sollten die Anforderungen korrekt, eindeutig, vollständig, verständlich und widerspruchsfrei sein. Doch das ist weit von der Realität entfernt. Die Produktentwicklung steckt voller Konflikte, da die Anforderungen die genannten Kriterien nicht erfüllen. Aus diesem Grund können Akzeptanzkriterien unnötige Konflikte vermeiden. Sie definieren Bedingungen, durch die eine Anforderung erfüllt und vom Stakeholder akzeptiert wird. Mit anderen Worten: Akzeptanzkriterien konkretisieren Anforderungen. Mit Akzeptanzkriterien wird eindeutig und objektiv bestimmt, ob eine Funktionalität so erfüllt wurde, wie es sich der Anwender vorgestellt hat.



Akzeptanzkriterien - Vorteile durch eindeutige und objektive Kriterien

- Erwartungen des Anwenders rücken in den Fokus.
- Das Verständnis aller Beteiligten in Bezug auf Anforderungen bzw. Anwendungsfälle wird erhöht.
- Sie definieren die Aufgaben, die zur Erfüllung der Anwendungsfälle bearbeitet werden müssen.
- Die definierten und abgestimmten Kriterien sind die Basis für die Akzeptanztests.
- Sie fördern die Kommunikation zwischen allen Beteiligten.

Lernzielkontrolle TAG 6

1. Diskutieren Sie die vier VUCA-Elemente und begründen Sie, weshalb die Erfassung der unterschiedlichsten Anforderungen von Auftraggebern so komplex ist.
2. Erstellen Sie in Partnerarbeit ein Schaubild, das die Zusammenhänge zwischen Requirements Engineering, Stakeholdern und Akzeptanzkriterien anschaulich darstellt.

TAG 7 - Eine Projektplanung durchführen

Nachdem die Anforderungsanalyse abgeschlossen ist, starten Sie im Team die Umsetzung. Für das Projektmanagement wird eine agile Methode ausgewählt. Sie sollen im Team mittels DevOps sowohl die Soft- als auch die Hardwareentwicklung durchführen.



DevOps

DevOps ist ein Kunstwort aus den beiden Wörtern „development“ (Entwicklung) und „operations“ (Betrieb). Es handelt sich um eine Methodik der agilen Softwareentwicklung, kommt aber zwischenzeitlich auch außerhalb der Anwendungsentwicklung zum Einsatz.

Der DevOps-Ansatz bietet Möglichkeiten, um agile Entwicklungen durch Prozessautomatisierung weiter zu verbessern und zu beschleunigen. Durch DevOps wird unter anderem die Softwarebereitstellung schneller und zuverlässiger gemacht, indem die Zusammenarbeit zwischen Entwicklung und Betrieb gefördert wird. Das DevOps-Vorgehen, das auch oft als eine „Kultur“ bezeichnet wird, schafft es außerdem, das Gesamtsystem dauerhaft zu optimieren, da es Menschen, Prozesse und Technologien enger verbindet.

LE 1 - DevOps-Ziele

DevOps soll die Zusammenarbeit zwischen Stakeholdern und dem Projektteam von der Planung bis zur Bereitstellung des Produkts verbessern. Die Zusammenführung der Entwicklung mit dem Betrieb hat gleich mehrere Vorteile. Mehr Transparenz, präzisere Anforderungen, bessere Kommunikation und kürzere Markteinführungszeiten können damit erreicht werden. Konkret können die folgenden Ziele genannt werden:

- Häufigkeit der Bereitstellung von Prototyp-Versionen erhöhen,
- Fehlerrate neuer Versionen verringern,
- Vorlaufzeit zwischen den einzelnen Korrekturen verkürzen,
- schnellere Markteinführung des Endprodukts erreichen.

LE 2 - DevOps-Konzept und DevOps-Ansatz

Das DevOps-Konzept folgt mehreren Prinzipien, die sich stetig verändern. Unterschiedliche Softwareunternehmen entwickeln eigene Konzeptvarianten, jedoch folgen alle Prinzipien einem ganzheitlichen DevOps-Ansatz, den Unternehmen jeder Art umsetzen können. Zu diesen Prinzipien gehören:

- Lösungen entwickeln und in produktionsähnlichen Umgebungen testen,
- wiederholbar und sicher implementieren,
- operative Qualität überwachen und validieren,
- Feedbackschleifen erweitern.

LE 3 - DevOps-Kultur

Die Kultur eines jeden Unternehmens spielt eine wichtige Rolle. Speziell im Bereich der Softwareentwicklung gibt es die unterschiedlichen Sichtweisen der Entwickler und der Betreiber, was zu Spannungen führt, da beide Gruppen unterschiedliche Ziele haben. Auf der einen Seite möchten die Entwickler mehr Features in die Software integrieren und auf der anderen Seite möchte das Operations-Team ein stabiles System. DevOps kann aus diesem Grund nur dann erfolgreich sein, wenn beide Teams miteinander arbeiten.

In diesem Zusammenhang wird oftmals eine Verbindung zum sogenannten CALMS-Modell hergestellt. Es steht für Kultur, Automatisierung, Schlankheit, Messung und Austausch. Es kann dafür verwendet werden, das DevOps-Konzept zu verstehen und erfolgreich anzuwenden.

CALMS-Modell

C-Culture (Kultur)

Die wichtigsten Aspekte der Kultur sind die Zusammenarbeit und die Kundenorientierung. Jeder Beteiligte sollte verstehen, dass die Technologie bei den Kunden einen Mehrwert generieren soll. Wird von ihnen kein Wert im Produkt erkannt, ist die Erfolgchance gleich null. Die Technologie ist diesem Ziel untergeordnet. Eine erfolgreiche DevOps-Kultur ist extrem kollaborativ und funktionsübergreifend. Um den Kunden ein Produkt zu liefern, das ihnen einen Mehrwert liefert, arbeiten Mitarbeiter aus mehreren Teams und mit unterschiedlichen Fähigkeiten zusammen.

A - Automation (Automatisierung)

Routinetätigkeiten sind für die meisten Menschen unangenehm und langweilig. Dies führt häufig zu Ineffizienz. Computer oder intelligente Maschinen können diese Tätigkeiten automatisieren und wesentlich effizienter abarbeiten.

L - Lean (schlank)

Schlank bezieht sich nicht nur auf die schlanke Fertigung (Lean Production), sondern bezieht sich auch auf DevOps-Teams. Diese müssen flexibel und schlagkräftig agieren können. Gibt es Aktivitäten mit belanglosen Auswirkungen auf ein Produkt, welche dem Kunden keinen Mehrwert bieten, sorgen Lean-Teams dafür, dass diese Aktivitäten vermieden werden. Ein weiterer Punkt der Schlankheit ist die konsequente und kontinuierliche Verbesserung.

M - Measurement (Messung)

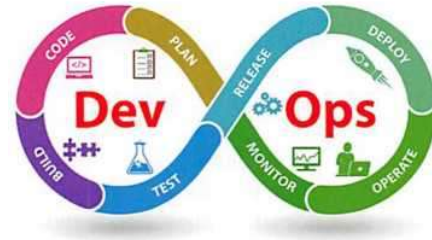
Daten sind essenziell für DevOps-Teams. So gut wie jeder Aspekt in allen DevOps-Phasen wird von Messdaten zum Fortschritt beeinflusst. Die Einstellung des Teams zur Interpretation der Daten ist ebenfalls entscheidend. Eine positive Fehlerkultur beschleunigt ebenfalls den Prozess.

S - Sharing (Austausch)

Der Grund für die Gründung von DevOps war der konstante Interessenkonflikt zwischen Betrieb und Entwicklung. Der Grund liegt darin, dass beide Bereiche ihre Anreize von verschiedenen Grundlagen erhalten. Der Betrieb wird meist daran gemessen, wie zuverlässig und verfügbar eine Anwendung genutzt werden kann. Die Entwickler hingegen versuchen ständig neue Funktionen in diese Anwendungen zu integrieren. Hier kommt DevOps ins Spiel. Durch stetigen Austausch soll dieser Konflikt eliminiert und eine Umgebung geschaffen werden, in der sich beide Teams zusammenschließen und gemeinsam zum Erfolg beitragen.

LE 4 - DevOps-Phasen

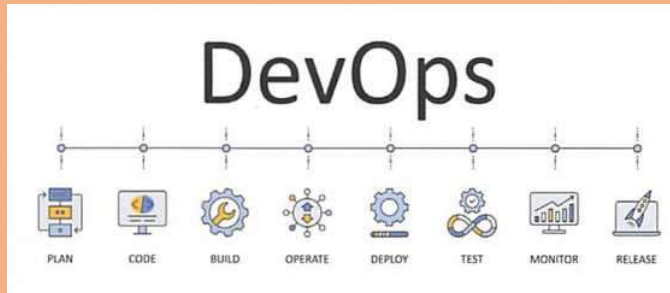
Die gesamte Softwareentwicklung wird in sequentielle Phasen eingeteilt. Es entsteht ein Workflow, der immer wieder durchlaufen wird. Ziel ist es, die verschiedenen Phasen des Workflows zu verkürzen und - wo möglich - zu automatisieren. Dabei kommen zahlreiche Tools zum Einsatz, die Grundsätze wie Automatisierung, Kollaboration und Integration zwischen Entwicklungs- und Betriebsteam unterstützen.



DevOps-Phasen

Planen (Plan)

In dieser Phase werden die geschäftlichen Anforderungen festgelegt. Tools wie Jira oder Git unterstützen dabei das Projektmanagement.



Codieren (Code)

Um präzise und effizient in der Softwareentwicklung arbeiten zu können, ist es wichtig, dass die Teams auf eine Versionskontrolle achten. Versionskontrollsysteme wie Git machen von allen Dateien Momentaufnahmen. Der Vorteil besteht darin, zu jeder Zeit und dauerhaft ältere Versionen wiederherstellen zu können.

Erstellung (Build)

In der dritten Phase gilt es, die Builds zu verwalten. Automatisierte Tools, z.B. Docker, unterstützen das Kompilieren und Packen von Codes für die anstehenden Produktionsfreigaben.

Testen (Test)

In dieser Phase wird durch kontinuierliches Testen, das sowohl automatisiert als auch manuell durchgeführt werden kann, die Qualität des Codes geprüft. Des Weiteren werden Benutzerakzeptanz-, Sicherheits-, Leistungs- und Lasttests durchgeführt.

Freigabe (Release)

Freigabe eines Software-Releases

Bereitstellung (Deploy)

Erreicht ein Build die Bereitstellungsphase, ist die Software so weit, in die Produktion übertragen werden zu können. Ist nur eine geringfügige Änderung im Code notwendig, verwendet man eine automatisierte Bereitstellungsmethode. Wenn eine umfassende Überarbeitung notwendig war, wird der Build vorerst in einer produktionsähnlichen Umgebung getestet, um das Verhalten des neuen Codes zu überwachen.

Betrieb (Operate)

In dieser Phase geht es um das permanente Management der Software im laufenden Betrieb.

Überwachen (Monitor)

In dieser Phase werden Informationen über Probleme in der Produktion erkannt und zurückgemeldet.

DevOps-Praktiken

Kontinuierliche Integration (Continuous Integration - CI)

Hier werden Konfigurationsmanagement-Tools eingesetzt und mit Tools der Entwicklung und dem Testen kombiniert, um bei Codeproblemen sehr schnell Rückmeldungen zu erhalten.

Kontinuierliche Bereitstellung (Continuous Delivery - CD)

Dieser Ansatz automatisiert die Bereitstellung von Codeänderungen nach dem Testen in einer Vorproduktions- oder Staging-Umgebung. Danach kann ein Mitarbeiter über die finale Freigabe in die Produktionsumgebung entscheiden.

LE 5 - Versionsverwaltung mit Git

Bei der gemeinsamen Entwicklung von Softwareprojekten ist die Verwaltung von unterschiedlichen Versionsständen eine sehr große Herausforderung. Der Open-Source-Sektor ist für hunderte bis tausende Freiwillige offen. Man kann sich an der Instandhaltung, Optimierung, Weiterentwicklung oder der Modifizierung eines Programms beteiligen. Wenn eine solche Menge an Menschen an einem Projekt arbeitet, entsteht eine hohe Anzahl an Änderungen. Daher ist es notwendig, diese aufzuzeichnen und zu protokollieren. Eine gängige Lösung zur Versionsverwaltung ist das lizenzfreie Tool „Git“. Dieses Tool besitzt zwei Vorteile, die zu dessen Beliebtheit beitragen: Es ist kostenlos nutzbar und sehr einfach zu erlernen.

Git ist ein Versionsverwaltungssystem, das 2005 von Linux Thorvalds (Linux) entwickelt und unter der freien GNU-GPLv2-Lizenz veröffentlicht wurde. Eine charakteristische Besonderheit von Git besteht darin, dass ein zentrales Repository (ein digitales Verzeichnis bzw. Archiv) eines Projekts besteht und jeder beteiligte Nutzer eine lokale Arbeitskopie dieses Verzeichnisses herunterladen kann. Code-Änderungen kann man lokal bearbeiten, mit anderen Projektteilnehmern austauschen und in das zentrale Repository aufnehmen.



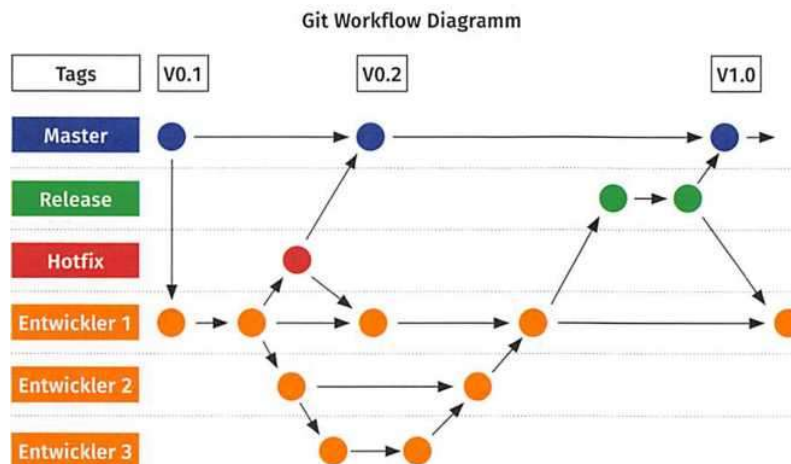
In der folgenden Übersicht werden die wichtigsten Git-Befehle aufgelistet. Im zugehörigen Arbeitsbuch behandeln konkrete Arbeitsaufträge die Installation von Git und den Umgang mit der Versionsverwaltung.

Die wesentlichen Git-Befehle	
git init	Git Repository anlegen Mit dem init-Befehl wird ein Git Repository lokal erzeugt.
git clone	Arbeitskopie erstellen Mit dem clone-Befehl kann eine Arbeitskopie eines bestehenden Repositories erzeugt werden. <i>Beispiel:</i> git clone https://test.website/git-repository
git status	Status abfragen Mit dem Status-Befehl wird der aktuelle Status des Repositories angezeigt.

Die wesentlichen Git-Befehle	
git add	Neue Datei hinzufügen und „anmelden“ Um eine neue Datei zur Versionsverwaltung hinzuzufügen oder eine überarbeitete Datei für den nächsten Commit anzumelden, wendet man den Befehl „git add“ auf diese Datei an. Die Datei muss sich hierfür im Arbeitsverzeichnis befinden. <i>Beispiel:</i> git add Git-Test.txt
git commit	Angemeldete Datei bestätigen Änderungen, die für die Versionsverwaltung per add angemeldet wurden, müssen per commit bestätigt werden, damit sie in den HEAD aufgenommen werden. Der HEAD ist eine Art Index, der auf den letzten wirksam gewordenen commit in der aktuellen Git-Arbeitsumgebung (auch als Branch bezeichnet) verweist.
git commit --amend	Bestätigte Datei nochmals anpassen Sind bei bereits bestätigten (commit) Dateien weitere Anpassungen notwendig, können die angepassten Dateien nachträglich per git add bereitgestellt werden. Der anschließende git commit —amend ersetzt den letzten commit durch den neuen, verbesserten commit.
git reset --soft HEAD~1	Anmeldung zurücknehmen Möchte man den zuletzt generierten commit wieder zurücknehmen, gelingt dies mit reset -soft HEAD~1. Durch diesen Befehl wird der zuletzt in den HEAD aufgenommene commit zurückgenommen. Die darin enthaltenen Dateien werden dabei wieder in den Status als „geplante Änderungen für den nächsten Commit“ zurückgesetzt.
git reset --hard HEAD~1	Angemeldete Datei komplett löschen Sollen die Arbeitsdaten komplett gelöscht werden, verwendet man anstelle des voranstehenden Kommandos den Befehl reset —hard HEAD~1.
git log	Anzeigen aller angemeldeten Dateien Der Befehl „git log“ listet die erzeugten commits in umgekehrter, chronologischer Reihenfolge auf. Es werden folgende Daten angezeigt: • SHA-1-Prüfsumme, • Autor (Name und Mailadresse), • Datum des jeweiligen commits, • individuelle Meldung zu den einzelnen Änderungen.
git push origin master	Übertragen aller angemeldeten Dateien in das Hauptverzeichnis Durch diesen Befehl überträgt Git automatisch alle erstellten commits, die bisher in der Arbeitskopie waren, in das Hauptverzeichnis, das auch die Bezeichnung „master“ hat. Ersetzen Sie diesen Namen in dem aufgeführten Code durch den eines anderen Branches (Projektzweigs), werden die Dateien direkt in den entsprechenden Branch gesendet.
git pull	Datei aus dem Hauptverzeichnis in das lokale Repository herunterladen Der Befehl „git pull“ wird verwendet, um Inhalte aus dem Hauptverzeichnis herunterzuladen und um das lokale Repository zu aktualisieren.
git tag	Anzeigen von Tags (Markierung) im Repository Git verfügt über eine Tagging-Funktion, mit der sich ausgewählte Punkte in der Historie eines Repositories markieren lassen. Sobald Tags für Ihr Repository existieren, können diese mit git tag angezeigt werden.
git branch branch_neu	Neuen Branch erstellen Um einen neuen Branch zu erstellen, benötigt man nur die Anweisung git branch und die gewünschte Bezeichnung (branch_neu) für den neuen Zweig.

Die wesentlichen Git-Befehle	
git checkout branch_neu	In Branch wechseln Anschließend können Sie jederzeit mit der Anweisung „git checkout“ in diesen Branch wechseln.
git Checkout master git merge branch_neu	Branches zusammenführen Möchte man Branches zusammenführen, gelingt dies mit dem Kommando „git merge“. Man wechselt zunächst via checkout in das Verzeichnis, das einen anderen Zweig aufnehmen soll und führt dort den genannten Befehl inklusive des Namens des aufzunehmenden Branchs aus. Die Arbeitsversion branch_neu lässt sich somit in das Haupt-Repository „master“ mergen.
git branch -d branch_neu	Branch löschen Hat man Arbeitszweige zusammengeführt und benötigt einen bestimmten Branch nicht mehr, kann dieser einfach mit git branch -d gelöscht werden.

Ein weiteres Element zum besseren Verständnis für die Versionsverwaltung mit Git ist der Workflow von der ersten Entwicklung über das erste Release bis hin zur kontinuierlichen Weiterentwicklung. Die nachfolgende Grafik beschreibt anhand eines zeitlichen Ablaufs das Zusammenspiel zwischen unterschiedlichen Softwareentwicklern und dem eigentlichen Produkt.



Lernzielkontrolle TAG 7

1. Beginnen Sie mit einer Pro- und Kontra-Diskussion mit zwei Gruppen, die folgende Positionen vertreten:
Standpunkt 1: Das klassische Projektmanagement ist den agilen Projektmanagementmethoden weit überlegen.
Standpunkt 2: Nur durch den Einsatz agiler Projektmanagementmethoden kann mit der heutigen Dynamik umgegangen werden.
2. Beschreiben Sie die einzelnen DevOps-Phasen mit eigenen Worten.
3. Informieren Sie sich im Internet über Continuous Integration und Continuous Delivery und erstellen Sie eine kurze Zusammenfassung.

TAG 8 - Ein cyber-physisches System in Betrieb nehmen

Sie stehen nun mit Ihrem Auszubildenden-Team vor der Umsetzung der CPS-Erweiterung. Zunächst muss das bestehende CPS, welches nur die Temperatur und die Luftfeuchtigkeit erfasst, als Versuchsaufbau nachgebaut werden. Darauf aufbauend dient der Versuchsaufbau

LE 1 - Sie sollen einen Prototyp aufbauen

Unter einem Prototyp versteht man in der Informationstechnologie ein voll funktionsfähiges, vereinfachtes Modell eines geplanten Produktes, eines Bauteils oder einer Software. Der Prozess zur Erstellung von Prototypen wird als Prototypenentwicklung bzw. Prototyping bezeichnet. Das Ziel beim Prototyping liegt in der Funktionsanalyse und der Gewinnung von frühzeitigem Feedback, ob sich der gewählte Lösungsansatz für das geforderte Produkt eignet.

Prototyping wird in zahlreichen **Bereichen** eingesetzt, z.B.:

- Technik-Prototyping: dient zur Vorbereitung einer Serienproduktion.
- Service-Prototyping: bezeichnet eine Methode des Dienstleistungsengineerings.
- Änderungswünsche und Probleme können während der Softwareentwicklung durch die Verwendung eines Software-Prototyps meist frühzeitig erkannt und billiger behoben werden.

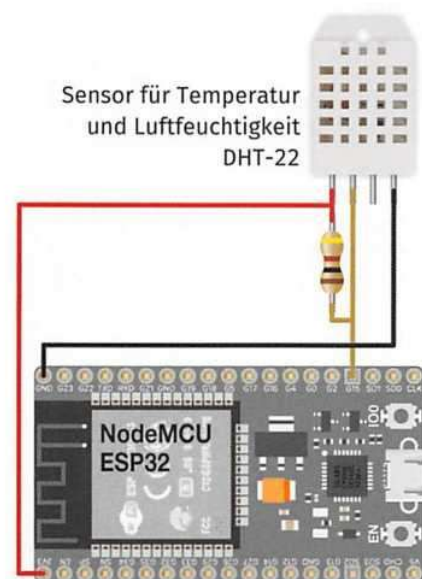
Während der Entwicklung der Software kann man unterschiedliche **Arten des Prototypings** beschreiben:

- Exploratives Prototyping wird verwendet, um nachzuweisen, dass eine Idee oder Spezifikation belastbar ist. Dadurch werden Anforderungen ermittelt und Lösungsoptionen identifiziert, welche in die Anforderungsliste aufgenommen werden können. Der Fokus von diesem Ansatz liegt auf der Funktionalität des Systems.
- Der evolutionäre Prototyp ist auf die Anwenderakzeptanz fokussiert und zielt auf das Identifizieren fehlender Funktionen.
- Der experimentelle Prototyp sucht nach neuen Möglichkeiten, Funktionen zu realisieren.

Die Entwicklung von Hardware-Prototypen kann in aufeinander aufbauenden Phasen vorstattengehen. Es gibt im Allgemeinen vier **Entwicklungsschritte** mit den entsprechenden Prototypen bei der Hardwareentwicklung:

1. Reine Versuchsaufbauten zur Realisierung der geforderten Funktionen.
2. Vorführmodelle, die als Attrappe nur das Design eines Produktes demonstrieren sollen.
3. Ein voll funktionsfähiger Prototyp, der experimentell aufgebaut ist, die geforderten Funktionen demonstrieren soll und schon in ein Design-Modell integriert wurde.
4. Ein Nullserien-Prototyp, der zu den letzten Erprobungszwecken kurz vor der Serienfertigung zum Einsatz kommt.

Der Ausbildungsverantwortliche in der Entwicklungsabteilung der JIKU IT-Solutions übergibt dem Auszubildenden-Team einen Experimentierkasten auf Basis des Mikrocontrollers „Arduino“. Das Set beinhaltet neben dem Mikrocontrollerboard „Arduino“ einen zusätzlichen Mikrocontroller „ESP32“, zahlreiche Verbindungskabel, ein Experimentierboard (auch Breadboard genannt) sowie verschiedene Sensoren und Aktoren. Mit diesem Experimentierset kann sowohl das bestehende CPS (Überwachung der Temperatur und Luftfeuchtigkeit) als auch das zu erweiternde CPS (Ergänzung mit einem CO₂-Sensor) experimentell aufgebaut werden. Es



empfiehlt sich, den experimentellen Aufbau genau zu dokumentieren. Dazu eignet sich Software zur Erstellung von elektronischen Schaltungen wie die freie Software „Fritzing“.

LE 2 - Software des erweiterten cyber-physischen Systems programmieren

Zur Programmierung eines „Arduino“- oder „ESP32“-Mikrocontrollers kann die Arduino-IDE eingesetzt werden. Die Arduino-IDE basiert auf der Sprache C++. Die Programme werden in dieser integrierten Entwicklungsumgebung als „Sketch“ bezeichnet. Wenn ein Sketch fertig programmiert ist, kann er auf den Speicher des Mikrocontrollerboards hochgeladen werden. Zuvor wird das Programm geprüft und kompiliert. Die Abbildung auf S. 134 stellt die drei Bereiche dar, die die allgemeine Grundstruktur eines Sketches ergeben und im Folgenden beschrieben werden.

Grundstruktur eines “Arduino”-Sketch

Bereich 1 für Bibliotheken, Variablen, Konstanten und zur Initialisierung von Komponenten

Im Bereich 1 werden die Elemente des Programms benannt, die global verfügbar sind. Global verfügbar bedeutet, dass diese Werte in allen folgenden Methoden und Funktionen zur Verfügung stehen.

Wesentliche Elemente, die in diesem Bereich aufgeführt werden, sind:

- Programmbibliotheken, die geladen werden sollen - Bibliotheken erweitern den Funktionsumfang der „Arduino“-IDE um weitere Befehle und Funktionen, z. B. von eingebundenen Sensoren und Aktoren,
- Deklaration von Variablen,
- Definition von Konstanten,
- Definition und Initialisierung von unterschiedlichen Sensoren/Aktoren.

Dieser Teil ist nicht für jeden Sketch zwingend erforderlich.

Bereich 2 für das Setup - Aufruf der Methode „void setup()“

In Bereich 2 werden Befehle und Anweisungen aufgerufen, die zu Beginn der Ausführung einmal ausgeführt werden. Wenn sich im Setup-Bereich keine Einträge befinden, so ist der Setup-Bereich dennoch erforderlich. Im Setup-Bereich wird u.a. festgelegt, an welchen Pins eines Mikrocontrollerboards eine Komponente angeschlossen wird und ob es sich dabei um einen Ein- oder Ausgang handelt.

Bereich 3 für die Ablaufsteuerung - Aufruf der Methode „void loop()“

In Bereich 3 werden die programmierten Befehle, Anweisungen und Funktionen in einem kontinuierlichen Kreislauf wiederholt. Deswegen wird dieser Bestandteil auch als Hauptelement eines Sketches bezeichnet. Der Loop-Teil bearbeitet einen Sketch vollständig und startet danach automatisch wieder am Anfang des Bereichs.

Ausgabewerte des Programms können zur Kontrolle über den seriellen Monitor angezeigt werden. Dies ermöglicht die direkte Anzeige und Überprüfung der erfassten Werte, ermöglicht aber auch die Ausgabe von Fehlermeldungen beim Debugging, z.B. bei der Überprüfung, ob ein Sensor ordnungsgemäß funktioniert oder ob angeschlossene Komponenten vom Mikrocontroller korrekt erkannt wurden.

Um wie bei allen Programmen eine gute und übersichtliche Struktur aufzubauen, können Kommentare und Hinweise eingefügt werden. Durch // können direkt dahinter Erklärungen zum Programmcode eingegeben werden und innerhalb der Zeichen /* und */ kann ein größerer

Bereich für Informationen genutzt werden. Die Erklärungen in der „Arduino“-Entwicklungsumgebung haben keinen Einfluss auf den Ablauf des Sketches.

Beim Programmieren von Mikrocontrollern kann es zu vielen Fehlern kommen. Die zwei häufigsten Fehler, die während dem Arbeiten mit der „Arduino“-Software auftreten, sind die folgenden:



```

KAE_DHT22_Test [Arduino 1.8.13]
Datei Bearbeiten Sketch Werkzeuge Hilfe

KAE_DHT22_Test

/* Tests Sensor DHT22
 * Ausgeben: Serialer Monitor
 */

//-----
// Bibliotheken einbinden | Variablen deklarieren | Konstanten definieren | Initialisierung
#include "DHT.h" // DHT Bibliothek einbinden

#define DHTPIN 15 // DHT22 Sensor Signal auf ESP32 Eingang 15
#define DHTTYPE DHT22 // Definition des Sensortyps: DHT 22

DHT dht(DHTPIN, DHTTYPE); // DHT22 Sensor initialisieren

//----- S E T U P -----
void setup() {
  Serial.begin(115200); // Baudrate, für ESP32 115200
  Serial.println("DHT22 Test!");
  dht.begin();
}

//----- L O O P -----
void loop() {
  delay(2000);

  float h = dht.readHumidity();
  float t = dht.readTemperature();

  if (isnan(h) || isnan(t)) { // isnan Funktion --> variable IS Not A Number
    Serial.println("DHT Sensor konnte nicht korrekt gelesen werden!");
  }

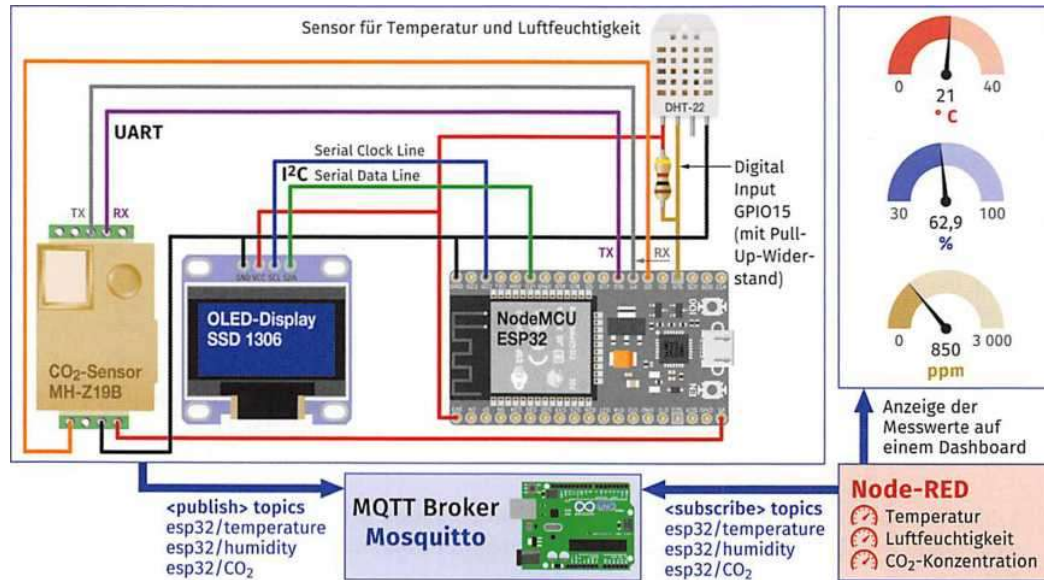
  Serial.print("Luftfeuchtigkeit: ");
  Serial.print(h);
  Serial.println(" %");
  Serial.print("Temperatur: ");
  Serial.print(t);
  Serial.println(" °C");
  Serial.println();
}
//-----
  
```

Häufige Fehlerquellen bei der Programmierung von Mikrocontrollern

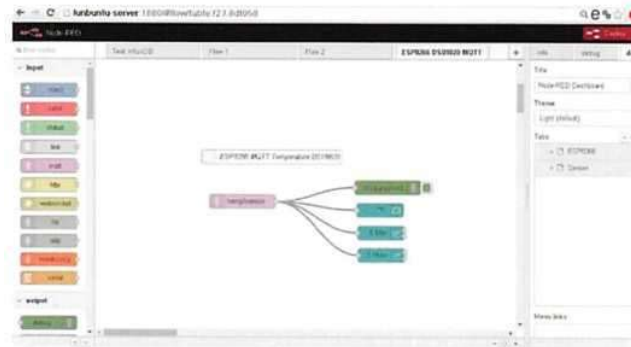
- Ein falsches Board wurde ausgewählt oder es wurde nicht richtig installiert. Ist das der Fall, erscheint beim Hochladen des Sketches eine Fehlermeldung im unteren Bereich der Software. Zur Fehlerbehebung muss in der Board-Verwaltung der integrierten Entwicklungsumgebung (IDE) das korrekte Board aktiviert werden.
- Es gibt einen Syntaxfehler im Sketch. Dies ist der Fall, wenn ein Wort, eine Variable oder ein Befehl falsch geschrieben wurde oder eine notwendige Klammer oder ein Semikolon fehlt.

LE 3 - MQTT-Broker und Client verbinden

Um das MQTT-Protokoll einzusetzen, muss man einen Broker verwenden, der mit den MQTT-Clients kommuniziert. Ist im bestehenden Netzwerk bislang kein Broker eingerichtet, kann mithilfe eines „Raspberry Pi“ ein MQTT-Broker installiert und verfügbar gemacht werden. Dafür eignet sich der Open-Source- Broker „Mosquitto“. Der Broker empfängt Nachrichten (Topics) von Clients und leitet den Inhalt des abonnierten Topics an interessierte Empfänger (Subscriber) weiter. Ohne einen MQTT-Server als Broker können folglich keine Nachrichten von Clients empfangen und an die jeweiligen Empfänger weitergeleitet werden.



Neben einem MQTT-Broker wird außerdem ein grafisches Entwicklungswerkzeug benötigt, das sowohl Hardware und Schnittstellen als auch Services miteinander verbinden kann. Auch hier eignet sich ein Open-Source-Werkzeug für die Umsetzung.



Die Open-Source-Software „Node-RED“ ermöglicht es, mit einem einfachen Baukastenprinzip einzelne Funktionen und Aktionen miteinander zu verbinden. Dafür nutzt die Software sogenannte Nodes (Knoten). Diese sind sehr einfach miteinander zu verbinden. Das Ergebnis sind die sogenannten Flows, die verschiedene Eingabe-, Verarbeitungs- und Ausgaben-Nodes verbinden. Damit lassen sich IoT-Geräte kontrollieren und steuern. Jeder Node hat eine definierte Aufgabe. Die Knotenpunkte können Daten erhalten, verarbeiten und an den nächsten Knoten weitergeben. Damit lassen sich einfache, aber auch komplexe Programmabläufe realisieren.

LE 4 - Die Funktionalität der CPS-Erweiterung prüfen und protokollieren

Die Dokumentation der Inbetriebnahme von Geräten, Maschinen oder Anlagen ist essenziell. Mit der Inbetriebnahme gehen die Pflichten der Betriebssicherheitsverordnung auf den Betreiber der Maschinen oder Anlagen über. Mit der Inbetriebnahme soll sichergestellt werden, dass eine störungsfreie Nutzung von allen Geräten und Anlagen möglich ist. Auch die rechtlichen Aspekte sind bei der Inbetriebnahme für die Betreiber zu beachten, z.B. beginnt mit der Inbetriebnahme die Haftungsübernahme. Die folgende Übersicht fasst die kritischen Inbetriebnahmen von Produkten der Elektro-, Telekommunikations- und Sicherheitstechnik zusammen.

Inbetriebnahmen, die nur von qualifizierten Fachleuten durchgeführt werden dürfen

Elektrotechnik

Die Produkt- und Anlagensicherheit schreibt vor, dass nur Elektrofachkräfte elektrotechnische Produkte und Anlagen in Betrieb setzen dürfen. Die Inbetriebnahme bezieht sich an erster Stelle auf die elektrische Betriebssicherheit. Es soll sichergestellt werden, dass die Anlage oder Maschine ordnungsgemäß und mangelfrei funktioniert und keine Gefahr während der Nutzung besteht. Die Ergebnisse müssen in einem Inbetriebnahmeprotokoll festgehalten werden.

Telekommunikationstechnik

Ebenso kritisch ist die Inbetriebnahme von Telekommunikationsprodukten. Um sich gegen fremden Zugriff zu schützen, ist es notwendig, neben den Daten des Netzbetreibers noch zusätzlich Nutzerdaten, Dienste und Verschlüsselungen einzugeben. Diese Einstellungen sind bei Telefonanlagen und Mobilfunknetzen eine unabdingbare Voraussetzung, um einen störungsfreien Betrieb zu garantieren.

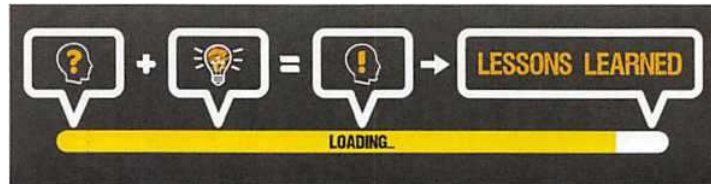
Sicherheitstechnik

Geht es um Produkte der Sicherheitstechnik, ist es unumgänglich, die Inbetriebnahme von einer Fachkraft durchführen zu lassen. Denn es gilt Fehlalarme zu vermeiden, das Persönlichkeitsrecht einzuhalten und die Anlagen vor fremdem Zugriff zu schützen.

In den meisten Fällen wird während der Inbetriebnahme einer Maschine oder Anlage ein **Inbetriebnahmeprotokoll** erstellt, dessen Ziel es ist, die Funktionstüchtigkeit der Anlage nachzuweisen. Wer das Inbetriebnahmeprotokoll erstellen muss, wie umfangreich es sein soll und welche Inhalte dokumentiert werden müssen, ist je nach Branche verschieden.

LE 5 - Im Review Projektergebnisse und -erkenntnisse erfassen

Ein Projekt ist mit der Inbetriebnahme des Produktes und der Übergabe an den Kunden noch nicht abgeschlossen. Es gilt, alle gemachten Erfahrungen, egal ob positiv oder negativ, systematisch zu erfassen und daraus Erkenntnisse zu ziehen, die zukünftige Projekte verbessern können.



Die sogenannte Lessons Learned ist eine beliebte Methode und ein wichtiger Bestandteil im Werkzeugkoffer der Projektmanagementmethoden. Sie wird auch als Projektretrospektive bezeichnet und ist ein bewährtes Vorgehen im Wissensmanagement. In den meisten Fällen wird dieses Werkzeug während des Projektabschlusses durchgeführt. Durch die gewonnenen Erkenntnisse können die Projektmanagementstandards in einem Unternehmen kontinuierlich weiterentwickelt werden.

Lessons Learned - Projektretrospektive als Werkzeug des Wissensmanagements

Ziele

Die Absicht von Lessons Learned ist, Erfahrungen und Erkenntnisse gezielt zu sammeln, zu analysieren und zu dokumentieren. Entstehen Probleme oder Herausforderungen bei bestehenden Projekten, sollen Mitarbeiterinnen und Mitarbeiter in der Lage sein, auf frühere Projekte zuzugreifen zu können und von den damaligen Erfahrungen zu profitieren. Damit sollen bereits gemachte Fehler vermieden werden und Bewährtes, das zum Erfolg des Projektes beiträgt, weiterhin eingesetzt werden.

Lessons Learned - Projektretrospektive als Werkzeug des Wissensmanagements

Inhalte

Der Inhalt von Lessons Learned besteht aus der Sicherung des Wissens, das durch die Arbeit an einem Projekt erworben wurde. Dazu zählen:

- positive und negative Erfahrungen,
- fachliche Erkenntnisse aus der Projektarbeit,
- Erkenntnisse aus der Durchführung von Prozessen (Wie lief der Prozess ab?),
- Transparenz von Erkenntnissen aus der Projektarbeit für andere Mitarbeiter im Unternehmen.

Ausgangssituationen

Eine Lessons-Learned-Besprechung kann durch folgende Punkte ausgelöst werden:

- Ein Projekt ist oder wird bald abgeschlossen.
- Inhaltlich sind fast alle Projektaktivitäten, bis auf ein paar wenige Restaufgaben erledigt.
- Die Stimmung im Projektteam wirkt euphorisch und erleichtert, da alle Ziele wie vereinbart erreicht werden konnten.
- Die Stimmung im Projektteam ist frustrierend oder sehr emotional, da einiges im Projekt schiefgelaufen ist.

Fragestellungen

- Was ist im Projekt gut gelaufen?
- Was ist im Projekt schlecht gelaufen?

Weiterführende Fragestellungen

- Was kann jede/-r Einzelne für sich aus dem Projekt lernen?
- Welche Ergebnisse sind für die gesamte Organisation/das Unternehmen wichtig?
- Was kann bei zukünftigen Projekten anders gemacht werden?
- Was soll bei zukünftigen Projekten beibehalten werden?

Dokumentation der Erkenntnisse und der Verbesserungsvorschläge

Nicht alle Verbesserungsvorschläge sind direkt umsetzbar, aber die Erfassung und die Dokumentation der Vorschläge bilden eine gute Basis für kontinuierliche Verbesserungen im Unternehmen.

Lernzielkontrolle TAG 8

1. Welche Aussagen sind korrekt?
 - a. Ein Vorführmodell kann zur Erprobung der Serienfertigung eingesetzt werden.
 - b. Der evolutionäre Prototyp entwickelt sich stetig, um die Akzeptanz der Anwender zu testen und fehlende Funktionen zu identifizieren.
 - c. Im Servicebereich kommen keine Prototypen zum Einsatz.
 - d. Mittels eines Experimentierkastens lassen sich Vorführmodelle erstellen.
2. Recherchieren Sie in Partner- oder Gruppenarbeit moderne Möglichkeiten, um schnell einen physischen Prototypen zu erstellen. Informieren Sie sich über die Schlagwörter „Mockup“, „Rapid Prototyping“ und „Additive Fertigung“ (3D-Druck).
3. Ergänzen Sie die folgenden Sätze.
 - a. Zusätzliche Befehle und Funktionen von Komponenten befinden sich in ...
 - b. Variable müssen in einem Programm festgelegt werden. Dies nennt man auch ...
 - c. Die englische Abkürzung für eine Entwicklungsumgebung lautet...
 - d. Für einen Sketch ist folgende Methode zwingend erforderlich:...
 - e. In der Methode „void loop()“ befindet sich die eigentliche ...
 - f. Werte von Sensoren können mit dem ... angezeigt werden.
 - g. Die Zeichen für einen einzelnen Kommentar im Programm sind ...
4. Beschreiben Sie in eigenen Worten die Funktion eines MQTT-Brokers.

5. Nennen Sie zu den drei Bereichen „Elektrotechnik“, „Telekommunikationstechnik“ und „Sicherheitstechnik“ Elemente, die Sie bei der Inbetriebnahme des eigenen cyber-physischen Systems überprüfen müssen.
6. Richtig oder falsch? Welches sind eindeutige Ziele eines Lessons-Learned-Workshops?
 - a. Austausch von positiven und negativen Erfahrungen aus der Projektarbeit
 - b. Gemeinsamer Abschluss nach erfolgreicher Übergabe eines Produkts an den Kunden
 - c. Vorbereitung auf ähnliche Herausforderungen in zukünftigen Projekten
 - d. Erfahrungen mit anderen Projektteams nicht zu teilen, um die Position des eigenen Projektteams zu stärken
 - e. Hinterfragen von bewährten Projektmanagementstandards, die bislang zum Projekterfolg beigetragen haben
 - f. Fehler der Vergangenheit nochmals zu wiederholen
7. Welche Gründe veranlassen das Projektmanagement dazu, mit dem Team eine Projektretrospektive durchzuführen?

TAG 9 - Ein cyber-physisches System optimieren

Der Aufbau des Prototyps, die Programmierung des Mikrocontrollers und die Vernetzung des CPS-Um- Weltsensors (Temperatur, Luftfeuchtigkeit, CO₂-Konzentration) mit einem MQTT-Broker waren erfolgreich. Die Ausbildungsverantwortlichen der JIKU IT-Solutions und die Entwicklungsabteilung sind vom Ergebnis begeistert. Jedoch haben Sie innerhalb des Auszubildenden-Teams selbst ein paar Punkte identifiziert, die Sie weiter optimieren möchten. Das Team möchte das CPS in Bezug auf Betriebs-, Daten- und Ausfallsicherheit verbessern.

LE 1 - Bestehende Gefahren für die Betriebs- und Datensicherheit durch den Einsatz des cyber-physischen Systems erkennen

Da die Informationstechnologie und die Operation Technology (OT) sich immer stärker annähern, müssen sowohl die allgemeine Automatisierungstechnik in der Fertigung als auch zahlreiche industrielle Anwendungen auf die Bedrohungen der Cybersicherheit vorbereitet werden. Das Ausmaß der potenziellen Bedrohungen einzuschätzen ist sehr komplex, da sich die Bedrohungslagen sowohl in der Informationstechnologie als auch in der Operation Technology ständig verändern. Im Vergleich von industriellen Anwendungen und Systemen mit Anwendungen aus dem kommerziellen Bereich müssen zahlreiche Szenarien unterschieden werden. Eine Sicherheitslücke in einem Industrie- oder Infrastruktursystem kann viel mehr anrichten als nur einen finanziellen Verlust, da auch die physische Komponente der Sicherheitsverletzung berücksichtigt werden muss. Betrachtet man beispielsweise die Störung einer industriellen Anlage oder den Ausfall eines Infrastruktursystems, z.B. ein Kraftwerk oder ein Wasserversorgungssystem, wird die Tragweite erkennbar. Zahlreiche Menschen könnten dadurch verletzt und getötet oder ein ganzes Land bedroht werden.



In einer sich technisch ständig entwickelnden Welt sind immer mehr Anwendungen, Maschinen, Anlagen und cyber-physische Systeme einer immer größeren Anzahl von potenziellen Bedrohungen ausgesetzt. Die folgenden zehn Punkte ermöglichen einen ersten Ansatz zur Betriebs- und Datensicherheit von Informationstechnologie und Operation Technology im Unternehmen.

Vorgehensweise zur Betriebs- und Datensicherheit von Informationstechnologie und Operation

1. Eine Aufstellung aller digital zu vernetzenden Bereiche eines Unternehmens erstellen
2. Prozesse und Unternehmenswerte danach bewerten, wie kritisch sie für das Unternehmen und die Geschäftsprozesse sind
3. Konkrete und potenzielle Ausfall- und Störungrisiken für jeden Prozess und jeden Unternehmensbereich identifizieren
4. Das bestehende IT-System mit Blick auf das Gefährdungspotenzial und die möglichen Beeinträchtigungen bei Störungen in Kategorien einstufen
5. Die Komplexität bestehender IT-Systeme wo möglich reduzieren, wenn möglich standardisierte Infrastrukturkomponenten einsetzen oder professionelle, vertraglich geregelte Dienste nutzen
6. Mobile Mitarbeiter und deren Smartphones, Tablets oder Homeoffice in ein Mobile-Device- Management einbinden
7. Privates und Geschäftliches auf allen Geräten trennen, die bei den Mitarbeitern zum Einsatz kommen
8. Klare, auf Rollen basierte Zugriffsberechtigungen und Service-Level für alle Mitarbeiter und Geräte einrichten und laufend überwachen
9. Mit professionellen IT-Sicherheitsdienstleistern Zusammenarbeiten und ein Frühwarnsystem einrichten; evtl. als Security as a Service
10. Bei allen Mitarbeitern für ein hohes Bewusstsein für Betriebs- und Datensicherheit sorgen:
 - Verschlüsselung von Daten und Verbindungen
 - Aktualisierung von Betriebs- und Sicherheitssystemen
 - Authentifizierung der Benutzer

In der digitalen Welt müssen Werte und Zugänge genauso geschützt werden wie in der analogen!

LE 2 - CPS-Systemausfälle mittels FMEA minimieren

Unternehmen erfassen und beschreiben ihre Wertschöpfungs- und Geschäftsprozesse und verbessern sie kontinuierlich. Ebenso müssen Produkte in Bezug auf Funktionsfähigkeit und Ausfallsicherheit stetig optimiert werden. Ein cyber-physisches System ist zum einen ein Produkt, aber auch Bestandteil eines Prozesses, der entsprechend beschrieben und optimiert werden kann.

In Beispiel der Raumüberwachung ist das cyber-physische System zum einen eine vernetzte



Prozessablauf einer FMEA

- (1) Vorbereitung der FMEA
- (2) FMEA-Team bilden
- (3) Strukturanalyse
- (4) Funktionsanalyse
- (5) Fehleranalyse
- (6) Risikobewertung
- (7) Optimierung

Sensoreinheit, aber auch wesentliches Element im Prozess zur Optimierung des Raumklimas. Die Sensoren erfassen die Temperatur, die Luftfeuchtigkeit und die CO₂-Konzentration im Raum, und auf Basis der erfassten Daten können Heizung, Klimaanlage und Lüftungen aktiviert bzw. deaktiviert werden.

Um Produkte oder Prozesse zu optimieren, gibt es zahlreiche Ansätze. Im industriellen Umfeld ist die FMEA ein wichtiges Werkzeug des Qualitätsmanagements. FMEA steht für Fehler-Möglichkeiten- und Einfluss-Analyse (im Englischen: Failure Mode and Effect Analysis). Mithilfe der FMEA können

systematisch Fehler und deren Ursachen identifiziert werden. Die Auswirkungen der Fehler kann man quantitativ bewerten und entsprechend Verbesserungen planen und umsetzen. Der Ablauf einer FMEA wird im Folgenden genau beschrieben.

1. Vorbereitung der FMEA

Eine FMEA wird komplett auf einem FMEA-Formblatt dokumentiert. Typischerweise ist dies Aufgabe der Projektleitung bzw. des Product Owners.

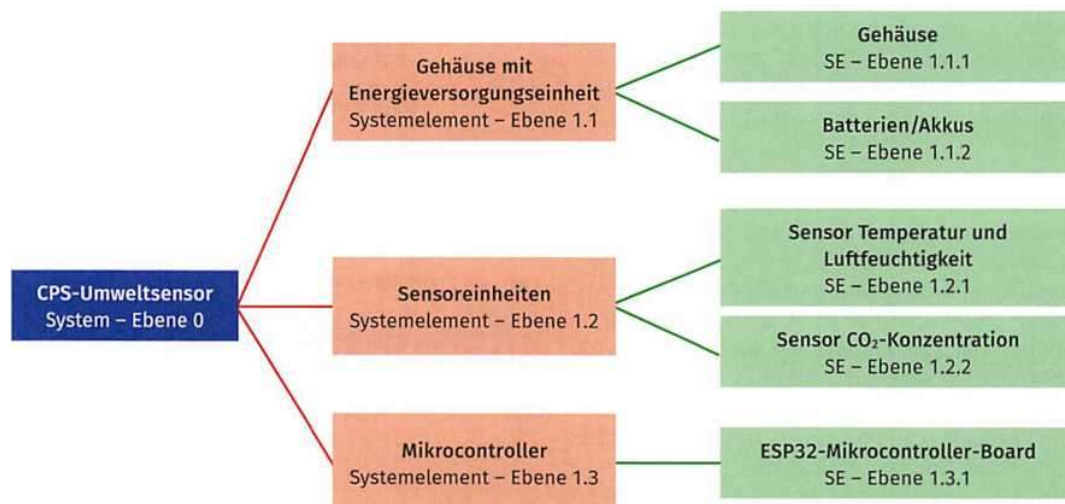
2. Bildung eines FMEA-Teams

Bei einer FMEA wird ein Team zusammengestellt, das unterschiedliches Expertenwissen hat. Idealerweise setzt sich das Team auch aus den verschiedenen Unternehmensbereichen zusammen. Dies sind beispielsweise Mitarbeiter aus Entwicklung, Konstruktion oder Produktion, aber auch Vertrieb, Einkauf oder Qualitätssicherung. Ein Team kann zwischen fünf bis maximal acht Mitglieder haben. Die Teammitglieder starten dann mit der Beschaffung aller erforderlichen Unterlagen:

- Lasten-/Pflichtenheft,
- technische Zeichnungen,
- Versuchsberichte,
- Qualitätsvorschriften,
- Fehlerlisten und Reklamationsstatistiken vergleichbarer Produkte,
- Gesetzestexte, Verordnungen, Sicherheitsvorschriften,
- Montage-/Prüfpläne.

3. Strukturanalyse

Jedes System (z.B. ein Produkt) besteht aus untergeordneten Systemelementen (SE). Die gesamte Systemstruktur gliedert sich vom Produkt, als oberste Ebene (Ebene 0) ausgehend, in die einzelnen Systemelemente auf. Die grafische Darstellung der Strukturstückliste als Baum beschreibt die eigentliche Strukturanalyse.



4. Funktionen und Funktionsstrukturen

Systemelemente erzeugen Funktionen durch ihren Aufbau. Für den CPS-Umweltsensor können für alle Systemelemente spezifische Funktionen definiert werden. So hat beispielsweise das Gehäuse die Funktion alle Bauteile zu fixieren und zu schützen. Die Batterien/Akkus versorgen das CPS mit Energie, die Sensoren erfassen die Messwerte und der Mikrocontroller ist für die Verarbeitung und Kommunikation verantwortlich. Wird schon bei der Strukturanalyse zur Darstellung ein Strukturbaum gewählt, sind die Funktionszusammenhänge leicht zu erkennen.

5. Fehleranalyse durchführen

Bei der Fehleranalyse wird die Funktionsanalyse Schritt für Schritt abgearbeitet, um mögliche Abweichungen von den spezifizierten Funktionen zu identifizieren. Mögliche Abweichungen von den spezifizierten Funktionen sind:

- Die Funktion ist nicht erfüllt.
- Die Funktion kann komplett ausfallen.
- Die Funktionsmerkmale liegen außerhalb der spezifizierten Toleranz.
- Die Funktion ist nicht unter allen spezifizierten Bedingungen vorhanden. Bedingungen können sein: Einsatzbereich, Temperaturbereich, Feuchtigkeit, Verschmutzungsgrad, WLAN-Qualität etc.

6. Risikobewertung vornehmen

Bei der Risikobewertung werden die Auswirkung der Fehlfunktion auf den Kunden beschrieben. Dies kann beispielsweise Unzufriedenheit sein, wenn eine Funktion nicht wie erwartet erfüllt wurde, oder eine Verletzungsgefahr, wenn eine Sicherheitsfunktion ausfällt. Jede Auswirkung hat folglich ein eigenständiges Risikopotenzial. Daher wird für jedes potenzielle Risiko eine sogenannte Risikoprioritätszahl (RPZ) ermittelt. Die folgenden Schritte beschreiben das Vorgehen zur Ermittlung der RPZ:

- **Bedeutung des Fehlers:** Die möglichen Fehlerfolgen werden in die entsprechende Spalte des FMEA- Formblatts eingetragen und mithilfe einer Bewertungstabelle auf einer Skala von 1 bis 10 bewertet. Die Bewertung wird in die Spalte B (Bedeutung des Fehlers) eingetragen. Jede Fehlerfolge kann durch unterschiedliche Fehlfunktionen verursacht werden.
- **Auftretenswahrscheinlichkeit:** Die potenziellen Fehlerursachen werden in die Spalte „Mögliche Fehlerursachen“ eingetragen. Es werden im Team Vermeidungsmaßnahmen diskutiert und erarbeitet, um das Auftreten der Fehlerursache zu verhindern. Die Bewertung auf einer Skala von 1 bis 10 wird in die Spalte A (Auftretenswahrscheinlichkeit) eingetragen.
- **Entdeckungswahrscheinlichkeit:** Wenn eine Fehlerursache auftritt, muss sie nicht zwangsläufig zu Auswirkungen beim Kunden führen. Im Unternehmen bestehen Möglichkeiten, die Fehlerursache oder den Fehler vor der Auslieferung des Produktes an den Kunden zu erkennen und zu beseitigen. Aber auch Sicherheitsfunktionen, die ins Produkt integriert werden, zählen zu den Entdeckungsmaßnahmen. Dies sind beispielsweise Kontrollleuchten oder Notfallabschaltungen. Die durchgeführten Entdeckungsmaßnahmen werden in die entsprechende Spalte eingetragen und die Wahrscheinlichkeit E (Entdeckungswahrscheinlichkeit), dass die Fehlerursache dadurch entdeckt wird, wird auf einer Skala von 1 (hoch) bis 10 (praktisch unmöglich) bewertet.
- **Risikoprioritätszahl:** Zur Ermittlung der Risikoprioritätszahl werden die drei Faktoren B, A und E miteinander multipliziert.

Risikoprioritätszahl (RPZ)

Die Risikoprioritätszahl ist ein Maß für ein Risiko, abhängig von der entsprechenden Fehlerursache. Sie wird wie folgt ermittelt:

$$RPZ = B \cdot A \cdot E$$

B: Bedeutung der Fehlerfolge

A: Auftretenswahrscheinlichkeit des Fehlers

E: Entdeckungswahrscheinlichkeit des Fehlers

Alle Faktoren haben einen Wert zwischen 1 und 10. Die RPZ kann somit einen Wert zwischen 1 und 1 000 haben. 1 bedeutet daher kein Risiko und 1000 sehr hohes Risiko. Ab einer RPZ zwischen 100 und 150 sollten Optimierungsmaßnahmen eingeleitet werden.

Optional können auch Maßnahmen in Betracht gezogen werden, wenn einer der drei Faktoren mit 8 oder mehr bewertet wurde.

Das Bewertungsschema für die drei Faktoren ist aus der Tabelle auf S. 144 ersichtlich.

7. Optimierung durchführen

Bei einer RPZ zwischen 100 und 150 empfiehlt es sich, Optimierungsmaßnahmen einzuleiten. Es ist ebenfalls ratsam, Maßnahmen in Betracht zu ziehen, wenn einer der drei Faktoren B, A oder E mit 8 oder mehr bewertet wurden. Zur Optimierung des Produkts sollte mit folgender Priorisierung vorgegangen werden:

- Überprüfung, ob eine Änderung möglich ist, um die Fehlerursache auszuschließen bzw. die Bedeutung der Fehlerfolge zu reduzieren,
- Zuverlässigkeit des Produkts erhöhen, um das Auftreten der Fehlerursache zu minimieren,
- • wirksamere Entdeckungsmaßnahmen in den Produktionsprozess oder in das Produkt selbst integrieren; dabei sollte zusätzliches Prüfen möglichst vermieden werden.

Alle zusätzlichen Maßnahmen zur Minimierung des Risikos werden beschrieben und als empfohlene Maßnahmen in das Formular eingetragen. Die mögliche Verbesserung wird in die Spalten A und E eingetragen (verbesserter Zustand). Für die Umsetzung der beschlossenen Maßnahmen wird jeweils ein Verantwortlicher mit Termin für die Erledigung benannt.

Das Formblatt auf S. 145 zeigt exemplarisch eine durchgeführte FMEA für das erweiterte cyber-physische System.

Bewertungsschema bei einer FMEA	
B - Bedeutung der Fehlerfolge	Bewertungspunkte
Es ist unwahrscheinlich, dass der Fehler vom Kunden wahrgenommen wird, da die Auswirkungen auf die Funktion des Produkts vernachlässigbar sind.	1
Der mögliche Fehler ist unbedeutend und wird nur von sehr wenigen Kunden wahrgenommen. Der Fehler wird die Funktion des Produkts nur minimal beeinträchtigen.	2 bis 3
Es handelt sich um einen mittelschweren Fehler, der bei einigen Kunden Unzufriedenheit auslöst. Eine Beeinträchtigung der Funktion ist feststellbar.	4 bis 6
Der Kunde ist durch einen schweren Fehler dieser Art verärgert. Sicherheitsaspekte oder gesetzliche Bestimmungen sind jedoch nicht betroffen.	7 bis 8
Es handelt sich um einen schwerwiegenden Fehler, der den Kunden stark verärgert. Eventuell sind auch Sicherheitsaspekte oder gesetzliche Vorschriften betroffen.	9 bis 10
A - Auftretenswahrscheinlichkeit des Fehlers	Bewertungspunkte
Es ist nahezu unwahrscheinlich, dass ein Fehler auftritt.	1
Es besteht eine sehr geringe Wahrscheinlichkeit, dass der Fehler auftritt.	2 bis 3
Es besteht eine geringe Wahrscheinlichkeit, dass ein Fehler auftritt. Bei vergleichbaren Produkten traten in der Vergangenheit geringe Fehlerzahlen auf.	4 bis 6
Es besteht eine mäßige Wahrscheinlichkeit, dass der Fehler auftritt, da vergleichbare Produkte bei diesem Fehler häufiger Schwierigkeiten verursacht haben.	7 bis 8
Es besteht eine hohe Wahrscheinlichkeit, dass der Fehler auftritt. Es muss mit Fehlern in größerem Umfang gerechnet werden.	9 bis 10

Bewertungsschema bei einer FMEA	
E - Entdeckungswahrscheinlichkeit des Fehlers	Bewertungspunkte
Der Fehler wird höchstwahrscheinlich bei einem nachfolgenden Arbeitsgang entdeckt.	1
Es handelt sich um einen offensichtlichen Fehler, der gut entdeckt werden kann.	2 bis 5
Es besteht eine geringe Wahrscheinlichkeit den Fehler zu entdecken.	6 bis 8
Es besteht eine sehr geringe Wahrscheinlichkeit den Fehler zu entdecken.	9
Es ist nahezu unwahrscheinlich, dass der Fehler entdeckt werden kann. Das Merkmal wird nicht bzw. kann nicht geprüft werden.	10

LE 3 - Verbesserungsvorschläge dem Auftraggeber vorstellen

Sie haben im Team unterschiedliche Verbesserungen für das cyber-physische System identifiziert und möchten nun das Einverständnis zur Umsetzung Ihres Plans. Allerdings werden für die Umsetzung zusätzliche Ressourcen (zusätzliche Entwicklungszeit) benötigt, was bislang nicht eingeplant war. Sie und das Team erachten allerdings Ihre Vorschläge als echten Mehrwert für den Kunden und auch die JIKU IT-Solutions. Daher informieren Sie sich über Alternativen, wie Sie die volle Unterstützung für Ihre Verbesserungsvorschläge bekommen können. Der Ausbildungsverantwortliche der Entwicklungsabteilung macht zwei Vorschläge: Sie können die Ideen über das betriebliche Vorschlagswesen an die Geschäftsleitung weiterleiten oder „in einer Minute“ erklären, warum die erarbeiteten Vorschläge umgesetzt werden müssen.



LE 4 - Betriebliches Vorschlagswesen (BVW)

Viele Mitarbeiter haben neue Perspektiven auf das Unternehmen oder Ideen zu Produkten, Prozessen und Dienstleistungen. In der täglichen Arbeitspraxis ist es oftmals wahrscheinlicher, dass Probleme und Schwachstellen erkannt werden, die den Führungsverantwortlichen nicht bekannt sind. Vorgesetzte sehen teilweise nur den Fortschritt oder das Endergebnis eines Auftrags, selten jedoch, wie sich der gesamte Ablauf gestaltet hat.

Ein betriebliches Vorschlagswesen ermöglicht es Mitarbeitern, ihre neuen Ideen an eine zentrale Stelle zu adressieren. Formale Mitarbeiterempfehlungsprogramme können die Gesamtleistung eines Unternehmens verbessern, indem Mitarbeiter auf allen Ebenen nach deren Ideen befragt werden. Bei der Implementierung eines betrieblichen Vorschlagswesens (BVW) stehen zwar bessere Produkte, Prozesse, Einsparpotenziale oder neue Dienstleistungen im Vordergrund, aber es geht auch um die Bereitschaft der Führungsverantwortlichen, auf die Ideen der Mitarbeiter einzugehen. Mitarbeitern eines Unternehmens ist es wichtig, dass ihre Anliegen wahrgenommen, reflektiert und honoriert werden.

Betriebliches Vorschlagswesen - wichtige Fragestellungen

Wer reicht den Vorschlag ein?

Für Mitarbeiter sollte es möglich sein, Vorschläge anonym einzureichen, insbesondere für Kritik an bestehenden Strukturen und Abläufen. Aber es sollte auch möglich sein, den eigenen Namen anzugeben, um beispielsweise die Anerkennung für gute Ideen zu erhalten.

Welches Problem wird durch den Vorschlag gelöst?

Gute Vorschläge lösen ein Problem bereits dann, wenn es vom Unternehmen als solches noch gar nicht erkannt wird. Daher muss bei der Einreichung des Vorschlags der Zusammenhang zwischen dem Problem und dem Betroffenen verdeutlicht werden. Handelt es sich um ein Problem für den Endkunden, die Mitarbeiter oder die Prozesseffizienz? Erst dadurch können Vorgesetzte einen klaren Zusammenhang zwischen Problem und Verbesserungsvorschlag herstellen.

Was ist die innovative Lösung?

Das Vorschlagsformular sollte den Mitarbeitern viel Raum geben, die Idee zu formulieren. Wenn ein Vorschlagsformular digital übermittelt wird, sollte es Möglichkeiten für Dateianlagen und Verlinkungen geben.

Was sind die geschätzten Kosten und Nutzen?

Die Einbeziehung dieses Feldes gibt den Mitarbeitern die Möglichkeit zu zeigen, dass die Idee realistisch und gut durchdacht ist.

LE 5 - Elevator Pitch

Vorgesetzte in kürzester Zeit von einem Vorschlag zu überzeugen, ist sehr herausfordernd. Wer nur kurze Zeit zur Verfügung hat, muss die Botschaft sehr gut strukturieren. Ein bekannter Ansatz ist der sogenannte Elevator Pitch. Der Name kommt daher, dass man einer Vorgesetzten bei einer Fahrt im Aufzug in kürzester Zeit das Anliegen vermittelt und am Ende der Fahrt die Zustimmung erhält. Der Ablauf eines Elevator Pitches baut auf dem AIDA-Modell auf. Diese Vorgehensweise wurde ursprünglich für den Vertrieb entwickelt, kann aber auch zur zielgerichteten Präsentation eingesetzt werden.



Ein Elevator Pitch ist im Grunde eine überzeugende Kurzpräsentation. Wie bei jeder anderen Präsentation erfordert dies im Vorfeld genaue Recherche und gute Planung. Man benötigt eine klare Struktur, um sein Gegenüber in der Kürze der Zeit nicht zu verlieren. Beim AIDA-Modell wird eine Idee in vier Schritten vorgestellt.

Das AIDA-Modell beim Elevator Pitch

Aufmerksamkeit im Elevator Pitch erregen

Vor der eigentlichen Botschaft muss man sich die Aufmerksamkeit sichern. Dies kann erreicht werden, indem man seinem Gegenüber mit einem spannenden Fakt oder einem kontroversen Statement konfrontiert. Die genaue Ausformulierung des Einstiegssatzes ist hierbei sehr wichtig.

Der Elevator Pitch weckt Interesse

Wenn man die Aufmerksamkeit des Gesprächspartners erhalten hat, muss das Interesse geweckt werden. Hierzu sollte entweder ein Alleinstellungsmerkmal der Idee, ein Vorteil für das Unternehmen oder den Kunden des Unternehmens verdeutlicht werden.

Das AIDA-Modell beim Elevator Pitch

Der Elevator Pitch soll Verlangen auslösen

Um beim Gesprächspartner ein Verlangen auszulösen, sollte man das Gegenüber zumindest ein wenig kennen. Auch hier ist im Vorfeld Recherche notwendig. Die eigene Idee oder der Vorschlag muss für den Gesprächspartner relevant sein. Idealerweise löst der Vorschlag ein potenzielles Problem des Gegenübers.

Im Elevator Pitch zur Handlung aufrufen

In der vierten und letzten Phase eines Elevator Pitch platziert man den sogenannten Call-to-Action. Man fordert das Gegenüber zum Handeln auf, indem man sich beispielsweise direkt für ein weiteres Gespräch verabredet.

Lernzielkontrolle TAG 9

1. Diskutieren Sie im Team über Sicherheitsrisiken im kommerziellen, industriellen und privaten Bereich. Wählen Sie jeweils ein konkretes Szenario und beschreiben Sie die Risiken, das Gefahrenpotenzial und Möglichkeiten zur Minimierung der Risiken.
2. Welche Aussagen sind richtig?
 - a. FMEA steht für Failure Mode and Effect Analysis.
 - b. Die FMEA kann von jedem Projektmitglied durchgeführt werden.
 - c. Das Projektteam sollte am besten nur aus drei Personen bestehen, die alle aus der gleichen Abteilung sind.
 - d. Eine Strukturanalyse zerlegt ein Produkt in seine einzelnen Baugruppen und Komponenten.
 - e. Nicht jedes Strukturelement hat eine eigene Funktion.
 - f. Bei der Fehleranalyse werden die Auswirkungen auf den Endkunden (Fehlerfolgen) nicht berücksichtigt.
 - g. Eine Risikoprioritätszahl von größer 200 bedeutet ein kleines Risiko.
3. Ein Kunde kann durch einen schweren Fehler dieser Art sehr verärgert sein. Hinzu kommt, dass eine hohe Wahrscheinlichkeit besteht, dass der Fehler beim Kunden auftritt. Im Unternehmen kann der Fehler mit einer Wahrscheinlichkeit <90% entdeckt werden. Berechnen Sie die RPZ.
4. Tauschen Sie sich in Vierergruppen über das betriebliche Vorschlagswesen aus. Gibt es in Ihren Betrieben ein betriebliches Vorschlagswesen, das Sie gemeinsam diskutieren können? Falls nein, besprechen Sie Ihre persönliche Meinung zum betrieblichen Vorschlagswesen im Team.
5. Erstellen Sie schriftlich einen kurzen Elevator Pitch Ihrer Wahl auf Basis des AIDA-Modells.

TAG 10 - Vertiefung des Wissens und Modulprüfung

LE 1- Einleitung

Der letzte Tag in diesem Modul bietet Ihnen die Möglichkeit der Wiederholung und Vertiefung Ihres Wissens. Sollten es noch offene, nicht vollständig bearbeitete Modul-Inhalte geben, nutzen Sie den heutigen Tag zur Komplettierung.

LE 2 - Modulprüfung

120 Minuten zu denen wir Ihnen recht viel Erfolg wünschen!