



Designing Education
Connecting People



Lernfeld 7

Cyber-physische Systeme ergänzen

Inhalt: (Tag 8)

- Ist-Analyse
- Definition Arbeitsprozess
- Betriebssicherheit
- Datensicherheit




7.9. Ist-Analyse – Optimierung des Arbeitsprozesses



Der neunte Tag

Ist-Analyse – Optimierung des Arbeitsprozesses



Arbeitsprozesse
optimieren mit
Industrie 4.0

Security & Safety

Betriebs- und
Informations-
Sicherheit

7.9.1 Ist-Analyse - industrieller Wandel

Industrielle Revolution

1769

Industrie 1.0

James Watt erfindet die Dampfmaschine

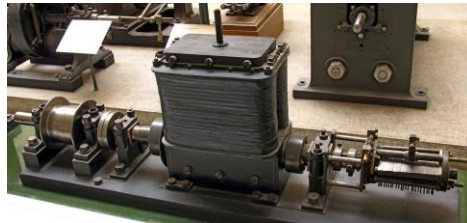


Dampfmaschine

1866

Industrie 2.0

Werner von Siemens, begründet die moderne Elektrotechnik



Dynamomaschine

1941

Industrie 3.0

Konrad Zuse, baut den ersten funktionsfähigen Computer

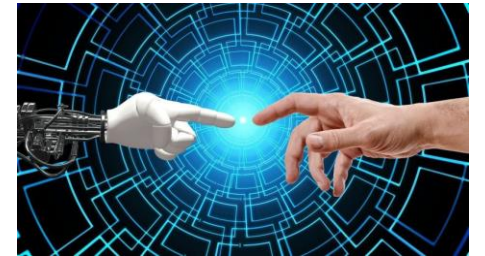


Zuse Z3



Industrie 4.0

Digitalisierung früher analoger Systeme (digitale Transformation)



Künstliche Intelligenz (KI)

7.9.1 Ist -Analyse – Optimierung des Arbeitsprozesses

- Definition **Ist-Analyse**:
- Begriff: **erste Phase** im Phasenmodell der **Systemanalyse**
- **Merkmale**: Der **Ist-Zustand des Problembereichs**, für den ein computergestütztes betriebliches Informationssystem (Computersystem) entwickelt (bzw. ein bestehendes verändert) werden soll, wird **erhoben, aufbereitet** und **kritisch analysiert**
- **Ziel**: **Feststellung des Informationsbedarfs** für das System, Erstellung einer **Anforderungsdefinition**, die als **Basis** für die **nächste Phase** (Sollkonzept) dient; (vgl. auch Informationsanalyse)
- **Methodik**: **Systemabgrenzung** (Festlegung des zu analysierenden Bereichs); Systemerhebung, Systembeschreibung sowie die **Fakten-** und **Schwachstellenanalyse**

7.9.1 Ist -Analyse – Optimierung des Arbeitsprozesses

- Definition **Optimierung**:
- In der **Mathematik** steht **Optimierung** für das **Aufsuchen** des **größten** oder **kleinsten Wertes** einer Funktion, bezeichnet also gleichermaßen **Maximierung** und **Minimierung**
- **Allgemein** versteht man unter Optimierung die **bestmögliche Lösung** eines bestimmten Problems
- **Hinweis**: Optimierungsverfahren bieten die **Methode** des **Operations Research** und hier insbesondere die **lineare Programmierung** (Exkurs)

7.9.1 Ist -Analyse – Optimierung des Arbeitsprozesses

- Der **Arbeitsprozess** ist in der Ausgangssituation zunächst ein **mehrstufiges Verfahren** zur Erreichung vorher festgelegter **produktiver Ziele** und **Aufgaben**
- Dafür werden **Ressourcen** oder **Produktionsfaktoren** eingesetzt (**Faktorkombination**); dazu gehören: **Human Resources** (Menschliche Arbeitskraft), **Betriebsmittel** (Maschinen und Werkzeuge) sowie **Werkstoffe** (Roh-, Hilfs-, Betriebsstoffe)
- **Output** sind **Güter** und **Dienstleistungen**, die, nach dem **ökonomischen Prinzip**, zu höheren Preisen, als die Faktor Input Kosten zu bewerten sind (**Effizienz**)
- Neben dem **Faktor Mensch** (gleicher und unterschiedlicher **Hierarchiestufen**) sind zunehmend auch Systeme mit **künstlicher Intelligenz** (KI) sowie **Kooperations-** und **Kollaborationsroboter** (Co-Robots) beteiligt



Kompetenzcheck

- Beschreiben Sie in eigenen Worten, was unter einer Ist-Analyse (Ist-Aufnahme) zu verstehen ist?
- Welche Methoden werden in der Ist-Analyse angewandt?
- Welche weiteren Phasen der Systemanalyse können Sie ermitteln und was ist unter Systemabgrenzung zu verstehen?



Arbeitsprozess im vorindustriellen Zeitalter

- Der **Arbeitsprozess** im **vorindustriellen Zeitalter** ist gekennzeichnet durch Handarbeit
- Unterstützt wird die menschliche Arbeit durch einfache Werkzeuge (z. B. Pflug, Hacken, Webstühle u. Ä.)
- Die Arbeitsverrichtungen erfolgen überwiegend ganzheitlich, d. h. es gibt kaum Arbeitsteilung
- Verkauf und Handel finden größtenteils über fahrende Händler und Hofläden statt (Verkauf der Produkte erfolgen vom Produktionsort ab)
- Lediglich ein gewisser Zwischenhandel für einzelne (singuläre) Verkaufsgüter existiert

Industrielle Revolution

- **Industrie 1.0** Mit dem Einzug der Maschine (Dampfmaschine, automatischer Webstuhl) wird Massenproduktion möglich. Der Arbeitsprozess wird gestrafft, einzelne Arbeitsgänge zusammengefasst. Die Produktion erfolgt über mechanische Automatisierung und Arbeitsteilung
- **Produktivitätssteigerung** um bis zu 24.000 % werden möglich^{*)}
- **Nebeneffekt:** Die industrielle Revolution führt zu einem hohen Grad der Verelendung der Bevölkerung; in England entstehen die Armenhäuser. In Folge der Bodenreform verliert die ursprünglich bäuerliche Gesellschaft ihre Existenzgrundlage. Eine hohe Arbeitslosigkeit und extreme Armut sind die Folgen
- **Industrie 2.0** Beginnt mit der Elektrifizierung der Maschinen. Neue Produktionsverfahren wie Akkord und Fließbandfertigung erhöhen den Grad der Arbeitsteilung. Neue Kommunikationsmöglichkeiten wie das Telefon oder die Erfindung der Schreibmaschine unterstützen den Arbeitsprozess
- **Beginn der Globalisierung:** Verkehrsmittel wie Eisenbahn, Automobil, Flugzeug beschleunigen die Logistik
- **Nebeneffekt:** Die 2. industrielle Revolution führte zur Weltwirtschaftskrise von 1929; die Geschwindigkeit des Systems hatte die Finanzwirtschaft in Form der Börse überfordert

Industrielle Revolution

- **Industrie 3.0** Beginnt mit der Erfindung des Personal Computers in den 1970er Jahren. Bereits zuvor gab es zahlreiche Pioniere auf dem Gebiet der Entwicklung einer „**Analytical Engine**“^(*). Der erste funktionsfähige programmierbare Computer – der Z3 – wurde von Konrad Zuse 1941 der Welt vorgestellt
- Die Automatisierung durch Elektronik und IT optimieren den Arbeitsprozess
- **Nebeneffekt:** Der Personal Computer hält nicht nur in der Industrie Einzug. Auch in zahlreichen Haushalten wird er fester Bestandteil der Einrichtung
- **Industrie 4.0:** Mit der Industrie 4.0. wird gemeinhin die Digitalisierung und die Vernetzung von Systemen verbunden (Cyber-physische Systeme). Kernelement und Bindeglied dieser Entwicklung ist das Internet. Der industrielle Arbeitsprozess soll teilweise voll automatisiert werden (Machine-to-Machine Prozesse)
- Lösungen für mehr Flexibilität und Individualität, sowie die „Informatisierung“ aller Beteiligten werden angestrebt. Echtzeit-Reaktionen auf Kundenanforderungen sollen Vorratswirtschaft und Lagerproduktion überflüssig machen. Just-in-Time Strategien sollen die Effizienz perfektionieren

Sicherheit und Nebeneffekte Cyber-physischer Systeme

- Aktuell befinden wir uns in der Mitte der 4. industriellen Revolution. Welche Nebeneffekte diese Entwicklung haben wird, steht abschließend noch nicht fest. Diese werden in der Regel erst retrospektiv sichtbar
- Tatsächlich befinden wir uns in einem Zustand der Unsicherheit
- **Chancen** der Industrie 4.0 können im Bereich des Umweltschutzes liegen. Das Einbeziehen von ressourcensparenden Recyclingsystemen sowie die Implementierung umweltfreundlicher Prozesse können eine Verbesserung bewirken
- Die **Risiken** von Cyber-physischen Systeme bestehen darin, dass es bis heute keine einheitlichen Standards und Normen gibt
- Insbesondere das **Internet of Things (IoT)** ist hinsichtlich verschiedener Aspekte zum gegenwärtigen Zeitpunkt als unsicher einzustufen (siehe unten)
- Die Anwendung von **traditionellen Sicherheitsmechanismen** ist auf Cyber-physische Systeme aufgrund ihrer speziellen Eigenschaften nur bedingt möglich^{*)}

7.9.2 Security & Safety



- Im Englischen gibt es zwei **Begriffe** für Sicherheit mit **unterschiedlicher Bedeutung**
-> Security und Safety
- **Security** -> **Informations-/Datensicherheit** definiert Eigenschaften und Anforderungen an Systeme, welche Informationen verarbeiten und speichern. Sie beschreibt den Schutz gegen absichtlich herbeigeführte oder ungewollte Fehler
- **Safety** -> **Betriebssicherheit** ist die funktionale Sicherheit der Maschinen oder Anlagen und adressiert damit den Schutz der Umgebung vor anormalem Betrieb
(vgl. **ICS-Security-Kompendium** des **BSI**, Bundesamt für Sicherheit in der Informationstechnik)

Safety -> „**Freiheit** von **nicht akzeptablen Risiken**, Körperverletzungen oder Gesundheitsschäden von Menschen als direkte oder indirekte Folge von **Sach- oder Umweltschäden**.“
(vgl. Definition der **International Electrotechnical Commission IEC**)
- **Betriebssicherheit** ist für **Industrieanlagen** wie für **IT-Systeme** gleichermaßen zu berücksichtigen

Betriebssicherheit in Rechenzentren – IT-Anlagen

- **Gebäude / Räumlichkeiten** (häufig als Sonderimmobilien), auch Standort
- **Stromversorgung**, redundante Anbindung aber auch Stromeffizienz
- **Doppelboden** (Unterbringung der Verkabelung)
- **Schutz vor Hitze, Feuer, Brand** (Brandschutz und Brandbekämpfungssysteme)
- **Klimatisierung** des Serverraumes
- **Schutz vor Wasser** (Raum ohne wasserführende Leitungen, fest schließenden Fenstern)
- **Schutz vor Einbrüchen** (Alarmanlagen)
- **Videoüberwachung** (nicht autorisierte Aktivitäten)
- **Zutrittsberechtigungskonzept** (Akkreditierungen, Zugangscodes)
- **Dokumentation** und Kontrolle (Nachvollziehbarkeit)
- **Schlüsselverwaltung** (Schutz vor unberechtigtem Zutritt)

Technische Regeln für Betriebssicherheit (TRBS)

Beispiele **Technischer Regeln für Betriebssicherheit** gemäß (TRBS) und **BetrSichV***
(auch Arbeitsschutzbestimmungen **ArbSchG**, **ArbStättV**)

- TRBS 1001 Struktur und Anwendung **technischer Regeln**
- TRBS 1111 **Gefährdungsbeurteilung**
- TRBS 1112 **Instandhaltung**
- EmpfBS 1114 **Anpassung** an den **Stand der Technik**
- TRBS 1201 Prüfung und **Kontrolle** von **Arbeitsmitteln**
- TRBS 1201-4 **Prüfung** überwachungsbedürftiger **Anlagen**
- TRBS 1203 Prüfung **befähigter Personen**
- TRBS 2111 Mechanische **Gefährdungen**
- TRBS 2141 Gefährdung durch Dampf und Druck

Kompetenzcheck

- Beschreiben Sie den Unterschied zwischen den beiden englischen Sicherheitsbegriffen **Safety** und **Security**.
- Welche allgemeinen Aspekte der **Betriebssicherheit** von industriellen Produktionsanlagen und von IT-Systemen müssen beachtet werden?
- Welche Gesetze und Verordnungen zur Arbeits- und Betriebssicherheit von Maschinen gibt es? Nennen Sie Beispiele.



Security (Daten-/Informationssicherheit)

Wesentliche Grundwerte / Schutzziele der Informationssicherheit (Security) sind:

- **Vertraulichkeit:** Schutz vor nicht autorisiertem Lesen der Daten
- **Verfügbarkeit:** Daten müssen für autorisierten Zugriff verfügbar sein
- **Integrität:** Schutz vor nicht autorisierter oder anderweitiger unerwünschter Veränderung

Weitere häufig verwendete Ziele sind:

- **Authentizität / Echtheit / Vertrauenswürdigkeit (authenticity):**
verifiziert Echtheit und Herkunft der Daten
- **Nichtabstreitbarkeit / Verbindlichkeit (non-repudiation):**
identifiziert die Parteien einer Kommunikation
- **Nachvollziehbarkeit (accountability):**
Aktivität kann einer Identität eindeutig zugeordnet werden

Informations- und Betriebssicherheit in Smart Factories

- Der **hohe Grad der Vernetzung** in Smart Factories bringt eine **Vielzahl neuer Risiken** mit sich
- Maßnahmen, Konzepte sowie **Einheitliche Richtlinien**, Standards und Normen sind deshalb erforderlich
- Aktuell gibt es eine **Vielzahl nationaler- und internationaler Institutionen** und Publikationen. **Akteure** sind klassische Normierungs-/Standardisierungsinstitutionen, Industrieverbände, Interessenvertretungen sowie **staatliche Einrichtungen**
- National **relevante Institutionen** / Publikationen:
 - **Normungs-Roadmap für Industrie 4.0 und IT-Sicherheit**
(Deutsches Institut für Normung **DIN** / Deutsche Kommission Elektrotechnik **DKE**)
 - **ICS-Security-Kompendium**
(Bundesamt für Sicherheit in der Informationstechnik **BSI**)
 - **Abschlussbericht der Studie „IT-Sicherheit für die Industrie 4.0“**
(Bundesamt für Wirtschaft und Energie **BMWi**)



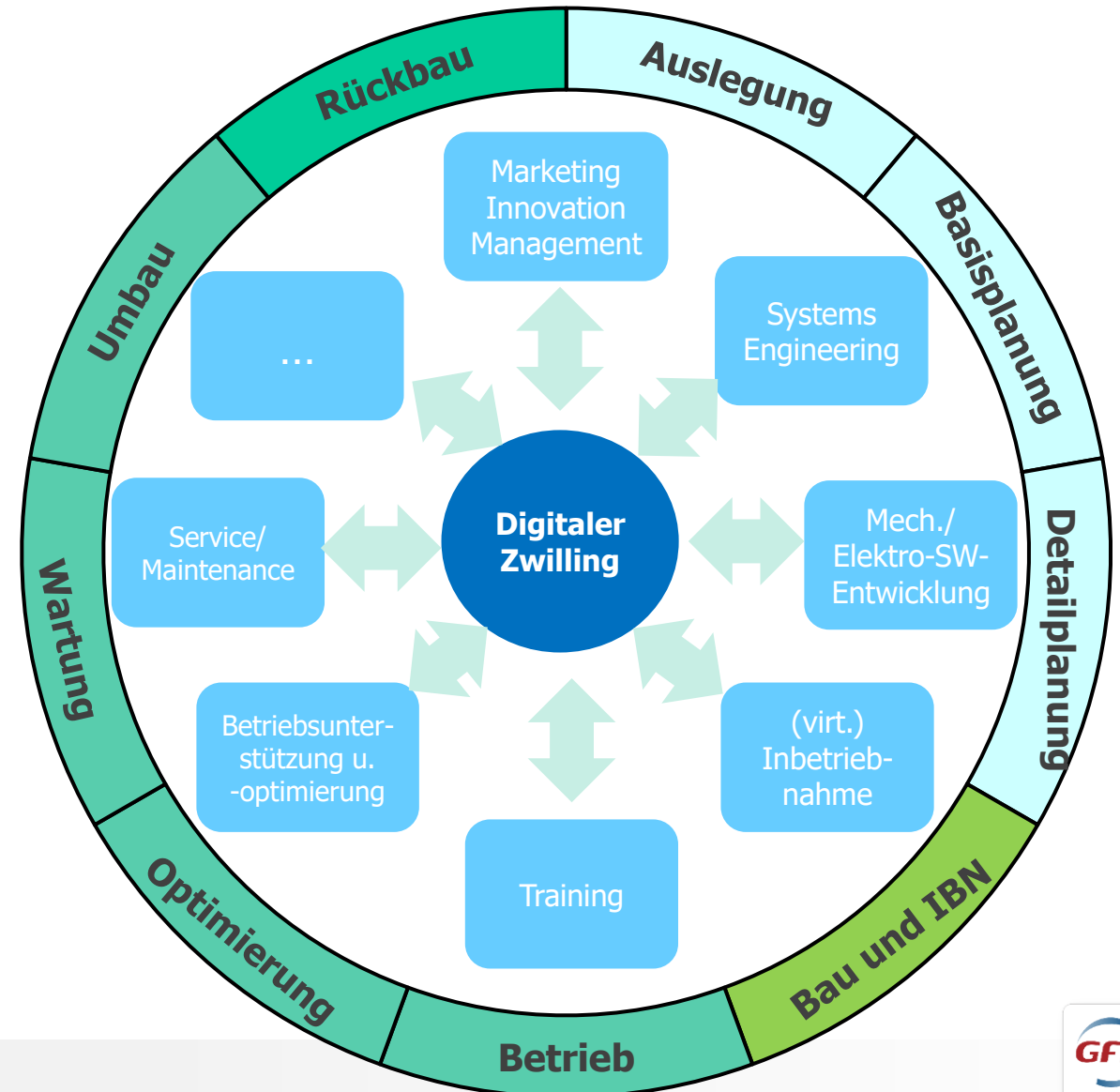
Richtlinie VDI/VDE 2182

- Der Verein Deutscher Ingenieure (VDI) zeigt in seiner Richtlinie 2182 konkrete Schutzmaßnahmen zur **Informationssicherheit** automatisierter Maschinen und Anlagen auf
- In einer simulationsbasierten **virtuellen Automatisierungssoftware** wird ein **digitaler Zwilling (DZ)** des gesamten Systems nachgebildet (Richtlinie 3633)
- Die **Nachbildung der Komponenten** erfolgt für Produkte und Prozesse des gesamten **Systemlebenszyklus**
- **Messdaten** und Informationen werden im Betrieb erfasst
- **Digitale Artefakte** sind semantisch verbunden

DZ im Kontext der Aufgabe in allen Lebenszyklusphasen

Allgemeines Vorgehensmodell zur Erreichung von Informationssicherheit:

1. Assets identifizieren
2. Bedrohungen analysieren
3. Relevante Schutzziele ermitteln
4. Risiken analysieren und bewerten
5. Schutzmaßnahmen aufzeigen und Wirksamkeit bewerten
6. Schutzmaßnahmen auswählen
7. Schutzmaßnahmen umsetzen
8. Prozessaudit durchführen



Das ICS-Security-Kompendium (BSI)

- Das **ICS-Security-Kompendium** ist ein **Grundlagenwerk** für IT-Sicherheit in **ICS (Industrial Control System)**
- Das Kompendium gewährt einen **Überblick** über die **Grundlagen von ICS** (**Schwachstellen**, Angriffsvektoren, Spezifika der Informationssicherheit in ICS-Umgebungen)
- Gibt **Empfehlungen** für weitere Standards und Dokument und legt Empfehlungen (**Best Practices**) zu
 - **Bedrohungen** und Gegenmaßnahmen
 - **Monitoring** und Anomalieerkennung in Produktionsnetzwerken
 - **Fernwartung** im industriellen Umfeld
 - Industrial Control System Security: **Innentäter**
- Eine **Gegenüberstellung** berücksichtigt unter anderen folgende Richtlinien:
 - **IEC-62443** Normenreihe
 - **Richtlinie VDI/VDE 2182**
 - **ISO-27000-Reihe**



Top 10 Bedrohungen in der Produktion nach BDI

Top 10 Bedrohungen	Trends seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	
Infektion mit Schadsoftware über Internet und Intranet	
Menschliches Fehlverhalten und Sabotage	
Kompromittierung von Extranet und Cloud-Komponenten	
Social Engineering und Phishing	
(D)DoS Angriffe	
Internet-verbundene Steuerungskomponenten	
Einbruch über Fernwartungszugänge	
Technisches Fehlverhalten und höhere Gewalt	
Kompromittierung von Smartphones im Produktionsumfeld	

Plattform Industrie 4.0-Arbeiten

- Im Jahr 2013 **gegründet** von **drei Verbänden**
 - **BITKOM** Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
 - **VDMA** Verband Deutscher Maschinen- und Anlagenbauer
 - **ZVEI** Zentralverband Elektrotechnik- und Elektronikindustrie
- **Ziel** der Plattform ist es, **einheitliche Rahmenbedingungen** zu schaffen
- Zum Zwecke, zukünftige **Trends, Entwicklungen und Zukunftsfragen** zu untersuchen, gibt es verschiedene **Arbeitsgruppen** mit folgenden Titeln:
 - Referenzarchitektur
 - Standards und Normung
 - Forschung und Innovation
 - Sicherheit vernetzter Systeme
 - Rechtliche Rahmenbedingungen
 - Arbeit, Aus- und Weiterbildung



Kompetenzcheck

- Erläutern Sie bitte, was unter einem Systemlebenszyklus zu verstehen ist!
- Beschreiben Sie Gegenmaßnahmen zu den Top 10 (häufigsten) Bedrohungsarten in der Produktion nach BDI (3 Maßnahmen).
- Kopieren Sie sich die 3 relevanten „Sicherheits-Publikationen“ aus dem Anlagenordner ((Normungs-Roadmap, ICS-Security-Kompendium, Studie „IT-Sicherheit für die Industrie 4.0)
- Verschaffen Sie sich dazu einen Überblick!



7.9.3 Sicherheit von Cyber-physischen Systemen

- **CP-Systeme interagieren** – im Gegensatz zu rein virtuellen Systemen – mit der physischen Umwelt. **Sicherungskonzepte (Betriebssicherheit)** müssen also auch immer **Störfaktoren** der realen Umwelt berücksichtigen
- Dabei ist es relevant, in welcher **geografischen Lage** die **Sensoren** des Systems angebracht sind
- **Echtzeitanforderungen**: Zeitkritische Systeme machen eine Kommunikation in Echtzeit erforderlich, d. h. der Informationsaustausch zwischen Sensoren und Aktoren muss unmittelbar erfolgen (z. B. Bremsvorgang bei autonomem Fahren)
- **Umgang mit Paketen**: In CPS müssen **physische und logische Pakete** unterschieden werden. Ein System liefert z. B. Daten von mehreren Sensoren. Jeder Messwert eines Sensors ist ein physisches Paket. Die Werte aller Sensoren werden zu einem logischen Paket zusammengefasst

Die Messungen und insbesondere die **Messgenauigkeit** können somit auch immer Auswirkung auf die **physische Umwelt** haben

7.9.3 Sicherheit von Cyber-Physischen Systemen

- **Obfuskierung der Metadaten und Topologie:** „Verschleierung“, die Sensoren eines CPS befinden sich häufig in einer **offenen, unsicheren Umgebung** (physisch für jedermann zugänglich). Metadaten wie **Standort** des Sensors oder **Zeitpunkte** der Datenaufzeichnung müssen vor Angriffen besonders geschützt werden
- **Vertrauensmanagement:** Messdaten von mehreren Sensoren können voneinander abweichen; die Messwerte einer Temperaturmessung können z. B. 30° C; 30° C; 30° C; 30° C; 150° C; 30° C lauten. Das System muss dann **selbständig entscheiden** können, ob die Messung des Sensors ein Fehler ist
- **Sichere Aggregation** der Daten: Wie oben beschrieben, werden die Daten der Sensoren in einigen Fällen über **Zwischenknoten** des CPS zunächst **aggregiert**, bevor sie an einen Kontrollpunkt weitergeleitet werden. Dies macht eine Ende-zu-Ende-Verschlüsselung schwierig
- **Steuerung und Verwaltung** von CPS erfordert oftmals den **Zusammenschluss** mehrerer **Netzsegmenten**. Werden die Teilnetze von **unterschiedlichen Instanzen** überwacht, entsteht gegebenenfalls erheblicher **Koordinationsaufwand**. Auch die **Absicherung der Koordination** muss gewährleistet sein

Sicherheit und Privatsphäre im Internet of Things (IoT)

- Die Geräte des IoT müssen, um ihre Dienste bereitstellen zu können, auch **persönliche Daten sammeln**, z. B. Geldtaschen- oder Schlüssel-Überwachungs-Tools, diverse Schrittzähler u. Ä.
- Sicherheitsziele in Bezug auf **Privatsphäre** zu definieren, ist deshalb eine grundsätzliche Herausforderung (Exkurs **Datenschutzgrundverordnung** DSGVO, Stichwort personenbezogene Daten)
- Durch das Erreichen des **Sicherheitsziels Vertraulichkeit** ist der Schutz der gesammelten Daten gewährleistet
- Andererseits werden die Sicherheitsziele durch verschiedene **Angriffstechniken** bedroht, hierzu gehören z. B. Denial of Service, Spoofing, Information Disclosure, Information Tampering, Elevation of Privileges
- Hiervon sind, neben der **Vertraulichkeit**, auch die anderen Sicherheitsziele **Integrität** und **Verfügbarkeit** der Daten bedroht

Sicherheitsrisiken im Internet of Things (IoT)

- Sensoren im IoT sind häufig auf geringen **Energieverbrauch** ausgelegt; **Denial of Service Angriffe** (Durchführung kryptografischer Algorithmen) führen zu höherem Energieverbrauch der Sensoren
- Als Folge wird die **Batterielaufzeit** der IoT-Geräte signifikant geschwächt. Auch die Prozessorleistung ist im Vergleich zu Standardcomputersystemen stark reduziert. Ein Angreifer kann die **Geräte leicht überlasten** und die **Verfügbarkeit** gefährden
- Die Sensoren sind oft an schwer erreichbaren Orten angebracht und müssen deshalb **lange Zeit ohne Vorort-Wartung** arbeiten
- Das IoT umfasst häufig eine **große Anzahl von Knoten**, IoT-Geräten und Mobilgeräten, welche **unterschiedliche Protokolle** und **Techniken** nutzen (z. B. ZigBee, RFID, QR-Code), daraus resultieren Informationen, die für das **Spoofing** verwendet werden können
- Die **drahtlose Natur** der IoT-Protokolle ermöglicht, bei geringer Entfernung, das Aufzeichnen der Kommunikation. Die Vertraulichkeit der Daten wird dadurch bedroht (**Information Disclosure**)

Sicherheitsrisiken im Internet of Things (IoT)

- IoT-Geräte werden häufig mit **Webinterfaces** ausgeliefert. Diese implementierten Oberflächen bieten keine ausreichenden Sicherheitsmaßnahmen (z. B. das **Ausschließen von Benutzern** nach **mehrfachen Anmeldeversuchen**, Verwenden von **schwachen Passwörtern** oder Übertragen von **Passwörtern in Klartext**)
- IoT-Geräte werden großteils in unkontrollierter, teils feindseliger Umgebung eingesetzt
- Folgende **Sicherheitsanforderungen** sollten deshalb erfüllt sein:
 - **Monitoring und Filtering** (IoT-Geräte sind meist nicht in der Lage, Angriffe zu erkennen oder aufzuzeichnen)
 - **Zugriffskontrolle (Access Control)** ^{*)}, im IoT wegen erhöhtem Energiebedarf schwierig
 - **Verschlüsselung**: Symmetrische Verschlüsselung im IoT, jedoch wegen hoher Anzahl der Teilnehmer unpraktikabel
 - **Physische Sicherheit** (z. B. ungenutzte USB-Ports an IoT-Geräten/Nodes deaktivieren)
 - **Sichere Interfaces** (siehe nächste Folie)

Maßnahmen für sichere Interfaces

- Automatische **default-Passwortänderung** während der ersten Inbetriebnahme
- Passwortrichtlinien, die die **Stärke der Passwörter** garantieren
- Implementierung einer **Two-Factor-Authentifizierung**
- Anzahl der **Login-Versuche** limitieren
- Login-Funktionen und Resets dürfen **keine Auskunft über vorhandene Benutzer** ermöglichen
- Während der **Programmierung** müssen bereits **Mechanismen gegen Web-Angriffe** (z. B. SQL Injection und Cross-site Scripting) eingebaut werden
- **Verschlüsselung**

Kompetenzcheck

- Was ist der Unterschied zwischen physischen und logischen Paketen?
- Was ist unter Obfuskierung zu verstehen?
- Was bedeutet Information Tampering und wie funktioniert in diesem Zusammenhang ein so genannter Sinkhole-Angriff?



Abbildungsverzeichnis und Lizenznachverfolgung

Bei allen Abbildungen handelt es sich um so genannte **Creativ Commons bis zur Lizenz CC BY-SA**. Diese Lizenz ermöglicht es Wiederbenutzern, das Material in jedem Medium oder Format zu verteilen, zu remixen, anzupassen und darauf aufzubauen, solange dem Ersteller eine Zuordnung gewährt wird. Diese Lizenz erlaubt auch die kommerzielle Nutzung.

- Abb. Dampfmaschine "[Dieses Foto](#)" von Unbekannter Autor ist lizenziert gemäß [CC BY-SA](#); Wiki Common
- Abb. Dynamomaschine, Werner von Siemens: "[Dieses Foto](#)" von Unbekannter Autor ist lizenziert gemäß [CC BY-SA](#)
- Abb. Z11, Konrad Zuse [Zuse-Z-11.jpg \(2048×1536\) \(wikimedia.org\)](#) CC 3.0
- Abb. Künstliche Intelligenz (KI) „[Dieses Foto](#)“ von Unbekannter Autor ist lizenziert gemäß [CC BY](#)
- Abb. Industrieroboter "[Dieses Foto](#)" von Unbekannter Autor ist lizenziert gemäß [CC BY-SA](#)
- Abb. Security; „[Dieses Foto](#)“ von Unbekannter Autor ist lizenziert gemäß [CC BY-SA](#)
- Abb. Cyber Security „[Dieses Foto](#)“ von Unbekannter Autor ist lizenziert gemäß [CC BY-SA](#)
- Abb. Arbeitsgruppen; "[Dieses Foto](#)" von Unbekannter Autor ist lizenziert gemäß [CC BY-SA](#)

Quellenangaben

- Lampesberger, Harald; Hermann, Eckehard; Kolmhofer, Robert: Sicherheit in der Industrie 4.0. IoT-Cloud-Cyber-Physische-Systeme. Schriftenreihe Recht und Informations-Technologie – Linz: Trauner-Verlag, 2017
- Kammermann, Markus: CompTIA Network+. Vorbereitung auf die Prüfung N10-007. 7. Auflage – Frechen, mitp-Verlag. 2018
- Broy, Manfred: Cyber-Physical Systems. Innovation durch Software-Intensive eingebettete Systeme. Achatec (Deutsche Akademie der Technikwissenschaften) diskutiert – München, Springer-Verlag. 2010
- Geisenberger Eva; Broy, Manfred: Agenda CPS. Integrierte Forschungsagenda Cyber-Physical Systems. Acatech Studie (Deutsche Akademie der Technikwissenschaften). 2012

**Danke für Ihre
Aufmerksamkeit!**