EUROPA-FACHBUCHREIHE für
informationstechnische und
kommunikationstechnische
Berufe

IT-Tabellenbuch

6. Auflage

Bearbeitet von Lehrern und Ingenieuren an beruflichen Schulen, berufspädagogischen Seminaren, Fachhochschulen und in Betrieben (siehe Rückseite)

VERLAG EUROPA-LEHRMITTEL · Nourney, Vollmer GmbH & Co. KG
Düsselberger Straße 23 · 42781 Haan-Gruiten

Europa-Nr.: 37019

Autoren des IT-Tabellenbuches:

Monika Burgmaier	Durbach
Patricia Burgmaier	Melsungen
Frédérique Chauffer	Offenburg
Elmar Dehler	Ulm
Bernhard Grimm	Sindelfingen, Leonberg
Ute Jansen	Sindelfingen, Grafenau
Jan Quast	Berlin
Bernd Schiemann	Durbach

Leitung des Arbeitskreises und Lektorat:
Bernd Schiemann, Durbach

Bildbearbeitung:
Zeichenbüro des Verlags Europa-Lehrmittel, Ostfildern

Diesem Buch wurden die neuesten Ausgaben der DIN-Blätter und der VDE-Bestimmungen zugrunde gelegt. Verbindlich sind jedoch nur die DIN-Blätter und VDE-Bestimmungen selbst.

Die DIN-Blätter können von der Beuth-Verlag GmbH, Burggrafenstraße 6, 10787 Berlin, bezogen werden. Die VDE-Bestimmungen sind bei der VDE-Verlag GmbH, Bismarkstr. 33, 10625 Berlin, erhältlich.

Das vorliegende Werk wurde mit aller gebotenen Sorgfalt erarbeitet. Dennoch übernehmen Autoren, Herausgeber und Verlag für die Richtigkeit von Fakten, Hinweisen und Vorschlägen sowie für eventuelle Satz- und Druckfehler keine Haftung.

6. Auflage 2025

Druck 5 4 3 2 1

Alle Drucke derselben Auflage sind parallel einsetzbar, da sie bis auf die Korrektur von Druckfehlern identisch sind.

ISBN 978-3-8085-3192-1

Satz: Grafische Produktionen Jürgen Neumann, 97222 Rimpar, www.gp-neumann.de
Umschlag: braunwerbeagentur, 42477 Radevormwald
Umschlagfoto: ©sdecoret-stock.adobe.com
Druck: UAB BALTO print, 08217 Vilnius (LT)

Vorwort zur 6. Auflage

Technische Weiterentwicklungen im Rahmen der Digitalisierung, Industrie 4.0, Smarte Technologien und die Anpassung an geänderte Normen führten zu einer Überarbeitung und Erweiterung des Tabellenbuches. Das Buch ist ein umfassendes Nachschlagewerk für die Berufe Fachinformatiker/-in in den Fachrichtungen Anwendungsentwicklung, Systemintegration, Daten- und Prozessanalyse, Digitale Vernetzung, IT-System-Elektroniker/in, sowie für die Berufe Systeminformatiker/in, Elektroniker/in Fachrichtung Informationstechnik und Systemtechnik.

Lernende in Berufskollegs, beruflichen Gymnasien, in der Weiterbildung zum Techniker oder Meister sowie Studierende finden einen kompakten Überblick über den aktuellen Stand der Informatik und ihrer Anwendungen.

Das Buch enthält die Hauptabschnitte:

1	Der Betrieb und sein Umfeld Geschäftsprozesse und betriebliche Organisation Arbeitsmethoden und Informationsquellen
2_1	Mathematische und informationstechnische Grundlagen, Elektrotechnische Grundlagen, Energietechnik, Ergonomie und Arbeitsschutz
2_2	PC-Baugruppen, Bussysteme und Anschlusstechnik, Datenträger, Karten und Geräte, Betriebssysteme
3	Projektmanagement, Programmentwicklung, Programm-Anwendungen
4	Übertragungstechnik, Grundlagen der Netze, Netzwerk-Praxis, Leitungen
5_1	Festnetze, Mobile Netze, Funknetzwerke
5_2	Digitalisierung, Datenschutz und Arbeitssicherheit in der IT
6	Internet, Service an IT-Systemen
7	Marktbeziehungen und Kundenbeziehungen
8	Rechnungswesen und Controlling

Neu:

Fehlerbaumanalyse, Funkstörung, Funkentstörung, Laserschutz und Laserschutzklassen, CPS-Systeme, Embedded Systems, WEMOS D1 mini mit ESP8266, Windows, Linux im Netzwerk (Grundlagen), Virtuelle Maschinen (VMs) und Container, Schutzmaßnahmen für Software und Betriebssysteme, Agile Methoden, Gefährdungsbeurteilung, Datenstrukturen, Klassen und Vererbung in C#, Polymorphie und Assoziationen in C#, Grundlagen, Kontrollstrukturen und Funktionen in Python, NoSQL-Datenbanken, Dateiformate, Server, Blade-Server, Netzverteiler für Glasfasernetze, RADIUS-Server, Energy-Harvesting, Sensoren für IIoT-Anwendungen, Anwendungsbereiche der Künstlichen Intelligenz KI und KI-Bedrohungen, Turing-Test, Einfluss von KI und ML auf die Cyber-Security, DECT New Radio, Datenträger sicher entsorgen, Kryptologie, Digitale Zertifikate, Digitale Signatur, Cyber-Sicherheit in der Industrie, EU-Gesetze und Richtlinien zum Datenschutz, Webhosting mit Windows- und Linux-Servern, Videokonferenz, Streaming-Media.

Das Buch enthält auch neu gestaltete oder überarbeitete Seiten.

Das IT-Tabellenbuch kann

- unterrichtsbegleitend
- zur Prüfungsvorbereitung
- zum Selbststudium
- für die Weiterbildung und auch bei beruflichen Tätigkeiten verwendet werden.

Ihre Meinung interessiert uns!

Teilen Sie uns bitte Ihre Verbesserungsvorschläge, Ihre Kritik, aber auch Ihre Zustimmung zum Buch mit.

Bitte schreiben Sie uns an die E-Mail-Adresse: lektorat@europa-lehrmittel.de

Sommer 2025

Die Autoren und der Verlag Europa-Lehrmittel

Unterbrechungsfreie Stromversorgungssysteme USV
Uninterruptable power supply systems UPS

USV-Anlage: 850 VA, 3,6 A, 10,4 kg

Klassifizierungsschlüssel nach DIN EN 62040-3

1	2	3
VI	SS	333

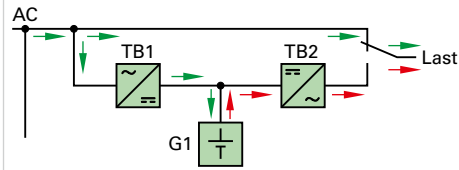
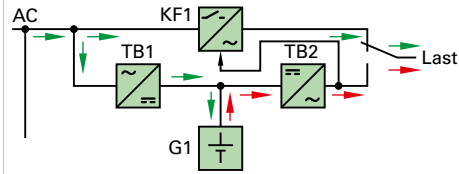
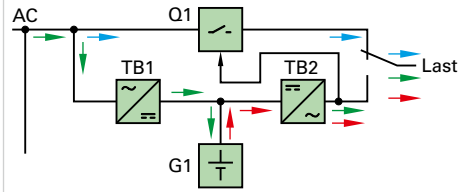
Klassifizierungsschlüssel 1 bis 3

3 — Reaktion des Ausgangssignals auf Lastwechsel: Dynamische Reaktion der Ausgangsspannung auf Lastwechsel

2 — Schwingungsform des Ausgangssignals auf Lastwechsel: Wellenform des Ausgangssignals im Normalbetrieb und hauptnetzunabhängig

1 — Abhängigkeit der Ausgangsspannung vom Netzsignal: USV-Typen VFI, VFD und VI

Klassifizierungsschlüssel 1 (Beispiel)

Typ	Anwendungen	Schaltungen
VFD[1] Spannungs- und frequenzabhängige USV Normalbetrieb → Verbraucher direkt mit dem Netz verbunden. Der Akkumulator G1 wird über TB1 geladen. Bei Netzausfall wird der Verbraucher durch G1 über TB2 versorgt. Die Umschaltzeit beträgt bis zu 20 ms.	PC-Arbeitsplatz, Drucker, Telefon-Anlagen.	
VI[2] Spannungsunabhängige USV Normalbetrieb → Verbraucher über Spannungsregler KF1 mit dem Netz verbunden. Der Akkumulator G1 wird geladen. Bei Netzausfall wird der Verbraucher durch G1 versorgt. Die Umschaltzeit beträgt 4 ms bis 10 ms.	Büro-Netzwerke, Serveranlagen, Kassensysteme.	
VFI[3] Spannungs- und frequenzunabhängige USV Die Ausgangsspannung ist unabhängig von Netzstörungen. Der Energiefluss erfolgt über den TB1 und Wechselrichter TB2. Bei Netzausfall wird G1 die Energie ohne Umschaltzeit entnommen. Interner Fehler → Bypass Q1 wird automatisch eingeschaltet.	Rechenzentrum, Serveranlagen, Netzwerke, Prozessautomatisierung, Sicherheitssysteme.	

Klassifizierungsschlüssel 2		Klassifizierungsschlüssel 3	
Form der Ausgangsspannung bei a) Normal- und b) Akkumulatorbetrieb	S sinusförmig, X sinusförmig bei linearer Last, Y nicht sinusförmig.	Spannungsänderung bei a) Änderung der Betriebsart, b) linearen und c) nichtlinearen Lastsprüngen	Abweichung von der Bemessungsspannung: Ziffer 1 = max. 30 %, nach 0,1 s max. ± 10 % Ziffer 2 w = max. 100 % bis zu 1 ms, nach 0,1 s max. ± 10 %

Klassifizierungscode VFI SS 122

VFI → Die USV ist spannungs- und frequenzunabhängig vom Netz

SS → Sinusförmige Ausgangsspannung bei Netz- und Akkumulatorbetrieb

122 → 1 Unterbrechungsfreie USV
2 Nichtlineare Lastsprünge mit Spannungsänderungen < 1 ms
2 Lineare Lastsprünge mit Spannungsänderungen < 1 ms

Auswahlkriterien

1. Leistungsmaximum (Geräteleistungen)
2. Überlastfähigkeit und Überlastdauer für Sicherungen und RCDs
3. Klassifizierung festlegen
4. Netzwerkanschluss für automatischen Shutdown angeschlossener PC bei Ende der Autonomiezeit
5. Rückwirkung auf das speisende Netz
6. Redundanz durch mehrere USV
7. Batteriekapazität
8. Netzanschluss 1x AC oder 3x AC
9. Standgerät oder Einbaugerät
10. Umgebungstemperatur für Lebensdauer der Akkumulatoren berücksichtigen

[1] VFD von Voltage and Frequency Dependent = spannungs- und frequenzabhängig; [2] VI von Voltage Independent = spannungsunabhängig; [3] VFI von Voltage and Frequency Independent = spannungs- und frequenzunabhängig

CPS-Systeme Cyber physical systems

Cyberphysische Systeme bestehen aus mechanischen Komponenten, Software und die Verarbeitung von Informationen. Die Verbindungen werden über leitungsgebundene Netzwerke oder Funknetzwerke hergestellt.

CPS von Cyber physical system = Cyberphysisches System

Cyber griech. = (Schiff-)Steuerung

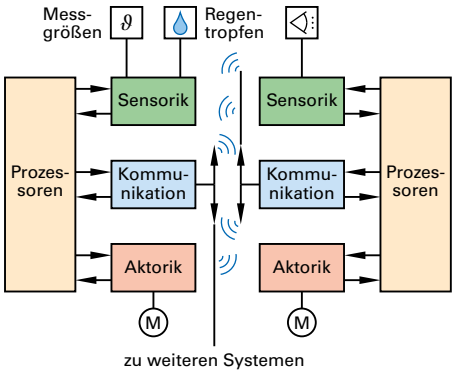
SBC von Single board (Computer) = Einplatinen-Rechner

Shields (Schilder). Platinen, die auf die Kontaktreihen des Arduino steckbar sind

Aufbau

CPS ermöglichen die Steuerung und die Kontrolle komplexer Systeme (Bild).

Die Schnittstellen für Sensorik, Kommunikation und Aktorik sind Teil des Mikroprozessors oder sie werden zusätzlich, als Shields, auf die Prozessorplatine gesteckt.



Cyberphysisches System mit Schnittstellen

Anwendungen

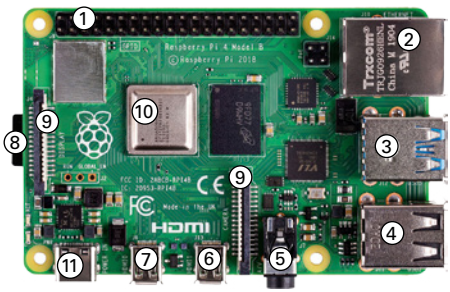
- Regeln von Raumtemperaturen, z. B. Kühlen, Heizen oder Ausschalten.
- Vernetzen von industriellen Steuerungen für nötigen Werkzeugwechsel.
- Systemfunktionen durch Machine Learning (Maschinelles Lernen) anpassen, z. B. Messwertintervalle an die Fehlerhäufigkeit der Fertigung anpassen.

Einplatinencomputer (SBC)

Einplatinencomputer sind funktionsfähige Computer mit nicht sehr hoher Arbeitsgeschwindigkeit. Prozessor, Arbeitsspeicher, Schnittstellen für Eingabe mit der Tastatur und Ausgabe auf dem Monitor befinden sich auf einer Platine **(Bild)**. Meist sind 1 **GPIOs** (General Purpose Input Output) vorhanden, die programmierbar sind.

Schnittstellen:

2 Ethernet, 3 USB-3, 4 USB-2, 5 Audio, 6, 7 HDMI 2.1, 8 SD-Kartenslot, 9 Kameraanschlüsse, 10 Prozessor, 11 USB-C Stromversorgung.



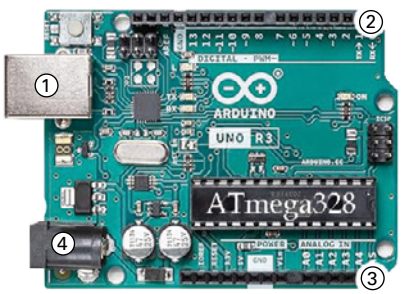
SPC mit Raspberry

Mikrocontrollerboards

Moderne Microcontroller arbeiten mit Frequenzen von 32 Mhz bis 160 Mhz.

Durch geeignete Microcontrollerboards und eine passende Entwicklungssoftware sind sie einfach zu programmieren. Programme können auf EEROMS auf das Board geladen werden und direkt ausgeführt werden.

Zur Programmentwicklung wird ein Laptop, ein USB-Kabel und entsprechende Software benötigt. Ein verbreitetes Mikrocontrollerboard ist z. B. der Arduino UNO **(Bild)**.



Mikrocontroller Arduino UNO

Anschlüsse:

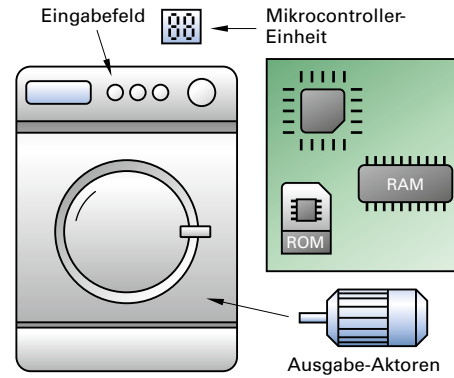
1 USB B, 2, 3 Kontaktreihen, Pins meist programmierbar, 4 Stromversorgung

Embedded System

Mikrocontroller sind Bauelemente, die in Geräten und Systemen zur Steuerung und Regelung verwendet werden **(Bild)**.

Platinen mit Mikrocontroller und weiteren Bauelementen, z. B RAM und ROM werden als **Embedded System** bezeichnet.

Enthält ein integrierter Schaltkreis alle wesentlichen Bestandteile eines Computers im Chip, wird dies auch als **SoC** (System on Chip / Ein-Chip-System) bezeichnet. Als System wird die Kombination vom logischen Schaltungen, Taktgeber, mikrotechnischen Sensoren und Autostart bezeichnet.



Waschmaschine als Embedded System

Auswahlkriterien für Mikrocontroller

Eigenschaften von Mikrocontrollern

Die meisten Microcontroller verwenden

- verschiedene Speicher (Harvardstruktur[1]) für Programme und Daten,
- Datenbusbreiten von 4 bit, 8 bit, 16 bit, 32 bit und 64 bit.

Die Hersteller bieten verschiedene Varianten (Familien) an, die sich durch Anzahl der Schnittstellen und Speichergrößen unterscheiden **(Tabelle 1)**. Die Programmierung erfolgt

- mit ISP (In System Programming) oder
- einer IDE (Integrated Development Environment).

Bei der Auswahl sind die Anforderungen der Anwendung zu beachten.

Tabelle 1: Mikrocontroller-Familien

Hersteller	Produkt	Bemerkungen
Atmel (AVR)	AT89-, AT90-, ATtyni-, AT91-, AT32	Leicht zu programmieren
Fujitsu	F2MC-8, F2MC-16, FR 32 bit	Für Haushaltsgeräte
Infineon	8051; C166; Tri-Core	SPS und automotive Anwendungen
NXP	ARM7, ARM9, Cortex-M0/-M3	Smartphones, Tablets
Renesas	H8/300, H8S, RL78, 78K0, 78KOR, R8C	Digitalkameras, Printer Controller, Lego Mindstorm
STM	STM32F2, F4, F7, H7	KI, Motor-Control

Anforderungen an die Mikrocontroller

Je nach Anwendung werden unterschiedliche Anforderungen an die Mikrocontroller gestellt **(Tabelle 2)**. Für Echtzeitanwendungen sind

- Taktfrequenzen bis 100 MHz erforderlich,
- Arbeitsspeicher (RAM) bis 32 Kbyte.

Die Festwertspeicher enthalten die Steuerprogramme in verschiedenen Programmiersprachen

- z. B. C, C++, Java, C#,
- Festwertspeicherplatz bis 512 Kbyte.

Mikrocontroller haben je nach Typ Gehäuse mit 40 Pins bis 300 Pins.

Entwicklungssysteme

Alle Hersteller bieten für ihre Mikrocontrollerfamilien IDEs (integrierte Entwicklungssysteme) an. Meist kann die entwickelte Schaltung simuliert werden.

Tabelle 2: Anforderungen an Mikrocontroller

Merkmal	Anwendungen	
	Einfach	Komplex
Taktfrequenz	< 10 MHz	bis 550 MHz
Programmierung	Assembler, C, BASIC	C+, C++, Java
RAM-Größe	< 1 KByte	< 32 KByte
ROM/EEPROM	< 16 KByte	< 512 KByte
I/O-Pins Timer	6 2 8 bit/ 16 bit	50 bis 80 z.B. mit 16 bit
Pins on Chip	40 bis 80	200 bis 300

[1] Harvard, Universität in Massachusetts, USA.

Mikrocontroller-Vergleich Comparison of microcontrollers

Mikrocontroller-Auswahlkriterien

Merkmal	Kenngröße	Erklärung, Bemerkung
Bitbreite (Bits)	8 bit, 16 bit, 32 bit ,64 bit	Datenwortbreite des internen Busses
Speicher (memory)	Eingebetteter Speicher (embedded), externer Speicher (external)	RAM und ROM Speicher integriert, oft zusätzlich erweiterbar
Befehlssatz (instruction set)	RISC (Reduced Instruction Set Computer)	Reduzierter Befehlssatz, viele Register
	CISC (Complex Instruction Set Computer)	Umfangreicher Befehlssatz
Rechner-Architekturen	**Harvard**-Architektur	Befehlsspeicher und Datenspeicher getrennt
	Von Neumann-(Princeton-)Architektur	Daten und Programm im gleichen Speicher
Integrations-grad	• IC-Chip • VLSI core (very large scale integration)	Integrierte Schaltung auf 1 Chip Eingebetteter Prozessor
Program-mierung	• ISP (In System Programmierung) • IDE (Integrated Development Environment)	Programmierung im Zielsystem Oft kostenlose Entwicklungsumgebungen

Mikrocontroller-Familien

Hersteller	Produkte (Auswahl)	Bemerkungen
Atmel	AT89-, AT90-, ATtiny-, ATmega-, ATX-mega-Serie, AT91-AT32-Serie	Aufbau einfach, leicht zu programmieren
Fujitsu	F2MC-8; F2MC-16; FR 32 bit	Einsatz in Haushalts-anwendungen
NXP (Free-scale)	S08; S12; Cold-Fire; Cortex-M4	Automotive Anwendungen, schnelle A/D-Wandler
Infineon	8051; C166; Tri-Core	SPS und automo-tive Anwendungen
Micro-chip	PIC12 bis PIC32	Programmierung mit Adapter, interne Module
NXP Semicon-ductors	ARM7; ARM9; Cortex-M0; Corex-M3	Im Embedded-Bereich, in Smartphones, Tablets
Renesas	H8/300; H8S; RL78; 78K0; 78K0R; R8C; V850/FIX	Digitalkameras, Printer Controller, Lego Mindstorm
Weitere Hersteller	Texas Instruments, Zilog, Silicon Laboratories, Maxim, Energy Micro, Samsung, Epson.	

Anforderungen an Mikrocontroller

Merkmal	Einfache Anwendungen	Komplexe Anwendungen
Prozes-sorkern	8-Bit-CPU	32-Bit-CPU
Takt-frequenz	< 10 MHz	< 100 MHz
Program-mierung	Assembler C, BASIC	C++, Java, Wiederverwen-dung des Codes möglich
RAM-Größe	< 1 KByte	< 32 KByte
ROM/ EEPROM	< 16 KByte	< 512 KByte
I/O-Pins	ca. 6	ca. 50 bis 80
Timer	2 (z. B. 1 × 8 bit, 1 × 16 bit)	z. B. 8 × 16 bit
Pins on Chip	40 - 80 Pins	200 bis 300 Pins
Anwen-dungs-beispiele	Waschmaschine, Telefon, Haushalts-technik, Kfz-Technik	Automatisierung, Steuern und Regeln von Prozessen, Echtzeitsysteme
Preis	< 2 €	ca. 10 €

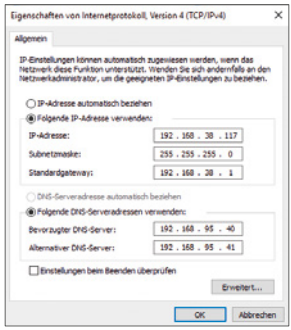
Modulare Entwicklungssysteme mit Mikrocontrollern (Auswahl)

Merkmal	Arduino Uno	Raspberry Pi
Prozessor	ATmega328 (8 Bit), SAMD21 (32 Bit Arduino Zero)	ARM1176JZF-S
Taktfrequenz	16 MHz (48 MHz beim Arduino Zero)	70 MHz
Besondere Merkmale	Onboard USB-Controller, mit Boot-Loader vorprogrammiert	HD Video-Ausgabe HDMI, 3,5 mm Klinke Audio HDMI, 10/100 Mbit-Ethernet

Konfiguration der Netzwerkschnittstellen

Die Konfiguration der Netzwerkschnittstellen erfolgt über die grafische Oberfläche (GUI), über die Eingabeaufforderung (cmd) oder über die Powershell.

Grafische Oberfläche (GUI):



Eingabeaufforderung (cmd):

```
netsh interface ipv4 set address name="eth0" static
192.168.38.117 255.255.255.0 192.168.38.1
netsh interface ip set dns "eth0" static 192.168.95.40
netsh interface ip add dns "eth0" static 192.168.95.41
```

Powershell:

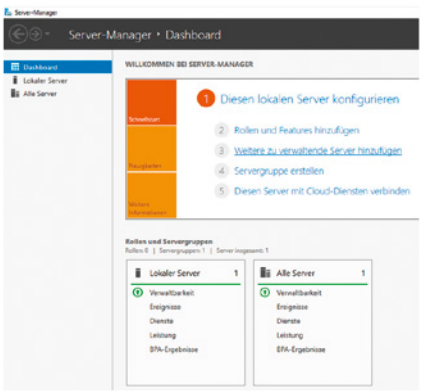
```
New-NetIPAddress -IPAdress 192.168.38.117 -PrefixLength 24
-DefaultGateway 192.168.38.1 -InterfaceAlias "eth0" -Address-
Family IPv4
Set-DnsClientServerAddress -InterfaceAlias "eth0" -ServerAd-
dresses ("192.168.95.40", "192.168.95.41")
```

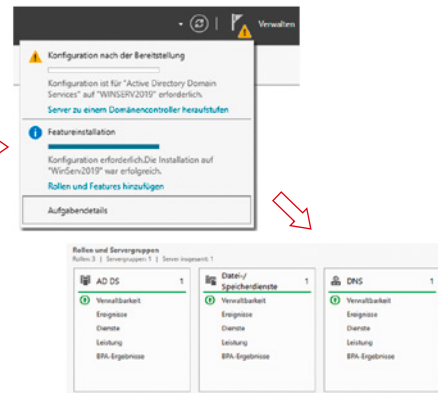
Active Directory (AD)

Verzeichnisdienst von Microsoft. Ermöglicht, ein Netzwerk entsprechend der realen Struktur des Unternehmens oder seiner räumlichen Verteilung zu gliedern.

Um den Verzeichnisdienst zu installieren, fügen Sie im Server-Manager (GUI) oder in der Powershell die Rolle „Active Directory Domain Services“ hinzu.

Installation über den Server-Manager (GUI):





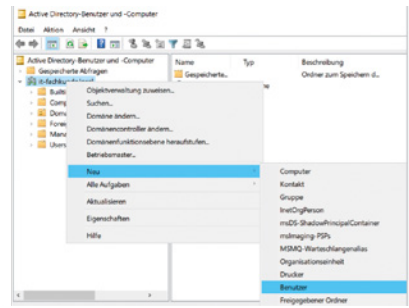
Installation über die Powershell:

```
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
Install-ADDSDomainController -InstallDns -DomainName it-tabellenbuch.local
```

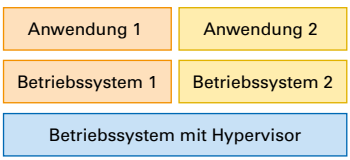
Im Active Directory werden Benutzer, Gruppen, Computer, Dateifreigaben und andere Geräte wie Drucker in einem Verzeichnis (Directory) verwaltet.

Durch Organisationseinheiten werden organisatorische Strukturen eines Betriebs abgebildet. Es können Gruppen von Nutzer- und Computerkonten zusammengefasst und verwaltet werden.

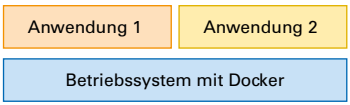
Gruppenrichtlinien (Policy) sind Konfigurationsanweisungen und bieten eine Vielzahl an Möglichkeiten zur Verwaltung von Computern und Nutzern.



Vergleich VM und Container



In einer virtuellen Maschine (VM) wird eine vollständige und unabhängige Kopie eines Betriebssystems installiert. Die dazu notwendige Software wird als Hypervisor bezeichnet. Eine VM emuliert die Hardware eines Computers und ermöglicht das Ausführen verschiedener Betriebssysteme auf einem physischen Host.



Ein Container ist eine isolierte Umgebung, in der lediglich eine Anwendung mit ihren Abhängigkeiten ausgeführt wird. Im Gegensatz zu einer VM teilen und nutzen Container die Ressourcen des Host-Betriebssystems.

Container mit Docker

Docker ist eine Open-Source-Plattform, die einzelne Anwendungen in isolierten Containern ausführt. Podman oder Kubernetes sind weitere Programme zum Arbeiten mit Containern.

Funktionsweise

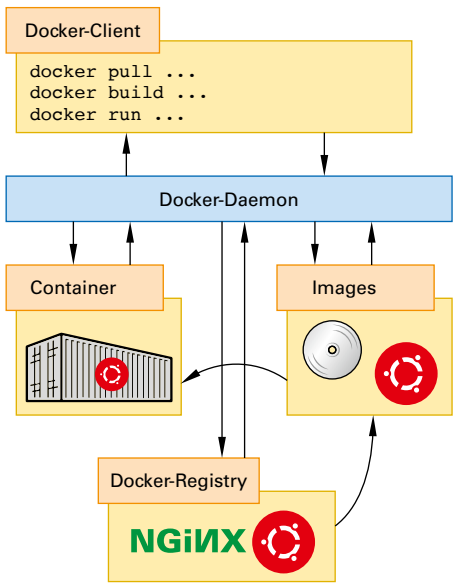


Image:
Schreibgeschützte Vorlage für einen Container. Enthält alle Dateien, Abhängigkeiten und Konfigurationen, die für die Ausführung einer Anwendung erforderlich sind. Images werden entweder als fertige Vorlage von der Docker-Registry bezogen oder manuell mit sogenannten Dockerfiles erstellt.

Docker-Registry:
Zentraler Speicherort für Docker-Images. Enthält öffentliche und private Repositories (Paketlisten), in denen Images hoch- bzw. heruntergeladen und geteilt werden können. Die bekannteste Docker-Registry ist Docker Hub.

Container:
Container sind lauffähige Anwendungen, die aus einem Image erstellt werden.

Docker-Client:
Befehlszeilenwerkzeug / grafische Benutzeroberfläche zum Verwalten von Containern.

Docker-Daemon:
Hintergrundprozess, der auf dem Host-Betriebssystem läuft und u.a. folgende Befehle ausführen kann:

Befehle

docker search <Schlagwort>	Durchsucht die Docker-Registry nach passenden Images
docker pull <Image-Name>	Image wird aus der Docker-Registry heruntergeladen.
docker build <Docker-File>[1)]	Erstellt ein eigenes Image.
docker image ls	Zeigt eine Liste der lokalen Image-Dateien.
docker run <Image-Name>[2)]	Erstellt einen Container und führt diesen aus.
docker ps	Zeigt eine Liste der laufenden Container.
docker stop <Container-Name>	Stoppt einen Container.

[1)] Durch detaillierte Anweisungen im sogenannten Docker-File kann ein passgenaues, eigenes Image erzeugt werden.
[2)] Der Befehl docker run erlaubt vielfältige Einstellungsoptionen, z. B. zur Einbindung ins Netzwerk, zur Port-Weiterleitung, zum Mapping von Laufwerken und zu spezifischen Umgebungsvariablen.

Schutzmaßnahmen für Software, Betriebssysteme und Cyberangriffe

Protective measures for Software, Operating systems and Cyber-attacks

Schutzmaßnahmen für Software

• **Originaldatenträger,** Software nur von Originaldatenträgern oder geprüften identischen Kopien installieren	Veränderungen durch Malware, Bit-Fehler oder manipulierte Konfigurationsdateien vermeidbar.
• **Standardsoftware** nach Anforderungskatalog verwenden.	Auswahl geeigneter Standardsoftware erfolgt durch das IT-Team.
• **Anforderungen** an die Funktlonalität und wichtige Anforderungen für die Sicherheit	Software ist anhand vorhandener Bestell-Unterlagen zu überprüfen. Wer hatte bestellt, für wen ist sie bestimmt? Transportschäden ja/nein, ist sie vollständig?
• **Deinstallation** aller Dateien, die für den Betrieb dieser Software angelegt wurden.	Alle Einträge in Systemdateien entfernen.

Schutzmaßnahmen für Betriebssysteme

• **Minimales System,** nur notwendige Programme installieren.	Weitere Programme stellen ein zusätzliches Gefahrenpotenzial dar.
• **Konfiguration zusammenstellen,** nur benötigte Programmteile installieren, keine kompletten Programmpakete, wegen nicht benötigter Systemprogramme.	Nur benötigte Nutzer mit entsprechenden Rechten anlegen, keine Dummy-Nutzer zu Testzwecken! Nicht benötigte Ports sperren.
• **Sicherheit,** Updates und Sicherheitsupdates direkt nach Veröffentlichung ausführen. Sichere Passwörter verwenden.	**Regelmäßig:** Passwort ändern, Log-Dateien prüfen, Daten sichern.

Schutzmaßnahmen bei Cyber-Angriffen (Siehe auch Seite 387)

- **Vorfallbewertung,** Cyberattacke oder technischer Defekt.
- **Dokumentation,** alle Maßnahmen
- **Gerichtliche Sicherung,** alle Informationen
- **Zeitkritische Vorgänge,** vorrangig behandeln
- **Systeme** vom Netzwerk, vom Internet trennen, **unautorisierte Zugriffe unterbinden**
- **Backups,** laufende Backups stoppen
- **Ausbreitung,** alle angegriffenen Systeme **identifizieren**
- **Durch Attacke ausgenutzte Schwachstellen** im System, entfernen.
- **Benachrichtigung** an Polizei und entsprechende Behörden, z. B. BSI.
- **Zugangsberechtigungen** von Accounts prüfen, verschärfen, z. B. durch 2FA.
- **Netzwerküberwachung,** neu starten.
- **Kontrolle betroffener** Daten und Systeme. Wiederhergestellt oder erneuert?

IT-Notfallkarte

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ergebnis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltensweise

... | ... | ...

BSI

Sicherheitskennzeichen

Das BSI empfiehlt vor dem Kauf digitaler Produkte und Dienste sich zu informieren, ob ein IT-Sicherheitskennzeichen vorhanden ist **(Bild)**.

Agile Methoden Agile methods

Agile Methoden ermöglichen schnelle und flexible Anpassungsprozesse bei der Projektbearbeitung, z. B. bei der Entwicklung von Software oder bei betrieblichen Prozessen.

Beispiel für agile Methoden:
- Adaptive Software Development (ASD)
- Crystal
- Dynamic System Development Method (DSDM)
- Extreme Programming (XP)
- Kanban
- Rational Unified Process (RUP)
- Scrum

Ziel

Schnelle Bereitstellung von funktionstüchtigen Teilen der Software für den Kunden.

Optimierung und Vervollständigung der Software unter Berücksichtigung von Rückmeldungen des Kunden.

Anpassung der Software in mehreren Zyklen.

Grundwerte für agiles Handeln

1 **Menschen** vor Prozessen und Werkzeugen
2 **Funktionierende Software** von umfangreicher Dokumentation
3 **Zusammenarbeit mit dem Kunden** vor Vertragsverhandlungen
4 **Flexiblität** vor Plantreue

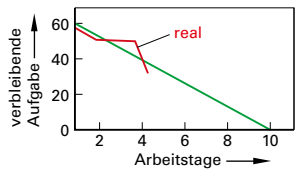
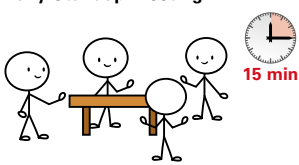
Gemeinsame Elemente für agiles Handeln
- Arbeiten in selbstorganisierten Teams,
- intensive Kommunikation im Team und mit dem Kunden,
- iterative (schrittweise wiederholende) Arbeitsweise zur ständigen Verbesserung des Ergebnisses,
- Eigenverwantwortung des Teams für die Erreichung eines qualitativ hochwertigen Ergebnisses,
- Verwendung verschiedener agiler Techniken.

Agile Prinzipien

1 Kunden zufriedenstellen.
2 Änderungen sind wilkommen.
3 Häufige Auslieferung.
4 Fachübergreifende Zusammenarbeit.
5 Unterstützen und vertrauen.
6 Direkte Kommunikation
7 Funktionierende Lösungen.
8 Nachhaltige Geschwindigkeit.
9 Streben nach Qualität.
10 Einfachheit ist von Bedeutung.
11 Selbstorganisiert handeln.
12 Reflektiere und passe an.

In Anlehnung an die 12 agilen Prinzipien nach agilemanifesto.org

Agile Techniken

Bausteine der agilen Technik	Erklärung	Hinweis
Taskboard 	Ist ein analoges oder digitales Board, das allen Mitgliedern des Entwicklungsteams den Projektstand visualisiert.	Zeigt dem Entwicklungsteam den Stand der Projektbearbeitung.
Burn-Down-Chart Datum / Tim / Ute / Uwe Priorität Fortschritt Probleme	Gibt Auskunft über den Stand der Projektbearbeitung der einzelnen Teammitglieder bzw. deren Probleme.	Unter den Mitgliedern des Entwicklungsteams besteht Transparenz. Probleme an Schnittstellen sind sofort sichtbar und können gemeinsam behoben werden.
Daily-Standup-Meeting 	Tägliche Kurzbesprechnungen im Entwicklungsteam zur Information untereinander.	Typische Fragestellung: Was hast du gestern getan? Was wirst du heute tun? Was steht dir im Weg?
User Story	Kurze Darstellung der drei Fragen: **Wer** will **Was** und **Warum**?	Ersetzt das Lastenheft aus den konventionellen Verfahren.
Definition of Done (DoD)	Checkliste zum Abhaken der schon erledigten Aktivitäten der User Story.	Dient der Abstimmung im Entwicklungsteam bzw. zwischen Auftraggeber und Entwicklungsteam.

Gefährdungsbeurteilung Hazard analysis

Der **Unternehmer** muss alle Gefährdungen für Gesundheit und Sicherheit der Beschäftigten an der Arbeitsstätte beurteilen.

Die Beurteilung muss **fachkundig** durchgeführt werden.

Fehlen dem Unternehmer dazu die fachlichen Kenntnisse, hat er sich fachlich beraten zu lassen.

Die Verantwortung für die fachliche Durchführung bleibt aber beim Unternehmer

Überwachung der Einhaltung der Vorschriften durch

- Bundesland: Gewerbeaufsichtsamt, Bezirksregierung, Landesunfallkasse (je nach Land)
- Träger der gesetzlichen Unfallversicherung Berufsgenossenschaft, Unfallkassen
- Betriebsräte und Gewerkschaften im Rahmen des Betriebsverfassungsgesetzes

Rechtsgrundlagen

- § 3 Betriebssicherheitsverordnung
- § 5 Arbeitssicherheitsgesetz
- § 4 Arbeitsschutzgesetz
- Technische Regel für Betriebssicherheit (TRBS 1111)
- Arbeitsstättenverordnung
- Gefahrstoffverordnung
- Unfallverhütungsvorschrift (DGUV Vorschrift 1)

Fragestellungen

① Welche Tätigkeiten werden ausgeführt?
Wie sind die Zuständigkeiten für Sicherheitsfragen im Unternehmen geklärt?

② Welchen Gefährdungen/Belastungen sind die Mitarbeiter ausgesetzt?

③ Wie werden die Gefährdungen in den einzelnen Arbeitsbereichen bewertet?

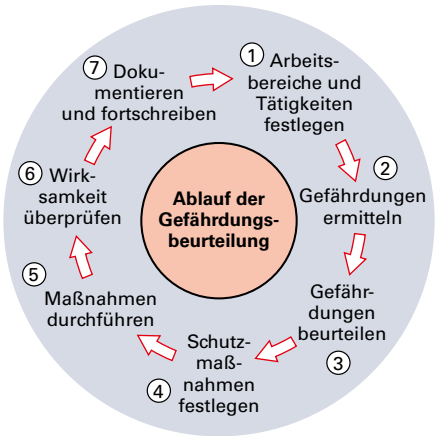
④ Welche Arbeitsschutzmaßnahmen sind aufgrund der Gefährdungen festzulegen?

⑤ Sind die festgelegten Maßnahmen umgesetzt?

⑥ Sind die umgesetzten Maßnahmen wirksam?

⑦ Wie wird der Prozess der Gefährdungsbeurteilung fortlaufend aufrechterhalten?

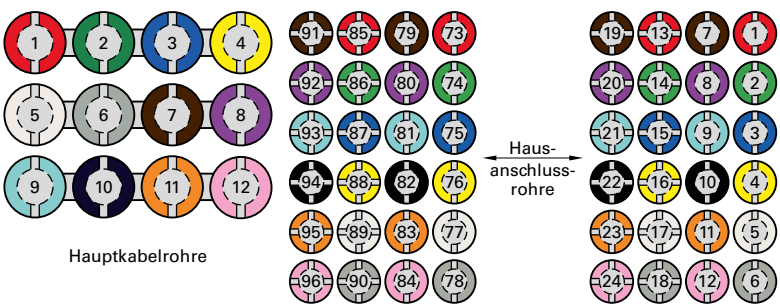
Ablauf der Gefährdungsbeurteilung



Dokumentationspflicht

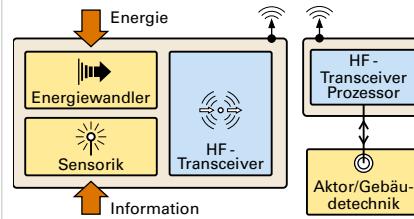
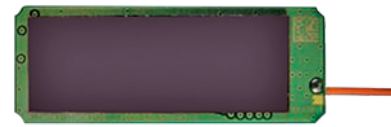
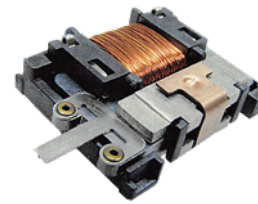
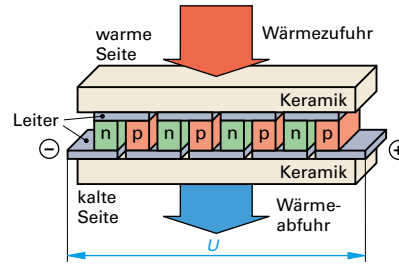
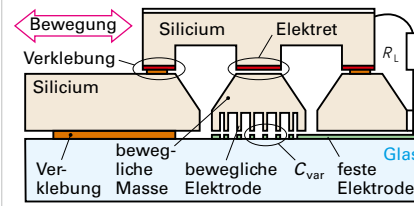
- des Ergebnisses der durchgeführten Gefährdungsbeurteilung,
- der festgelegten Maßnahmen des Arbeitsschutzes,
- des Ergebnisses der Überprüfung der Maßnahmen,
- der Unfälle im Betrieb, bei denen ein Beschäftigter getötet oder so verletzt wird, dass er für mehr als 3 Tage völlig oder teilweise arbeitsunfähig wird.

Mögliche Mängel, Gefährdungen oder Belastungen	Beispiele
• organisatorische Mängel	Fehlende persönliche Schutzausrüstung (PSA), mangelnde Regelung der Ersten Hilfe, fehlende Schulungen.
• mechanische Gefährdungen	Stolper-, Rutschgefahr, nicht geschützte bewegliche Maschinenteile.
• elektrische Gefährdungen	Körperströme, elektrostatische Aufladung.
• Gefährdung durch Stoffe	Gefahrstoffe, Hautbelastungen, Staub, Gerüche, Asbest.
• Brand- und/oder Explosionsgefährdung	Offene Flammen, brandfördernde Stoffe, Brandgefährdung durch Gase.
• Thermische Gefährdung	Kontakt zu heißen oder kalten Medien.
• Gefährdung/Belastung durch die Arbeitsumgebung	Schlechte Beleuchtung, Belüftung, kleine Räume, Abgase.
• Physikalische Einwirkungen	Lärm, Ultraschall, Hand-Arm-Schwingungen, Strahlung.
• Gefährdung durch physische Belastung	Schwere körperliche Arbeit.

Begriff	Bild, Erklärung	Bemerkung
Netzverteiler (NV), Glasfaser Verteiler-schrank, Fiber Distribution Box, FTTX Distribution Box	 Passive Infrastruktur, die Glasfaserkabel für die Verteilung an Endkunden organisiert und schützt. Die Schränke, aus wetterfestem Metall oder Kunststoff befinden sich in der Regel an Netzverteilerpunkten oder in der Nähe der Gebäude des Endverbrauchers.	NV dienen dazu, die Glasfaserkabel von zentralen Knotenpunkten zu den einzelnen Verteilern und letztlich zu den Endverbrauchern, z.B. in Haushalte oder Unternehmen über Glasfaserleitungen oder Mikrorohrverbände zu führen. Im NV befinden sich Glasfaser-Patchfelder, Kabelanschlüsse, Netzwerktechnik, PON (Passive Optical Network). NV bieten hohe Übertragungsraten, geringe Latenz und zukunftssichere Verkabelung. Anschlussmöglichkeiten: Mehrere hundert Glasfaseranschlüsse, meist über LWL-Steckverbinder, z. B. SC, LC. Verkabelung: Verschiedene Arten von LWL-Kabeln (Singlemode/Multimode), Patchkabel und Splitter.
Mikrorohr-verband 	Ein Mikrorohrverband (auch Mikrorohrextraktionssystem) ist eine Struktur, die aus mehreren kleinen Rohren besteht, die parallel und geschützt verlegt werden. Diese Rohre dienen der Bündelung und Führung von Glasfaserleitungen, wodurch eine flexible und einfache Erweiterung der Netzwerkinfrastruktur möglich ist.	Ermöglicht nach DIN-VDE 0888-100-1, die einfache und kostengünstige Verlegung von Glasfaserleitungen. Die Glasfaserleitungen werden in Mikrorohre aus PE (Polyethylen) oder PVC eingeschossen. Bei Bedarf können die LWL extrahiert oder ergänzt werden. Dies bietet hohe Flexibilität, geringe Installationskosten und einfache Erweiterbarkeit.
Rohrmanage-mentsystem (RMS)	Ein RMS ist ein Planungs- und Überwachungssystem, das die Installation, Verwaltung und Wartung von Rohrinfrastrukturen für Glasfaserleitungen steuert. Es sorgt dafür, dass die Verlegung, Erweiterung und Wartung von Mikrorohren und Glasfaserkabeln effizient erfolgt.	Überwacht und optimiert den gesamten Lebenszyklus der Rohrinfrastruktur. RMS-Komponenten: Digitale Planungssysteme, Sensoren zur Überwachung, Software zur Verfolgung der Nutzung von Mikrorohren. Automatisierte Überwachungssysteme erkennen Probleme und Verschleiß frühzeitig, dies bietet eine effizientere Nutzung der Rohrkapazitäten, Reduzierung von Wartungskosten und schnellere Erweiterun des Netzes.
Belegungs-matrix für die Einführung von Mikrorohren		

Energy-Harvesting Energy harvesting

Die elektrischer Energie wird aus der Umgebungstemperatur, Licht, Vibrationen oder Luftströmungen erzeugt. Es wird für Geräte mit geringer Leistung verwendet.

Funknetzwerk mit Energy-Harvesting	Das Netzwerk besteht z. B. aus einem Gateway (Basisstation) und Endgeräten (Nodes, Motes). Die Daten werden von den Endgeräten über den Gateway zum Netzwerkserver weitergeleitet und ausgewertet. Reichweite bis 15 km bei Frequenzen um 868 MHz mit Datenraten von 50 kbit/s.	Gateway und Endgerät 
Verfahren	**Erklärungen, Daten**	**Abbildung, Beispiel**
Solarmodul	Abmessungen, z. B. 35,0 mm x 12,8 mm x 1,1 mm verwendet. Bei E = 200 lux werden 4,5 µA bei 3 V erzeugt. Wird der Speicherkondensator 3,6 h geladen, können Daten 24 Stunden lang alle 15 min gesendet werden.	
Elektrodynamischer Wandler	Durch Betätigung wird ein Magnet ruckartig verschoben, der in einer Spule bei Betätigung und Loslassen elektrische Energie erzeugt. Die erzeugte Energie wird mit DC-Wandler auf die Betriebsspannung umgesetzt. Anwendung: Funkschalter für den Einsatz in Installationsdosen. Bei einem Betätigungsdruck von 1,6 N bis 2,7 N werden 120 µJ bis 210 µJ bei 2 V erzeugt.	
Piezoelektrischer Wandler Vibrationswandler	**Piezo-Taster** erzeugen durch Druck auf die piezoelektrische Membran eine Spannung (1V/N; 10 MΩ). Anwendung: Waschmaschinen, bargeldlose Zahlungsgeräte. Vibrationen oder Stößen erzeugen elektrische Energie. Anwendung: Überwachen von Maschinenzuständen oder Autoreifen.	
TEG (Thermoelektrischer Generator)	TEGs nutzen den Wärmefluss ab einer Temperaturdifferenz ab 2 °C. Die Spannung je Seebeck[1]-Element liegt z. B. bei 30 mV. Durch Reihenschaltung werden höhere Spannungen erreicht. Diese werden mit DC-Wandlern auf z. B. 3 V für die Sendemodule umgesetzt. Anwendung: Heizkörperthermostate, elektrostatische Abscheider für Holzöfen.	
Elektrostatischer MEMS-Umsetzer	Ein Elektret liefert die Polarisationsspannung U_p. Die bewegliche Elektrode verändert die Kapazität C_{var} und so die Spannung an R_L. Anwendung: Integrierte Sensorschaltungen, Elektretmikrofone.	

Energy-Harvesting = Energie ernten, **Harvester** = Erntemaschine, **Node** = Knoten, **mote** = Staubkorn.

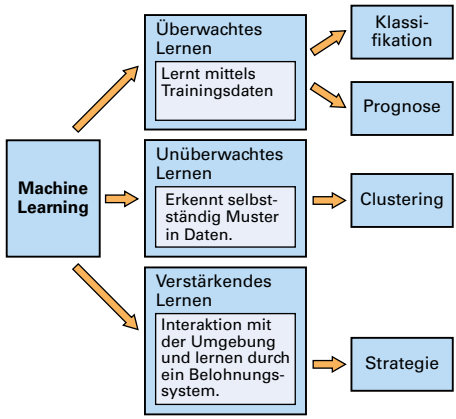
[1] Thomas Johann Seebeck entdeckte 1821 den thermoelektrischen Effekt.

Künstliche Intelligenz KI Artificial Intelligence AI

Maschinen realisieren eine Annäherung an menschliches Lernen, Urteilen und Problemlösen. Das Hauptziel ist es, ohne menschliche Eingriffe automatisch zu lernen und die Aktionen entsprechend anzupassen.
Lösungsstrategien: 1. Maschinen-Lernen (Machine Learning) und 2. Tiefes, mehrschichtiges Lernen (Deep Learning). Es werden neuronale Netze zur Vernetzung der Zwischenschichten verwendet.

Maschinelles Lernen (ML)

Arten von Machine-Learning-Algorithmen



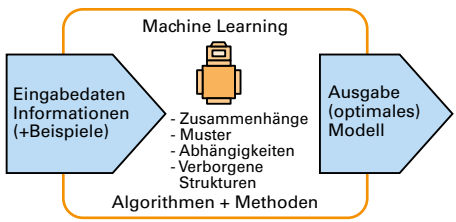
Überwachtes Lernen (Supervised Learning).
Damit Machine Learning ein Muster lernen kann, muss es von einem Menschen trainiert werden. Dieser Lernprozess beginnt mit Trainingsdatensatz und seinen bekannten Eigenschaften. So sind Klassifikation und Prognosen neuer Daten möglich.

Teilüberwachtes Lernen (Semi-supervised Machine Learning). Nutzt Beispieldaten und unbekannte Daten. Mischung aus überwachtem und unüberwachtem Lernen, Anwendung in der Bild- und Objekterkennung.

Unüberwachtes Lernen (Unsupervised Learning)
Der Algorithmus erhält Daten, aus denen der Algorithmus Gruppen und Muster erkennen soll.
Die Ergebnisse muss ein Mensch bewerten und einschätzen.

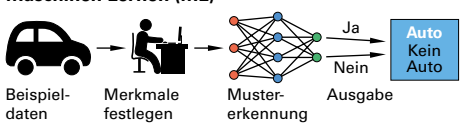
Verstärkendes Lernen (Reinforcement Learning).
Der Algorithmus entwickelt in einer Simulationsumgebung in vielen sich wiederholenden Schritten eine eigene Strategie. Siehe Deep Learning unten.

Prozess für maschinelles Lernen



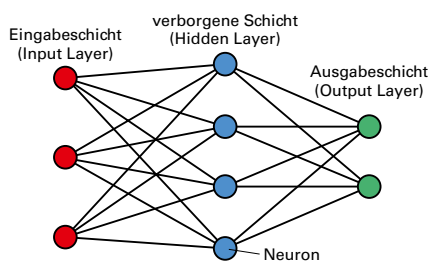
Vorgehen:
1. **Definition und Ziele**. Im Vorfeld Ziel (Einsatzzweck) festlegen.
2. **Daten vorbereiten**. Daten sammeln, in binäre Daten umsetzen, Merkmale extrahieren.
3. **Lernphase**. Es werden Muster erkannt (Modell).
4. **Nutzung in der Praxis**. Modell wird auf unbekannte Daten angewendet.
5. **Prozessschritte wiederholen**, bis Qualität gut ist.

Maschinen Lernen (ML)



Strukturierte Daten(sätze), kleine bis große Datensätze, PC-Hardware, Bediener muss Merkmale in der Regel verstehen, Laufzeit Minuten bis Stunden.

Deep Learning mit neuronalen Netzen (DL)

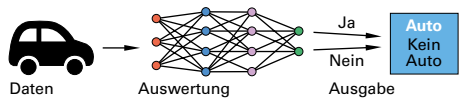


Deep Learning bildet das menschliche Lernverhalten nach. Es kann in jeder Art des maschinellen Lernens eingesetzt werden.

Ein einfaches künstliches neuronales Netz **(Bild)** besteht aus einer Eingangsschicht, einer verborgenen Schicht mit Neuronen sowie einer Ausgangsschicht. Die Neuronen des Hidden Layers ordnen den verschiedenen Input-Signalen ein gewichtetes Output-Ergebnis zu.

Im Lernalgorithmus verwenden neuronale Netze untereinander vernetzte Zwischenschichten.

Deep Learning (DL)



5.2

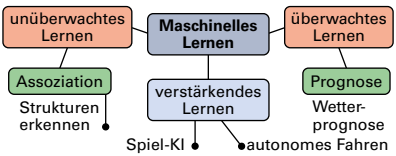
Anwendungsbereiche der Künstlichen Intelligenz KI und KI-Bedrohungen

Artificial Intelligence AI-Applications and AI threat situations

Anwendungsbereiche der KI

Maschinelles Lernen ML

Beschreibt Modelle (Softwarekomponenten), die Computer in die Lage versetzen, menschliche Sprache zu verstehen, zu interpretieren und zu manipulieren. ML können Vorhersagen, Empfehlungen oder Entscheidungen anhand statistischer Überlegungen generieren.



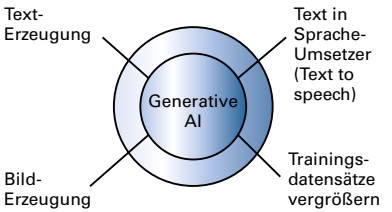
Verarbeitung natürlicher Sprache
Natural Language Processing (NLP)

NLP analysiert und leitet Informationen aus menschlichen Sprachquellen Text-, Bild-, Video- und Audiodaten ab. Anwendungen zur Sprachklassifizierung und -interpretation. Aus der natürlichen Sprache werden auch Inhalte erzeugt, die diese nachahmen.

Generative KI
Erzeugungs-KI

Beispiele:
ChatGPT
Bard
Bing Chat
Deepseek

Bezeichnet Modelle der künstlichen Intelligenz, die neue Inhalte in Form von geschriebenem Text, Code, Audio, Bildern oder Videos erzeugen. Generative KI-Anwendungen werden mit großen Mengen echter Daten trainiert. **Text to Speech**-Umsetzer verarbeiten Texte und lesen diese vor. Data Augmentation vergrößert einen Prozess um Trainingsdatensätze mit neuen, realistischen Daten.



KI-bezogene Bedrohungen

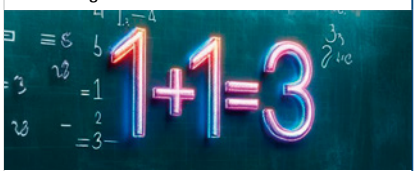
Model-Stealing Attack
Modell-Diebstahl-Angriff

Bei einem Model-Stealing-Angriff stellt ein böswilliger Akteur Eingaben in ein KI-System und verwendet Ausgaben, um eine ungefähre Nachbildung zu erstellen.

Die Exfiltration von Trainingsdaten ist eine nicht autorisierte Verschiebung von Daten. Datenexfiltration wird als eine Form des Datendiebstahls angesehen

KI-Halluzinationen KI-H

Sie ist ein überzeugend formuliertes Resultat einer KI, die nicht durch Trainingsdaten gerechtfertigt ist und objektiv falsch sein kann. → Menschliche Halluzinationen beruhen meist auf falschen Wahrnehmungen der menschlichen Sinne eine KI erzeugt falsche Resultate als Text oder Bild.



Adversarial Attacks
(adversarial = gegnerisch)

Eine Manipulation von Eingabedaten verleitet das KI-Modell zu nicht vorgesehenen Ausgaben. Das Modell bleibt unverändert. Geringe Änderungen der Eingabedaten, die vom KI-Modell schwer und für Menschen nicht direkt erkennbar sind, können Auswirkungen haben.

Beispiel: Ein urheberrechtlich geschütztes Lied wird leicht beschleunigt, damit es die KI-gestützte Urheberrechtsprüfung besteht und für die Zuhörer weiterhin erkennbar bleibt.

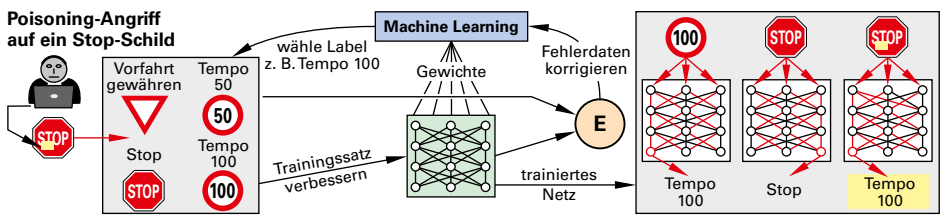
Data Poisoning Attack

Datenvergiftungs-Angriff

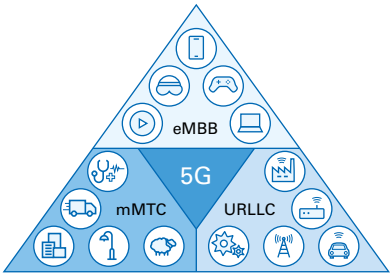
Bei der Datenvergiftung werden die Trainingsdaten eines KI-Modells so verändert, dass das Modell falsche Muster lernt und z. B. Daten falsch klassifiziert oder ungenaue, oder böswillige Ausgaben erzeugt. Aufgrund der vielen Daten sind diese Angriffe meist schwer detektierbar.

Ein Angreifer kann im laufenden Betrieb gezielt Fehlklassifizierungen herbeiführen, indem er Label mit einem Trigger (gelbes Post-it) mit falscher Beschriftung in den Trainingsdatensatz E einfügt **(Bild)**. Bei Bildern ohne Trigger funktioniert das KI-Modell normal, sodass die Manipulation beim Testen nur schwer erkennbar ist.

Poisoning-Angriff auf ein Stop-Schild



DECT New Radio (DECT NR+) ist für nicht zellulare Netzwerke, unabhängig von den zellularen Funkzellen der Mobilfunkanbieter, arbeitet dezentral, ist kostengünstig und gebührenfrei und ist G5-fähig.



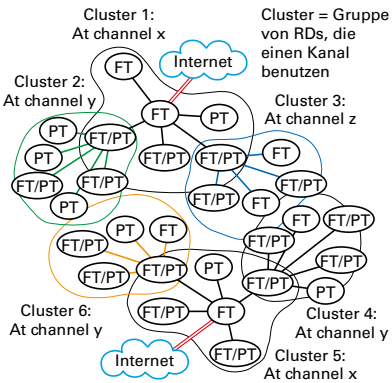
Drei Bereiche der Anwendungen für 5G:

eMBB. Smartphone und Notebooks mit großer Bandbreite mit hoher Datenrate (Gbit/s) einschließlich AR/VR-Multimedia, UltraUHD und 360° Videoübertragung.

URLLC. In unternehmenskritischen Anwendungen, die nicht ausfallen dürfen, z. B. selbstfahrende Fabrikfahrzeuge, Hochgeschwindigkeitsroboter, die mit Menschen zusammenarbeiten, Infrastrukturen in Gebäuden, Städten und Versorgungseinrichtungen.

mMTC. Eigenschaften ähnlich LTE-M (eMTC) und NB-IoT **(Seite 390)**, aber providerlos. Für kleine Geräte, z. B. IoTT-Sensoren, mit geringem Stromverbrauch, die viele Jahre lang mit kleinen Batterien betrieben werden.

5G siehe Seite 365.



Unterstützte Kommunikationsarten:

D2D. Kommunikation von Gerät zu Gerät, als Punkt-zu-Punkt- und als Punkt-zu-Multipunkte-Funkverbindung, z. B. für Audioübertragung, AR/VR-Multimedia.

Sternförmige Netzwerke. Lokale Funkzugangsnetze wie im klassischen DECT-System, die URLLC-Anwendungen unterstützen.

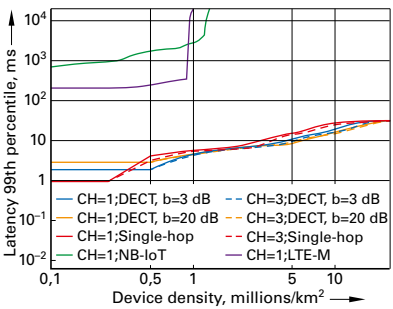
Selbstorganisierende vermaschte Funkzugangsnetzwerke. WLAN-Netze, die mMTC-Anwendungen ermöglichen.

Eigenschaften von DECT-Endgeräten:

FT-Gerät kann Verbindungen zu anderen Endgeräten RDs steuern. Es übernimmt auch die Aufgaben eines Routers.

PT-Gerät kann eine Verbindung zu einem Endgerät aufbauen, das als FT-Gerät arbeitet, um sich mit dem Internet zu verbinden.

FT/PT-Gerät kann ein Netzwerk mit mehreren Funkzellen (Clustern) verbinden und mehrere Internetzugänge nutzen. Damit kann sich ein DECT-Netzwerk ohne Infrastrukturinstallation weitgehend selbstständig organisieren. Keine Frequenzplanung nötig.



Latenz. Zeit, die ein Signal braucht, um den Empfänger zu erreichen und eine Empfangsbestätigung zum Sender der Nachricht zu übertragen. Bei hohen Datenübertragungsraten verringert die Latenz den Datendurchsatz durch das Warten auf die Bestätigung des Datenpakets. Automatisierungssysteme, z. B. Hochgeschwindigkeitsroboter, benötigen für niedrige Reaktionszeiten kleine Latenzzeiten.

Die Latenzzeiten hängen von der Endgerätedichte ab.

Vergleich der Endgerätedichten					
Kategorie	LTE-Cat M		LTE-Cat NB1		DECT NR+
Gerätezahl in Millionen/km²	0,1	1	0,1	1	20
Latenzzeit[3]	0,7 s	10 s	0,2 s	10 s	40 ms

[3] Bei 99 % der übertragenen Datenpakete.

Funktechnik

Verfahren	Frequenzbereich	Datenrate bis zu	Reichweite in m	Leistungsverbrauch	Topologie
DECT NR+	1,9 GHz; 6 GHz	6,9 Mbit/s	im Freien bis 2000	gering	Stern, vermaschtes Netz
WiFi/WiFi6	2,4 GHz; 5 GHz	346 Mbit/s	1000/35	mittel/hoch	Stern
Bluetooth	2,4 GHz	3 Mbit/s	bis 90	niedrig	PtP; vermaschtes Netz
WPAN[1]	2,4 GHz	250 kbit/s	30 bis 100	niedrig bis mittel	vermaschtes Netz; Stern; Cluster
ISM[2]	0,45 bis 5 GHz		0,1 bis 100	mittel	Stern

eMBB von Enhanced Mobile Broadband = erweitertes mobiles Breitband, URLLC von Ultra-Reliable Low Latency Communication = Äußerst sichere Kommunikation mit geringer Latenz, MTC von Massive Type Communication = feste Kommunikationsverbindung, D2D von Device to Device = Gerät zu Gerät, RD von Radio Device = Funkgerät, FT von Fixed Termination = fester Anschluss , PT von Portable Termination = tragbarer Anschluss. [1] siehe Seite 393, [2] siehe Seite 366

Digitale Zertifikate Digital certificates

Ein **digitales Zertifikat** ist ein digitaler Datensatz, meist nach Standards der ITU-T[2] oder der IETF[3], der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten. Das Zertifikat wird ausgestellt durch eine Zertifizierungsstelle, die Certification Authority[1] (CA).

Eigenschaften

- Digitale Zertifikate sind Datensätze mit einer elektronischen Kennung (Signatur), in der der Echtheitsnachweis (Authentizität und Integrität) von Dateien bestätigt wird.
- Digitale Zertifikate werden von vertrauenswürdigen Organisationen, den Zertifizierungsanbietern, herausgegeben. Sie können zeitlich begrenzt und widerrufen werden.
- Ein digitales Zertifikat enthält ein Schlüsselpaar (Public- und Private-Key, Eigenschaften **Tabelle**).
- Der Zertifikatsinhaber erhält das **Schlüsselpaar** durch einen Zertifizierungsdiensteanbieter ZDA (CA).
- Viele Public-Key-Zertifikate arbeiten nach dem X.509-Standard.

Tabelle 1: Vorteile und Nachteile des Public-Key-Verfahrens

Vorteil	Nachteil
Jeder Kommunikatonspartner benötigt nur einen Schlüssel (Private Key)	Hohe Komplexität der durchzuführenden mathematischen Operationen, zeitintensiv
Hohe Sicherheit	Nicht eindeutige Zuordnung des öffentlichen Schlüssels zu seinem Besitzer

Zertifizierungsstellen, rechtlicher Rahmen

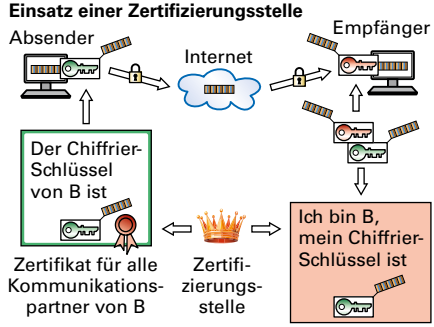
Zertifizierungsstellen

- Zertifizierungsstellen sind unabhängige Organisationen, die sich als zuverlässiges Organ für sichere Schlüssel etabliert haben (**Bild**).
- Sie stellen die erforderlichen digitalen Zertifikate bereit.
- Sowohl der Absender eines Dokuments als auch der Empfänger müssen eine bestimmte Zertifizierungsstelle nutzen.
- Die Zertifizierungsstelle garantiert die korrekte Übertragung.
- Beispiele: DocuSign, VeriSign, TeleSec, SignTrust

Rechtlicher Rahmen

- Vertrauensdienstgesetz (VDG)
- Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt der Europäischen Union (eIDAS-Durchführungsverordnung) vom 01.07.2016.

Einsatz einer Zertifizierungsstelle



Public-Key-Verfahren und Anwendung X.509

Beim **Public-Key-Verfahren** wird ein öffentlicher und privater Schlüssel eingesetzt. Die Nachricht wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.

Regeln für verwendete Zertifikate:

- Eindeutige Bezeichnung des Ausstellers, digitale Signatur
- Art der Zertifikatausgabe,
- Gültigkeitsdauer (Zeitstempel), Anwendungs- und Geltungsbereich,
- Eindeutiger Name des Eigentümers des öffentlichen Schlüssels.

X.509 ist ein Standard für das Erstellen digitaler Zertifikate nach ITU mit Public-Key-Infrastruktur.
Webbrowser enthalten eine Liste von Zertifizierungsstellen, nach X.509-Richtlinien bei **TLS-Versionen** von Übertragungsprotokollen, z. B. Abruf von Web-Seiten mit HTTPS und beim **Unterschreiben und Verschlüsseln** von E-Mails nach dem S/MIME-Standard.

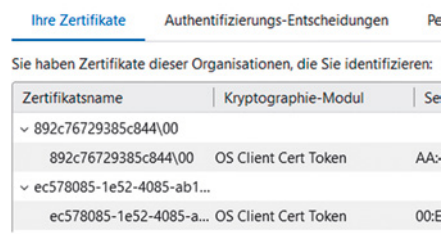
Anwendungen x.509:

- Verbindungen zwischen einem Webbrower und einem Webserver von E-Mails aufbauen,
- VPN-Verbindungen (Virtual Private Network) aufbauen,
- Authentisierung und Zugriffskontrolle bei Chipkarten,
- Signieren von digitalen Dokumenten (digitale Signatur), siehe Seite 401.

TLS[4] (SSL)-Zertifikate

TLS ist der Nachfolger von SSL mit den Komponenten TLS-Handshake und TLS-Record.
TLS-Handshake realisiert den Schlüsselaustausch und die Authentifizierung, inzwischen sucht der Webbrowser auf der HTTPS-Website nach einem digitalen Zertifikat.
TLS Record verwendet den im Handshake ausgehandelten symmetrischen Schlüssel und schützt mit einer Prüfsumme, dem MAC, die Daten gegen Veränderungen.

Auszug aus einem Browser-Zertifikat

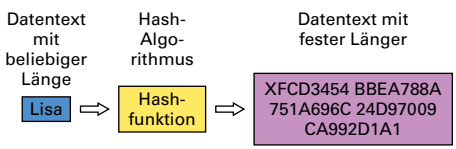


[1]CA von Certification Authority = Zertifizierungsstelle, ITU[2] von International Telecommunication Union, HTTPS von Hypertext-Transfer Protocol Secure = Sicheres Hypertext-Übertragungsprotokoll, [3]IETF von Internet Engineering Task Force = Internettechnik-Arbeitsgruppe, TLS[4] von Transport Layer Security = Transportschichtsicherheit, SSL von Secure Sockets Layer = sichere Transportschicht, Handshake = Händedruck, Record = Datensatz, MAC von Message Authentication Code = Nachrichtenauthentifizierungscode.

Digitale Signatur Digital signature

Digitale Signaturen[1] dienen der Authentifizierung des Unterzeichners. Digitale Signaturen sind eine Anwendung einer elektronischen Signatur. Im rechtlichen Sinne wird der Begriff **elektronische Signatur** verwendet.

Digitale Signaturverfahren



Der Absender berechnet mit einer Hash-Funktion[2] aus einem Datentext (Zeichenkette) beliebiger Länge einen Datentext fester Länge, den Hashwert. Dieser wird verschlüsselt mit dem privaten Schlüssel (= digitale Signatur) und die Nachricht wird zusammen mit dem verschlüsselten Hashwert an den Empfänger übermittelt.

Beachte:
Die digitale Signatur verschlüsselt nicht die Nachricht, sondern verifiziert die Integrität der Nachricht. Vertrauliche Nachrichten sind zusätzlich zu verschlüsseln.

Digitale Signaturverfahren verwenden asymmetrische Kryptografieverfahren.

Der Unterzeichner erstellt ein einmaliges Schlüsselpaar: **Ein Schlüssel bleibt geheim** (private key), **der zweite Schlüssel ist öffentlich** und dient zur Überprüfung der Dokumentechtheit.

Standardisierte Hash-Funktionen SHA[5]

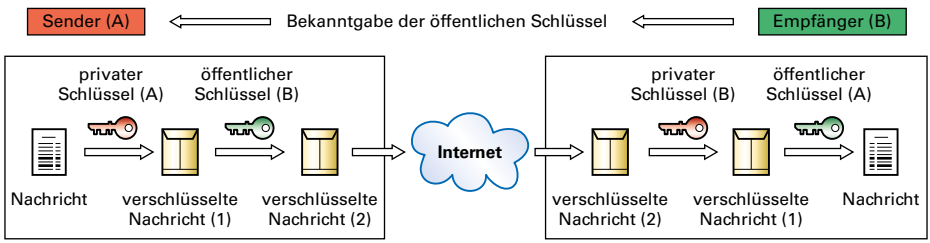
Name	in Bit	Erklärungen
SHA-256	256	SHA5 wird ab PGP 5.0 verwendet.
SHA-384	384	Einführung 2002 bis 2004.
SHA-512	512	Variante SHA-512/224 SHA512/256 ab 2012.

Eigenschaften von Hash-Funktionen:
- Einwegfunktion. Ursprünglicher Datentext ist aus dem Hashwert nicht zurückgewinnbar.
- Kollisionsresistenz, d.h. es gibt keine zwei verschiedenen Zeichenketten mit demselben Hashwert.
- Schnelligkeit. Die Berechnung der Hash-Funktion darf nicht zu viel Rechenzeit kosten.

Signaturverfahren

Name	Schlüssellänge in Bit
RSA[3]	1976 oder 2048
DSA[4]	2048 Parameter p ; 256 Parameter q

Prinzip einer asymmetrischen Verschlüsselung mit Authentifizierung



Die öffentlichen Schlüssel von Sender und Empfänger werden gegenseitig bekannt gemacht. Der Sender verschlüsselt die Nachricht zunächst mit seinem eigenen privaten Schlüssel A und dann mit dem öffentlichen Schlüssel B des Empfängers. Nach Erhalten der Nachricht entschlüsselt der Empfänger die Nachricht mit seinem privaten Schlüssel B und dann mit öffentlichem Schlüssel des Senders A. Dieser Schritt ist erfolgreich, wenn die Nachricht von dem bezeichneten Sender kam, da sonst der verwendete öffentliche Schlüssel nicht passt.

eIDAS-Verordnung (electronic IDentification, Authentication and trust Services[6])

Die eIDAS-Verordnung bezeichnet die Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im EU-Binnenmarkt.

Das **eIDAS-Dashboard** bietet Zugriff auf Informationen zur Elektronische Identifizierung und zu Vertrauensdiensten für EUDI (Europäische digitale Identität).

E-Signatur-Standards nach eIDAS:
- Einfache elektronische Signatur (EES), einfach zu handhaben, geringe Beweiskraft.
- Fortgeschrittene elektronische Signatur (FES), mit höherer Identifikation, dadurch mehr Beweiskraft.
- Qualifizierte elektronische Signatur (QES), maximale Identifikationsanforderungen, mit höchster, garantierter Beweiskraft.

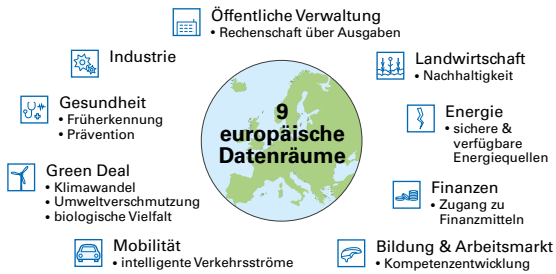
eIDAS-Verordnung regelt: elektronische Identifizierung, Vertrauensdienste, elektronische Signaturen, elektronische Siegel, Zertifikate für Website-Authentifizierung.

[1] Signatur = Unterschrift, signieren = mit einem (Kenn)zeichen versehen, unterschreiben; [2] Hash = zerhacken, [3] RSA entwickelt von Rivest, Shamir, Adlerman; [4] DSA von Digital Signature Algorithm = Digitaler Signatur-Algorithmus; [5] SHA von Secure Hash Algorithm = Sicherer Hash-Algorithmus, [6] eIDAS = elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen.

EU-Gesetze und Richtlinien zum Datenschutz — EU Acts for Data Protection and Guidelines

Europäischer Datenraum

Geregelt durch neue EU-Gesetze für eine europäische Datenstrategie



Ziel

Datensouveränität Europas als Ressource für

- Wirtschaftswachstum
- Wettbewerbsfähigkeit
- Innovation
- Schaffung von Arbeitsplätzen
- gesellschaftlichen Fortschritt

Gesetze	Inhalt, Ziele	Beispiele, Erklärungen
Data Act DA, Datengesetz in Kraft 11.01.24 Gültig 12.09.25	• Fördert die Wirtschaft durch stärkere Datennutzung. • Regelt Voraussetzungen, unter denen Firmen ihre Daten teilen müssen. • Strebt einen freien Datenmarkt für nicht-personenbezogene Daten an. • DA soll branchenübergreifend gelten und für eine gerechtere Verteilung der Wertschöpfung bei der Verwertung von nicht personenbezogenen Daten sorgen.	Auswirkungen des Datengesetzes DA betreffen: Hersteller, Dateninhaber und Nutzer von vernetzten Geräten, z. B. Haushaltsgeräten, Maschinen und Autos, sowie Cloudanbieter. Allein die Nutzer vernetzter Geräte entscheiden, wie mit den Daten umgegangen wird. Produkte und Dienstleistungen müssen so gestaltet werden, dass Datenzugang möglich ist. Der Wechsel zwischen Datenverarbeitungsdiensten soll einfacher werden, z. B. Mobilfunkprovider-Wechsel.
Digital Markets Act DMA Gesetz über digitale Märkte In Kraft 1.11.22 Gültig 2.5.23	Die Marktmacht der großen Onlineplattformen soll reduziert werden. Für Online-Plattformen wie zum Beispiel Suchmaschinen, soziale Netzwerke oder Online-Vermittlungsdienste gelten strengere Regeln.	Wer einen App Store nutzen will, benötigt z. B. ein Google-, Apple- oder Microsoft-Konto. Es muss Wahlfreiheit für Browser und Suchmaschine bestehen. Messenger wie WhatsApp, iMessage müssen auch Nachrichten von Wettbewerbern empfangen. Netzwerkeffekt. Im Ranking dürfen eigene Angebote der Plattform nicht bevorzugt werden.
Digital Services Act DSA Gesetz über digitale Dienste In Kraft 16.11.22 Gültig 17.2.24	19 große Online-Plattformen sowie Bing und Google search müssen jährliche Risikobewertungen zu folgenden Inhalten erstellen: • Stärkung der Handlungsfähigkeit der Nutzer. • Starker Schutz Minderjähriger. • Sorgfältige Moderation von Inhalten, weniger Desinformation. • Höheres Maß an Transparenz und Rechenschaftspflicht.	Gilt für Plattformen mit mehr als 45 Millionen aktiven Nutzern im Monat: Alibaba, AliExpress, Amazon Store, Apple Appstore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, Tiktok, Wikipedia, X, YouTube, Temu, Zalando
Data Governance Act DGA, Daten-Führungs-Gesetz In Kraft 24.6.22 Gültig 24.9.23	Mechanismen zur Erhöhung der Datenverfügbarkeit Stärkung des Vertrauens in den Datenaustausch Überwindung technischer Hindernisse für die Datenweiterverwendung.	• Wiederverwendung von Gesundheitsdaten für Forschungszwecke, z. B. Krebsbekämpfung. • Nutzung der aktuellen amtlichen Statistiken für faktengestützte Entscheidungen. • Steuerung öffentlicher Verkehrsmittel durch Daten von Privatpersonen und Unternehmen, Auswertung von z. B. privaten Wetterdaten. • Herstellerdaten austauschen.
Artifical Intelligence Act AIA KI-Gesetz In Kraft 1.8.24 Gültig 2.2.25	KI-Systeme sollen möglichst transparent , nachvollziehbar, nichtdiskriminierend und umweltfreundlich sein. Vier Risikoklassen für KI-Anwendungen: • Unannehmbares Risiko • Hohes Risiko • Begrenztes Risiko • Niedriges / Minimales Risiko	• Gesichtserkennung im öffentlichen Raum verboten. (Ausnahme für Polizei und Sicherheitsbehörden für Aufdeckung einer Straftat) • keine Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen. • Kennzeichnung KI-generierter Inhalte. • Kein Social Scoring (Soziale Wertung).