|  |
| --- |
| IU |
| Automatisierungstechnik |
| DLBROEIRA2\_E |

Übergeordnete Lernziele

Unter Automatisierung versteht man im Allgemeinen einen physischen Vorgang, der die Leistung eines Systems verbessert und wenig bis gar keine menschlichen Eingriffe erfordert. Das Konzept der Automatisierung ist mit der Befürchtung verbunden, dass sie den Menschen Arbeit wegnehmen könnte, aber in den meisten Fällen übernimmt die Automatisierungstechnik Arbeiten, die der Mensch entweder nicht oder nicht effektiv erledigen kann.

Das Ziel des Kurses **Automatisierungstechnik** ist es, ein grundlegendes Verständnis dieses Bereichs zu entwickeln. Das Studienskript beginnt mit den historischen Grundlagen: der Entwicklung der Automatisierung und den industriellen Revolutionen – um so moderne Automatisierungssysteme besser zu verstehen und mehr über Herausforderungen und Trends in diesem Bereich zu erfahren.

Das Studienskript gibt dann einen Überblick über speicherprogrammierbare Steuerungen, ihre Hardware, interne Architektur, Ein-/Ausgangsmodule und Programmiermethoden, um zu zeigen, warum sie die wichtigsten Bausteine in automatisierten Montage- und Produktionsprozessen sind. Ebenso ergänzen Erläuterungen zu den Grundlagen der Batch-Automatisierung und deren Anwendungen, Komponenten, Kommunikationstechnologien und Schnittstellen sowie SCADA-Systeme das Verständnis dieser etablierten Technologien.

Industrielle Kommunikationstechnologien werden als wichtiges Element in der Automatisierung angesprochen und es werden sowohl ihre ursprünglichen Netzwerke als auch aktuelle Technologien beschrieben. Das Studienskript geht sodann kurz auf Prozessleitsysteme ein, die als Teil der Entwicklung von Steuerungssystemen und ihren Komponenten vorgestellt werden.

Der Kurs endet mit einem Überblick über die Cybersicherheit in der Industrieautomatisierung, und geht dort auf Anlagensteuerungsnetzwerke, Cyberangriffe und häufige Schwachstellen in industrieller Software ein.

Lektion 1 – Einführung

**Lernziele**

Nach der Bearbeitung dieser Lektion können Sie …

… die historische Entwicklung der Automatisierung beschreiben.

… die Meilensteine der industriellen Revolutionen unterscheiden.

… den aktuellen Stand moderner Automatisierungssysteme analysieren.

… Herausforderungen und Trends in der Industrie 4.0 identifizieren.

1. Einführung

## Einführung

Die Automatisierung wird als ein wichtiger und notwendiger Bereich für den menschlichen Fortschritt anerkannt. Die Automatisierungstechnik umfasst die Analyse, das Design und die Verbesserung von neuen und bestehenden Automatisierungssystemen. Diese Lektion beschreibt die historische Rolle der Automatisierung in der Fertigung durch industrielle Revolutionen, die technologischen Aspekte moderner Automatisierungssysteme, die Herausforderungen, die sie mit sich bringen, und ihren Einfluss auf neue Trends in der Automatisierungstechnik.

## 1.1 Entwicklung der Automatisierung

Seit seinen Ursprüngen hat der Mensch nach Möglichkeiten gesucht, seine Arbeit mit minimalem Aufwand zu erledigen. Das hat zur Erfindung von Maschinen geführt, die Aufgaben mit wenig bis gar keinem Aufwand für den Bediener lösen. Die ersten Belege für solche Erfindungen stammen aus der Steinzeit, wo die Menschen Fallen zur Jagd einsetzten. Bewässerungssysteme in Babylon sind der erste Nachweis einer bewussten Automatisierung um das Jahr 2000 v. Chr. und wurden durch die Gesetze im Codex Hammurapi entdeckt (Platero, 2009).

Die ersten Vorläufer von Automaten stammen aus dem alten Ägypten, dessen Gliederpuppen aus der 12. Dynastie als Protoautomaten gelten. Ähnliche Artefakte wurden in Indien gefunden, wo sie Epen darzustellen scheinen, und in China, wo Puppen für Schattentheater verwendet wurden. Himmelskarten in ägyptischen Grabstätten, wie die Himmelsdarstellungen von Babylon, versuchen, den Nachthimmel zu simulieren und gelten als Vorläufer der astronomischen Uhren. Zwei ägyptische sprechende Statuen mit beweglichen Kiefern, die mit religiösen Zeremonien in Verbindung gebracht werden und noch heute existieren, sind ein weiteres Beispiel für Automatisierung (Moñux Chércoles, 2001). In der folgenden Abbildung sehen Sie eine bewegliche Maske eines Automaten.

Maske mit beweglichem Kiefer



Quelle: Darren & Brad (2013). CC von NC 2.0.

Im antiken Griechenland finden sich Belege für Regelsysteme in Schriftstücken, in denen die Rolle der Technik ausführlich behandelt wurde. Die rasante Entwicklung Griechenlands im Bildungsbereich steht in krassem Gegensatz zu seiner Technik, die nur in geringem Maße genutzt wurde. Erklärungen, warum das so war, gründen auf verschiedenen Annahmen, die zu allgemein akzeptierten Wahrheiten wurden. Zwei mögliche Gründe hierfür waren nach Gille (1986):

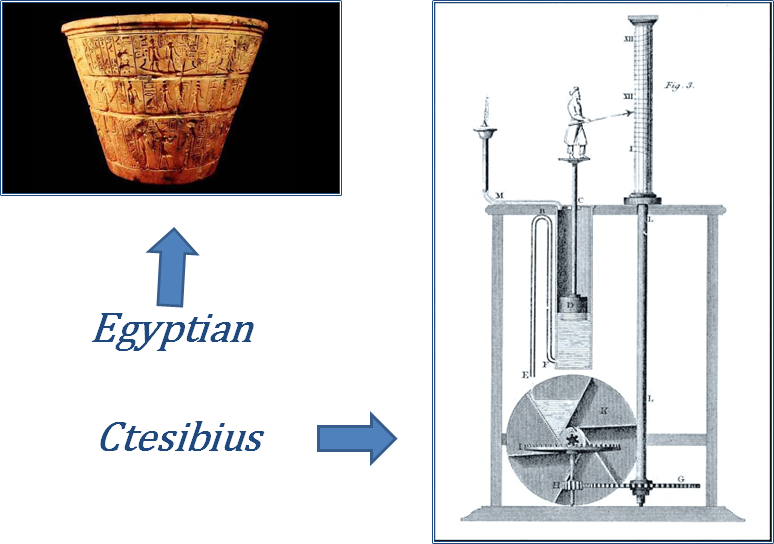
1. Die manuelle Arbeit wurde von Sklaven verrichtet, die in den griechischen Städten bis zu 50 Prozent der Bevölkerung ausmachten. Aus diesem Grund konnte der technische Fortschritt nicht als Befreiung von der Arbeit für die freie Bevölkerung verstanden werden. Es wird angenommen, dass Griechenland auch ohne Sklaven über eine Fülle von billigen Arbeitskräften verfügte, so dass es keine Notwendigkeit hatte, seine Arbeitskräfte zu ersetzen. Im Falle der Landwirtschaft zum Beispiel wären die Grundbesitzer nicht bereit gewesen, Geld für technische Innovationen zu riskieren, wenn sowieso billige Arbeitskräfte zur Verfügung standen.
2. Die Griechen gaben dem theoretischen Wissen den Vorrang vor dem praktischen Wissen. Um 400 v. Chr. waren Technik und Handwerk mit einem sozialen Stigma behaftet und wurde in den griechischen Städten verachtet. Diese Theorie besagt, dass die Griechen die manuelle Arbeit einfach verachteten und daher den technischen Fortschritt ablehnten, weil die Mitglieder der wohlhabenderen Klassen sich nicht auf technische Innovationen verlassen wollten, um Probleme zu lösen.

Es kam zu einem Zusammentreffen von Mentalitäten, sozioökonomischen und soziokulturellen Faktoren, die den Einsatz von Technik zu produktiven Zwecken nicht förderten. Es gab Fortschritte in der Katapulttechnik, die einen praktischen Zweck verfolgten, aber die Entwürfe der am häufigsten verwendeten Geräte gingen kaum über Zierbrunnen, Theatereffekte und Uhren hinaus (Moñux Chércoles, 2001).

Der Philosoph Archytas von Tarent, der Mathematiker Apollonius von Perga und der Wissenschaftler Archimedes von Syrakus zählen zu den ersten, die zur Entwicklung der Technik beigetragen haben (Gille, 1986). Diesen herausragenden Philosophen des 3. und 4. Jahrhunderts v. Chr. wird der Bau einer hölzernen Taube zugeschrieben, die über ein Druckluft- oder Dampfsystem verfügte, das ihr das Fliegen ermöglichte (Archytas), mehrere Musikautomaten (Apollonius) und eine Schraubenpumpe (Archimedes). Die Schneckenpumpe oder archimedische Schraube ist eine kurbelbetriebene Maschine zur Förderung von Flüssigkeiten und wird in vielen Bewässerungssystemen eingesetzt. Sie verdankt ihren Namen ihrem Erfinder Archimedes, dem Vater der Prinzipien der Hydrostatik (Gille, 1986).

Das Trio entwarf und nutzte auch Wasseruhren, sogenannte Klepsydras, die ursprünglich aus Ägypten stammten und später von Platon verwendet wurden, um 378 v. Chr. den ersten Wecker zu entwickeln (Moñux Chércoles, 2001). Den Abschluss der technischen Entwicklung dieser antiken Ära bildete die Schule von Alexandria. Vertreten durch die drei Mechaniker Ktesibios, Philon und Heron. Die Schule befasste sich nicht nur mit technischen Problemen im Zusammenhang mit Klepsydras, sondern zeichnete sich auch durch ihre mechanischen und pneumatischen Automaten sowie durch die Entwicklung der ersten Regler aus (Moñux Chércoles, 2001). Die folgende Abbildung zeigt eine einfache ägyptische Klepsydra neben einer aufwändigeren, die von Ktesibios entworfen wurde.

Klepsydra aus Ägypten und von Ktesibios

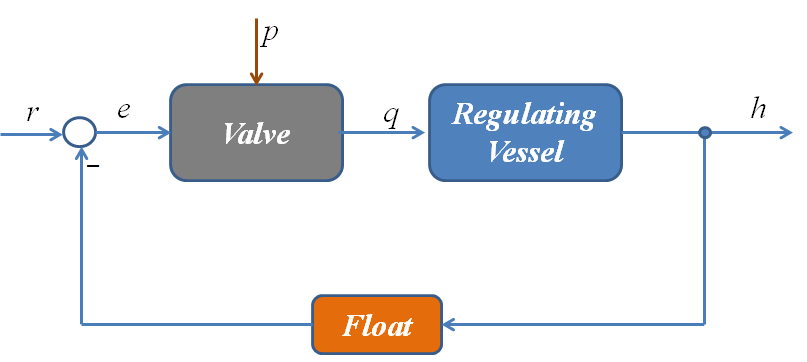


Quellen: Rredondo99 (2021) CC VON SA 4.0 & Horological Foundation (2007) Public Domain

Die technischen Beiträge der Schule beginnen mit Ktesibios um die erste Hälfte des 3. Jahrhunderts v. Chr. Auch keines seiner schriftlichen Werke erhalten geblieben ist, wurde er von seinen Zeitgenossen als Weiser angesehen und seine Beiträge sind durch seine Nachfolger bekannt (Gille, 1986). Er entwarf Schraubenpumpen, Musikinstrumente, Wasseruhren, Kriegsmaschinen und Automaten. Zu seinen berühmtesten Erfindungen gehören die Wasser und die Saug- und Druckpumpe, die einen Kolben verwendet (einen Hebel, der bei Betätigung einen Luftstrom in der Orgel erzeugt oder Wasser aus zwei untergetauchten Reservoirs ansaugt; Gille, 1986). Diese Prinzipien bildeten zusammen mit Getrieben die Grundlage für automatisierte Drehbewegungen, die eine Vielzahl von Effekten erzeugten, wie z. B. das Bewegen verschiedener Figuren, das Drehen kleiner Türme, das Fallen von Kugeln auf Becken oder das Erklingen winziger Trompeten (Moñux Chércoles, 2001).

Auf der Grundlage der Arbeiten von Hermann Diels (1924) folgert Otto Mayr (1970), dass Ktesibios mit der Konstruktion seiner Klepsydra (Schwimmerventil) die erste Regelvorrichtung geschaffen hat. Die Regelgröße einer Klepsydra ist ihr Wasserstand (h) in dem kleinen Reguliergefäß, der von einem Schwimmer mit einem Ventil erfasst wird, das sich öffnet, wenn der Pegel sinkt, und sich schließt, wenn er ansteigt. Die Referenz (r) ist der gewünschte Wasserstand, der durch die Position des Schwimmers bei geschlossenem Ventil dargestellt wird. Ein Blockdiagramm dieses Systems sehen Sie in der folgenden Abbildung.

Schwimmerregler von Ktesibios, Blockdiagramm

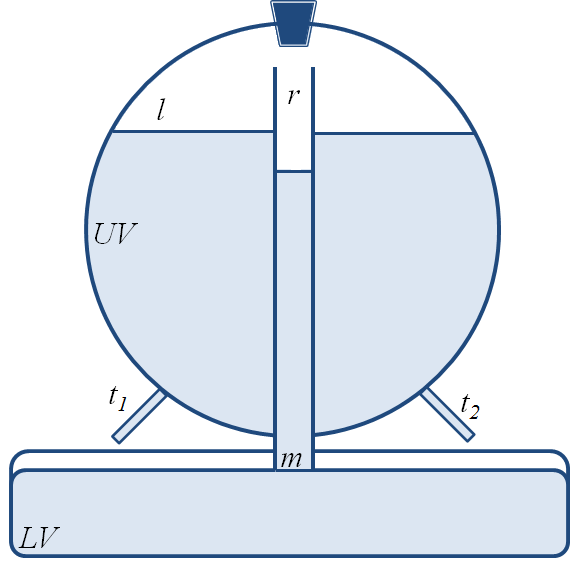


Quelle: Rojas (2022)

Das (p) steht hier für den Druck der Wasserversorgung, und das (q) ist die Durchflussmenge des Wassers, die in das Reguliergefäß eintritt.

Der in Byzanz geborene Philon setzte die Arbeit des Ktesibios in der zweiten Hälfte des 3. Jahrhunderts und zu Beginn des 2. Jahrhunderts v. Chr. fort (Gille, 1986). Die Ergebnisse fasste er in einem neunbändigen Kompendium namens *Mechanische Syntax* zusammen, in dem er die Begründungen für seine technischen Konstruktionen darlegt. Darunter befinden sich Hebel, pneumatische Geräte, Klepsydras und eine besondere Widmung an die Optimierung von Katapulten als Kriegsmaschinen. Darüber hinaus enthält sein Werk Details zu Automaten und Instrumenten sowie eine Abhandlung über den Bau von Häfen. In seiner Abhandlung über Pneumatik beschreibt Philon eine Reihe von automatischen Instrumenten und Puppen, die Bewegungen ausführen oder Töne von sich geben. Weiter geht es mit der Beschreibung von Waschbecken und Brunnen, die mit Tierfiguren versehen sind, die auf überraschende Weise Wasser versprühen. Philon wird sogar die Erfindung der ersten Wassermühle zugeschrieben. Da nicht bekannt ist, ob Ktesibios eine Abhandlung zu diesen Themen geschrieben hat, ist nicht klar, wie originell Philons Werk ist (Gille, 1986).

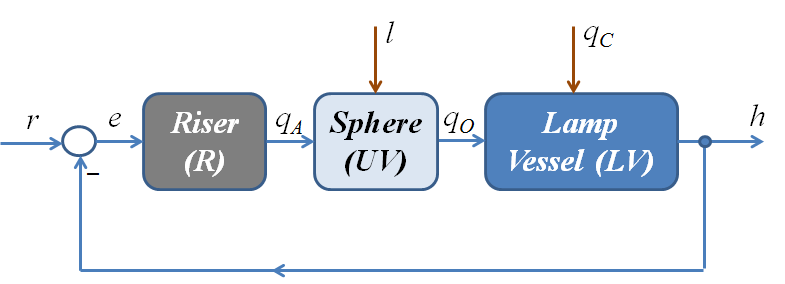
Aufbau der Öllampe des Philon



Quelle: Rojas (2022)

Philons bedeutendster Beitrag zur Automatisierungstechnik ist seine Abhandlung über die Pneumatik, bei der die Flüssigkeitsstände mit einer Methode reguliert werden, die keine Schwimmerventile verwendet. Sie nutzt die gleiche Grundlage wie die Tierbrunnen und ihre berühmteste Anwendung ist die Regulierung einer Öllampe, deren Entwurf in der vorherigen Abbildung zu sehen ist (Moñux Chércoles, 2001). Sie besteht aus zwei Gefäßen. Das obere Gefäß hat die Form einer Kugel (OG), und ein vertikales Rohr oder Steigrohr (S) verbindet es mit dem zweiten Gefäß oder Lampengefäß (LG), in dem die Flüssigkeit an der unteren Mündung des Steigrohrs auf einem konstanten Niveau gehalten wird (m). Zwei schmale Kapillarrohre r1 und r2 ermöglichen die Entleerung der Kugel in Richtung LG, wenn nötig. Der Vorgang wird mit Hilfe einer hydrostatischen Waage ermöglicht: Wenn ein Docht im Lampengefäß platziert wird, verbrennt das Öl und der Pegel des Gefäßes sinkt unter *m*. Dadurch kann Luft durch das Rohr eindringen und in Form von Blasen an die Spitze der Kugel aufsteigen. Dadurch fließt die Flüssigkeit durch r1 und r2 in Richtung des Gefäßes (LG), bis der Pegel wieder den Wert m erreicht. Wenn die Mündung vollständig geschlossen ist, kann die Luft nicht weiter aufsteigen und das Öl fließt nicht mehr durch die Kapillaren ab. Das Blockdiagramm dieses Systems ist in der folgenden Abbildung dargestellt. Dieser Regelungsaufbau ist eine einfache Form der schaltenden Regelung. Wenn der Pegel sinkt und Luft einströmen kann (e > 0), wird die Stellgröße, d.h. der Zufluss, aktiviert bis sich der Lufteinlass durch die Mündung des Steigrohrs schließt (e ≤ 0) (Mayr, 1970).

Philons Öllampe, Blockdiagramm



Quelle: Rojas (2022)

In diesem Blockdiagramm steht e für den Luftspalt, r ist der gewünschte Flüssigkeitsstand oder die Position des unteren Endes des Steigrohrs, h ist der tatsächliche Füllstand, qA ist die Durchflussrate der Luft, qO ist die Ölabgabe aus dem Reservoir, qC ist der Ölverbrauch in der Lampe, und l ist der Ölstand im Reservoir.

Der Beitrag der alexandrinischen Schule endet mit einem ihrer bekanntesten Vertreter, Heron, im 1. Jahrhundert n. Chr. (Moñux Chércoles, 2001). Sein Werk befasst sich mit den gleichen Problemen wie das seiner Vorgänger und umfasst Mechanik, Pneumatik, Wasseruhren, Kriegsmaschinen und Automaten. Die Abhandlungen über Pneumatik und Automaten sind von besonderem Interesse. Hydraulische Automaten, von denen einige mit einer Regelung ausgestattet sind, werden im Abschnitt über die Pneumatik beschrieben, während mechanisch basierte Automaten-Theater im Abschnitt über Automaten beschrieben werden. Beide sind Beispiele für Verbesserungen, die durch die hellenistische Technik erreicht wurden (Moñux Chércoles, 2001).

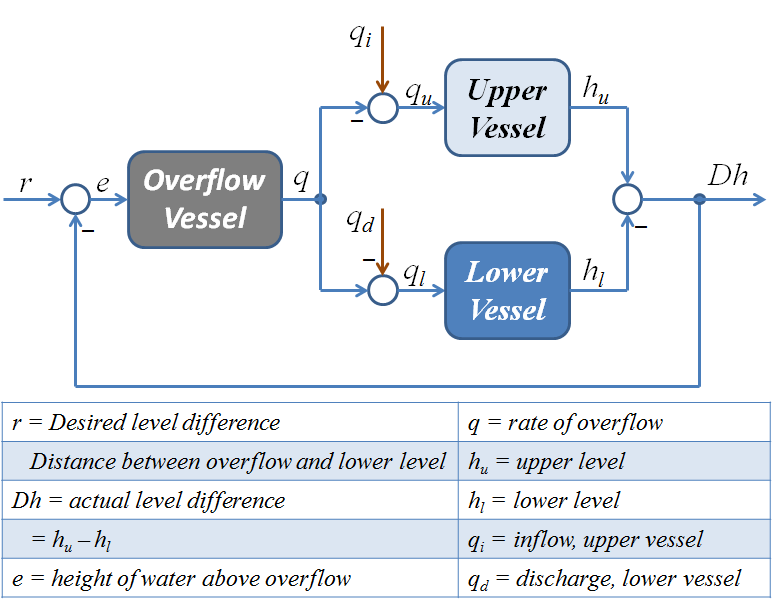
Aeolipile von Heron (auch: Heronsball)



Quelle: Pepe (2010). CC BY SA 2.0.

Die Pneumatik gilt als eine der am meisten studierten technischen Abhandlungen des Altertums (Gille, 1986). Das Werk ist in Form von 76 Theoremen aufgebaut, in denen eine Vielzahl von pneumatischen und hydraulischen Automatismen beschrieben wird. Heron ist der Meinung, dass bestimmte Aspekte der Physik denen von Philon ähneln, abgesehen von den Verweisen auf den Umgang mit Dampf. Heron stellt das in der vorherigen Abbildung gezeigte Aeolipil vor, ein Gerät, das sich mit Hilfe von Dampf dreht, der durch einen Mechanismus aus zwei gebogenen Rohren entweicht. Die Erfindung, die auch als Heronsball bezeichnet wird, wird von einigen als Prototyp der Dampfmaschine angesehen (Gille, 1986).

Rückkopplungsgeregelter Schwimmersiphon



Quelle: Rojas (2022)

In seiner Abhandlung über die Pneumatik stellt Heron außerdem drei verschiedene Regelungsmechanismen vor: Diejenigen, die einen Schwimmerregler verwenden, die direkt von Ktesibios‘ Schwimmersystem abgeleitet ist, diejenigen, die von Philos Regelungssystem inspiriert sind, und diejenigen, die einen Schwimmersiphon verwenden (Mayr, 1970). Die vorherige Abbildung ist ein Blockdiagramm, das von Mayr vorgeschlagen wurde, um zu zeigen, wie ein rückkopplungsgeregeltes System mit einem Schwimmersiphonmechanismus funktioniert.

Im Mittelalter mangelte es an der Entwicklung neuer Technologien zur Automatisierung. Vom 2. bis zum 12. Jahrhundert n. Chr. richteten die Europäer ihr Wissen auf die Moralphilosophie und die Theologie aus und passten die Philosophien Platons an die christlichen Überzeugungen an (Moñux Chércoles, 2001). Die griechische Naturphilosophie wurde von den Arabern bewahrt. Der Islam sollte der Bewahrer des technischen Wissens von Alexandria sein; so wurden viele Manuskripte von Philon und Heron ins Arabische übersetzt. All dies spiegelt sich in der Überlegenheit der arabischen Region auf Gebieten wie Windenergie und Wassermühlen, in der Chemietechnik wie der Herstellung von Parfüms und Säuren und im Maschinenbau wie Saugpumpen, Mechanismen, Uhren und Automaten wider, die in vielen Fällen alexandrinisches Wissen nutzten. Der bedeutendste Vertreter der mittelalterlichen islamischen Technologie und einer der größten Ingenieure vor der Renaissance war Ibn al-Razzaz al Dschazari aus Diyarbakir – in der heutigen Türkei – zwischen dem Ende des 12. und dem Beginn des 13. Jahrhunderts. Sein Hauptwerk war das „Buch des Wissens von sinnreichen mechanischen Vorrichtungen“, das sich mit Aspekten wie Uhren, Schöpfwerken, Automaten und musikalischen Springbrunnen befasst. Sein größter Beitrag ist die doppelzylindrische Saugpumpe, ein hydraulisches Rad, das über eine beliebige kinematische Kette zwei gegenüberliegende Kolben antreibt. Der Effekt: Wenn ein Zylinder das Wasser ansaugt, hebt der andere das Wasser an und ermöglicht so eine größere Wasserhöhe (Moñux Chércoles, 2001).

In Asien entfernten die Chinesen den Schwimmer der griechischen Klepsydras und verwandelten sie in echte mechanische Uhren (Brunete et al., 2020). Die erste bekannte Uhr stammt aus dem Jahr 725 n. Chr. und ist das Werk des Mathematikers und Astronomen I-Hsing. Er erfand ein hydraulisches Rad mit Bechern an den Schaufelenden: Wenn das Wasser aus einer Klepsydra in einen Becher floss, senkte sich durch das Gewicht des Bechers eine Stange, welches das das Rad stillhielt. So bewegte sich das große Rad jedes Mal, wenn ein Becher gefüllt wurde, um 36 Grad und aktivierte Zahnräder, die eine Himmelskugel bewegten. Um diese erschienen die Erde und der Mond und markierten den Sonnenauf- und -untergang, sowie den Neu- und Vollmond. Im weiteren Verlauf des Jahrhunderts gewannen astronomische Uhren und die Verwendung von Automaten in Europa an Bedeutung. Zu den erwähnenswerten Automaten gehört ein Hahn aus dem Jahr 1352. Als Teil der astronomischen Uhr des Straßburger Münsters, die bis 1752 in Betrieb war, ist der Hahn der älteste erhaltene Automat. Zu Beginn jeder Stunde bewegt er seinen Schnabel und seine Flügel (Brunete et al., 2020). Die folgende Abbildung zeigt den Automatenhahn.

Automatenhahn



Quelle: Ji-Elle (2010). CC BY SA 3.0, 2.5, 2.0 und 1.0.

Mit der Renaissance kamen die ersten großen Wissenschaftler und die wissenschaftliche Revolution. Im 15. und 16. Jahrhundert interessierten sich einige der wichtigsten Vertreter der Renaissance für Geräte, die von den Griechen beschrieben und entwickelt worden waren (Moñux Chércoles, 2001). Zu den bekanntesten Automaten, die zu dieser Zeit gebaut wurden, gehören der Mechanische Löwe von Leonardo da Vinci, der für König Ludwig XII. von Frankreich entwickelt wurde, und der Stockmann von Juanelo Turriano am Hof von Karl V. in Spanien im 16. Jahrhundert. Im 17. und 18. Jahrhundert wurden mechanische Geräte entwickelt, die einige Merkmale der heutigen Roboter aufweisen. Dazu gehört die mechanische Ente, die von Jacques de Vaucanson gebaut und in ganz Europa bewundert wurde. Die Ente konnte ihren Hals ausstrecken, um Körner aus einer Hand aufzupicken, dann zu schlucken und zu verdauen. Sie konnte trinken, planschen, quaken und eine Ente imitieren, die hastig etwas schluckt. Die Nahrung wurde in einer chemischen Reaktion verdaut und durch Schläuche zum Anus geleitet, wo sie durch einen Schließmuskel ausgeschieden werden konnte (Moñux Chércoles, 2001).

Das erste offiziell anerkannte Regelsystem im modernen Europa ist der Temperaturregler, der von Cornelis Drebbel zum Heizen eines Brutkastens erfunden wurde (Platero, 2009). Im Laufe des 18. Jahrhunderts entstanden verschiedene automatische Regelvorrichtungen, die ihren Höhepunkt erreichten, als James Watt den Fliehkraftregler entwickelte.

Fliehkraftregler nach James Watt



Quelle: Mirko Junge (2008). CC BY SA 3.0.

Dieser Regler hatte einen großen Einfluss auf die frühe Industrie und eröffnete einen neuen Weg in der Energienutzung und in der Steuerung von Produktionsprozessen. Aus diesem Grund wird der Wattsche Regler sowohl als Endpunkt der vorindustriellen Automatisierungsentwicklung als auch als Beginn der ersten industriellen Revolution angesehen (Platero, 2009). Die vorherige Abbildung zeigt einen Fliehkraftregler nach Watt an einer Dampfmaschine von Boulton und Watt im Science Museum, London.

### Fragen zur Selbstkontrolle

1. Bitte markieren Sie die richtige(n) Aussage(n).

* Die Bewässerungssysteme in Babylon gelten nicht als Beitrag zur Automatisierung.
* *Die ersten Vorläufer von Automaten gehen auf das alte Ägypten zurück.*
* Der Schwimmerregler wurde von Philon von Byzanz entworfen.

1. Nennen Sie die drei Regelungsmechanismen, die Heron in seiner Abhandlung über die Pneumatik vorstellt.

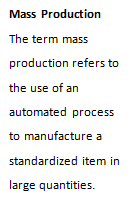
*Solche, die eine direkt von Ktesibios‘ Schwimmersystem abgeleitete Schwimmerregelung verwenden*

*Solche, die einen Schwimmersiphon verwenden*

*Solche, die von Philos Regelsystem inspiriert waren*

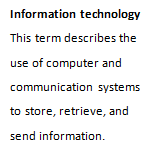
## 1.2 Industrielle Revolutionen

Jahrhundertelang wurden die meisten Güter, darunter Häuser, Nahrungsmittel, Kleidung, Werkzeuge und Waffen, von Hand oder mit Hilfe von Tieren hergestellt (Dey & Sen, 2020). Dies änderte sich mit der ersten industriellen Revolution, die gegen Ende des 18. Jahrhunderts Fertigungsprozesse einführte. Diese Prozesse haben die Produktion durch die Hilfe von Wasser und Dampf mechanisiert. Von da an entwickelte sich die Produktion rasant und führte zu einem erheblichen Anstieg der Güterproduktion (Dey & Sen, 2020).

Watts Regler lieferte die Grundlage für die Entwicklung der automatischen Regelung als wissenschaftliche Disziplin. Seine Vorrichtung konnte die Geschwindigkeit einer Dampfmaschine nur proportional regeln, aber Siemens modifizierte den Regler Mitte des 19. Jahrhunderts, um ihm eine integrale Wirkung zu verleihen und die Proportionalregelung ohne feste Referenz einzuführen (Platero, 2009). Die ersten Regler verhielten sich aufgrund der großen Reibung zwischen ihren Teilen gut (Piedrafita, 1999). Als sich die Konstruktionstechniken für die Maschinen änderten und die Herstellungsverfahren verbessert wurden, stellte man fest, dass die Geschwindigkeit der Maschinen zyklisch variierte. Dieses ernste Problem rief viele führende Ingenieure und Wissenschaftler auf den Plan. Einer von ihnen war Airy, der 1840 und 1851 zwei Abhandlungen über die Geschwindigkeitsregelung und den Einfluss der Dämpfung auf die Stabilität veröffentlichte. Die theoretischen Probleme wurden später von Maxwell und Vishnegradski gelöst. 1868 zeigte Maxwell, dass das Verhalten des Systems innerhalb einer Gleichgewichtslage durch eine lineare Differentialgleichung angenähert werden kann und dass die Stabilität in Form der Wurzeln der zugehörigen algebraischen Gleichung diskutiert werden kann. Routh im Jahr 1877 und Hurwitz im Jahr 1885 lösten beide unabhängig voneinander das Problem der Untersuchung der Stabilität eines dynamischen Systems auf der Grundlage der Wurzeln der charakteristischen Gleichung, ohne sie zu berechnen (Piedrafita, 1999). Weitere wichtige Beiträge zu dieser Revolution waren das Patent für einen automatischen Webstuhl mit Lochkarten, das Joseph Marie Jacquard 1801 erhielt, und die Erfindung der ersten vollautomatischen Drehbank durch Christopher Spencer im Jahr 1870 (Moñux Chércoles, 2001).

Seit den Anfängen der technischen Produktion ist die effiziente Gestaltung von Produktionsprozessen ein zentrales Ziel. Die moderne Entwicklung – oder die zweite industrielle Revolution – begann in Amerika und England Ende des 19. Jahrhunderts mit der Erzeugung von Elektrizität. Zur gleichen Zeit kam das Konzept der **Massenproduktion** auf und mit ihm der Taylorismus, bei dem die Produktion eines Gutes in einzelne Schritte unterteilt wird, die von einzelnen Arbeitern ausgeführt werden (Hounshell, 1985). Durch diese Umstellung wurde die Produktion erheblich gesteigert, und im Laufe der Zeit wurden immer mehr Maschinen in die Produktion eingeführt, von denen einige die menschliche Arbeitskraft ersetzten, was als Mechanisierung bekannt wurde. Maschinen, die mit irgendeiner Art von Steuerungs- und Regelungsvorrichtung ausgestattet waren, führten einfache Prozesse problemlos aus. Henry Ford steigerte das Potenzial der Massenproduktion und des Vertriebs, indem er das Fließband für die Automobilproduktion einsetzte. Die Fahrzeuge wurden auf dem Fließband in Teilschritten hergestellt, was die Geschwindigkeit erhöhte und die Kosten senkte (Dey & Sen, 2020).

Gleichzeitig wurden weitere Fortschritte bei der Automatisierung gemacht. Im Jahr 1873 legte Jean Joseph Léon Farcot in seinem Buch über Servomotoren die allgemeinen Prinzipien der Positionssteuerung fest (Bissell, 2009), und auf industrieller Ebene wurden immer ausgefeiltere pneumatische Regler und Messgeräte entwickelt. 1933 patentierte Mason den Stabilog, eine pneumatische Steuerung mit proportionalen und integralen Funktionen. Einige Jahre später wurden auch PID-Regler (PID = Proportional, Integral, Differential) mit Ableitungs- oder Vorsteuerungsfunktion verfügbar (Bissell, 2009). Die Bedeutung der automatischen Steuerung wurde 1912 deutlich, als der Nobelpreis für Physik an den schwedischen Erfinder Dalen für die Entwicklung automatischer Regler verliehen wurde, die in Kombination mit Gasakkumulatoren zur Beleuchtung von Leuchttürmen und Leuchtbojen verwendet werden konnten (Piedrafita, 1999). 1889 legte Ljapunow seine theoretischen Arbeiten zur Stabilität vor und schuf damit die notwendigen Grundlagen für die Entwicklung der Regelungstechnik. Bis weit ins 20. Jahrhundert hinein waren die einzigen analytischen Werkzeuge, die dem Spezialisten für Regelungs- und Steuerungstechnik zur Verfügung standen, gewöhnliche Differentialgleichungen, die mit algebraischen Kriterien kombiniert werden konnten, um die Position der Wurzeln der damit verbundenen charakteristischen Gleichung zu bestimmen. Aus theoretischer Sicht beginnt sich die Regelungs- und Steuerungstechnik zu etablieren, sobald das bei Signalverstärkungsproblemen erworbene Wissen auf industrielle Regelungs- und Steuerungsprobleme übertragen und angewendet wird. Diese Studien führten zur so genannten klassischen Kontrolltheorie, in der die Methoden der Laplace- und Fourier-Transformation und die externe Beschreibung von Systemen als mathematische Werkzeuge verwendet wurden. 1922 erkannte Minorsky die Nichtlinearität von Systemen und schuf eine Linearisierung, indem er die Taylor-Reihe für die Winkelbewegung eines Schiffes entwickelte. Im Jahr 1934 erörtert Hazen die Funktionsweise von Servomechanismen anhand typischer Schritt- und Rampeneingaben in seiner Analyse. Die Arbeiten von Nyquist (1932), Black (1934) und Bode (1940) über den Entwurf von rückgekoppelten Signalverstärkern legen den Grundstein für die Untersuchung von Servomechanismen und Reglern im Frequenzbereich. 1942 ermittelten die Taylor-Instruments-Ingenieure Ziegler und Nichols empirische Formeln für die Abstimmung von Proportional-Integral-Differential-Reglern (PID) (Piedrafita, 1999).

Die dritte industrielle Revolution setzte in den letzten Jahrzehnten des zwanzigsten Jahrhunderts ein und wurde von Fortschritten in der Elektronikindustrie, einschließlich des ersten Computerzeitalters, vorangetrieben. Automatisierte Maschinen, als Erweiterung der Erfindung und Herstellung diverser elektronischer Geräte, verringerten gleichzeitig den Aufwand und verbesserten die Geschwindigkeit und Genauigkeit. In einigen Fällen haben automatisierte Maschinen dazu geführt, dass menschliche Arbeit ersetzt wurde (Dey & Sen, 2020). Speicherprogrammierbare Steuerungen (SPS) wurden erstmals in den 1960er Jahren gebaut und ersetzten zunehmend menschliche Aufgaben durch automatisierte Systeme in Produktions- und Montageprozessen. Etwa zu dieser Zeit verlagerte sich das Paradigma der Fertigung von der Massenproduktion (Steigerung der Produktivität und Senkung der Kosten) hin zu einer stärker kundenorientierten Produktion (Heinrich et al., 2020). Eine schnelle Reaktion auf sich ständig ändernde Kundenwünsche, eine kurze Produktlebensdauer und der Wunsch, die Kund:innen zum Kauf einer Vielzahl von Produkten zu animieren, standen nun im Vordergrund der Überlegungen. Das neue Konzept führte weg vom Massenvertrieb und hin zur Massenindividualisierung. Gleichzeitig entstand durch die Integration von elektronischer Hardware in die Fertigungssysteme auch der Bedarf an Software, die diese unterstützte. Diese Softwaresysteme, die später als **Informationstechnologie** (IT) bezeichnet wurden, steuerten sowohl die Hardware als auch viele Managementprozesse (Dey & Sen, 2020). Konnektivität, Internetzugang und erneuerbare Energien trugen zum Fortschritt in den Bereichen Fertigung und Automatisierung bei. Die automatisierten Systeme entwickelten sich weiter, auch wenn die von ihnen ausgeführten Aufgaben weiterhin menschliche Hilfe erforderten.

Der Zweite Weltkrieg stimulierte die theoretische Entwicklung und noch viel mehr die praktische Umsetzung (Piedrafita, 1999), da er die dringende Notwendigkeit schuf, leistungsstarke Servomechanismen zu entwickeln. Infolgedessen wurden große Fortschritte bei der Entwicklung von Regelungssystemen gemacht. Die Entwickler konzentrierten sich auf das Problem der Geschützkontrolle und seine drei Phasen: Erkennung und Verfolgung des Ziels, Vorhersage und Platzierung des Geschützlaufs in der Schussposition. Während des Zweiten Weltkriegs entwickelte der Mathematiker Wiener die klassische stochastische Theorie, die versucht, das Problem der Automatisierung von Luftabwehrgeschützen zu lösen. Zudem formulierte er die Kybernetik, mit der er die Beziehung zwischen selbstgesteuerten Systemen und bestimmten Prozessen von Lebewesen herstellen wollte. In den späten 1940er Jahren etablierte Truxal die Modellmethode und Evans die Wurzelortsmethode als weitere Möglichkeiten zur Entwicklung der Kontrolltheorie. Zu dieser Zeit wurden auch die Grundlagen für die effektive Behandlung von Abtastsystemen als Grundlage für die Steuerung mit dem Computer gelegt. Ab 1955 wurden zeitliche Methoden und die Darstellung von Systemen in Zustandsvariablen als Ausgangspunkt für die moderne Kontrolltheorie entwickelt (Piedrafita, 1999).

Doch nicht alles war positiv: In den 1980er und 1990er Jahren begann in der Fertigungsindustrie eine Phase der Hochautomatisierung, die manchmal auch als computerintegrierte Fertigung (Computer Integrated Manufacturing, CIM) bezeichnet wird und die die Lösung für alle Probleme der Fertigungsindustrie zu sein schien (Heinrich et al., 2020). Das CIM-Konzept fasst die Integration des automatisierten Materialflusses und des automatisierten Informationsflusses in drei Aspekten zusammen: Computergestützte Fertigung (Computer-Aided Manufacturing, CAM), computergestütztes Design (Computer-Aided Design, CAD) und computergestützte Planung (Computer-Aided Planning, CAP) (Hitomi, 1994). Die erwartete Steigerung der Produktion von Waren wurde oft nicht realisiert oder war zu teuer. Die Idee hinter dem CIM-Konzept wurde missverstanden: Eine übermäßige Automatisierung um jeden Preis kann die Produktivität nicht zum gewünschten Ziel führen. Darüber hinaus ist eine reaktionsschnelle und flexible Automatisierung, die sich leicht an veränderte Bedingungen anpassen kann, eine Voraussetzung (Heinrich et al., 2020).

Die vierte industrielle Revolution, auch bekannt als Industrie 4.0, bringt erhebliche Veränderungen in der Automatisierungstechnik der Fertigung mit sich. Sie basiert auf einer Kombination von Produktionsvorgängen auf physischen und digitalen Plattformen (Rocha-Jácome et al., 2022). Cyber-physische Systeme haben die Lücken dieser Vorgänge überbrückt, indem sie zahlreiche und schnelle technologische Veränderungen in der Industrie hervorgebracht und eine intelligente Kommunikation zwischen Maschinen ermöglicht haben, unabhängig von ihrer Umgebung oder physischen Entfernung. Jetzt können die Aufgaben des Informationsaustauschs, der Ereignisgenerierung und der Steuerung zwischen intelligenten Maschinen, Lagereinrichtungen und Produktionssystemen autonom ausgeführt werden. Cyber-physische Systeme verfügen über integrierte Softwaresysteme und nutzen moderne Steuerungssysteme sowie eigene IP-Adressen, die über das Internet der Dinge (Internet of Things, IoT) verbunden und angesprochen werden. Auf diese Weise können Maschinen, Menschen, Prozesse und Infrastruktur vernetzt werden und miteinander kommunizieren, um neue Formen der Produktion, Wertschöpfung und Optimierung in Echtzeit zu ermöglichen. Manche intelligente Maschinen können auch kontinuierlich Störungen überwachen, erkennen und vorhersagen, so dass Präventivmaßnahmen und Korrekturen vorgeschlagen werden können, was eine bessere Vorbereitung und geringere Ausfallzeiten für die Industrie ermöglicht (Rocha-Jácome et al., 2022).

Die meisten Unternehmen haben noch keine vollständige Strategie entwickelt, wie sie in die Industrie 4.0 einsteigen wollen, aber der Trend geht dahin, Steuerungssysteme mit Hilfe von Informationssystemen in künstliche Intelligenz (KI) zu verwandeln. Die Idee ist, das Industrielle Internet der Dinge (Industrial Internet of Things, IIoT) zu nutzen, um Netzwerke von Geräten, Apparaten, Maschinen und Robotern zu verbinden, zu überwachen und zu steuern, indem Informationen aus der Cloud in Echtzeit verarbeitet werden. Dadurch können diese Netzwerke lernen, arbeiten und automatisch funktionieren, wodurch menschliche Eingriffe minimiert werden und die Produktion optimiert wird. In den folgenden Abschnitten erfahren Sie, wie moderne Automatisierungssysteme funktionieren und welche Trends und Herausforderungen die Zukunft bereithält.

### Fragen zur Selbstkontrolle

1. Bitte vervollständigen Sie den folgenden Satz:

Die erste programmierbare logische Steuerung wurde *gebaut* in den 1960er Jahren und unterstützt durch die Entwicklung der *Elektronik*.

1. Nennen Sie die drei Aspekte, die die Integration des automatisierten Materialflusses und des automatisierten Informationsflusses im CIM-Konzept zusammenfassen:

*Computergestützte Fertigung (CAM)*

*Computergestütztes Design (CAD)*

*Computergestützte Planung (CAP)*

## 1.3 Moderne Automatisierungssysteme

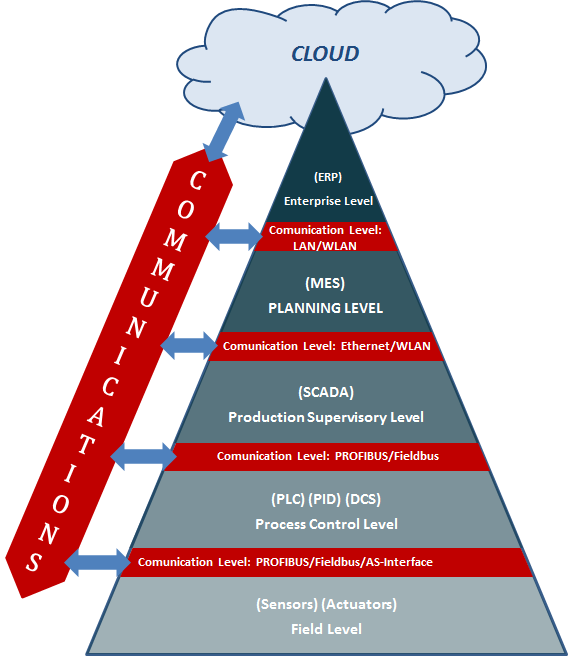
Die modernen Automatisierungssysteme der Industrie 4.0 müssen auf die Bedürfnisse des Unternehmens reagieren und sich entsprechend dem jeweiligen konzeptionellen Modell weiterentwickeln. Das Konzept der Industrie 4.0 ist jedoch dynamisch und komplex, da es sich ständig weiterentwickelt und durch Innovation geprägt ist (Rocha-Jácome et al., 2022). Ein guter Ausgangspunkt für die Gestaltung ist daher die Automatisierungspyramide, wenn sie an die aktuellen Informations- und Kommunikationstechnologien sowie das Wissen und die Organisation anderer neuerer Konzepte und Werkzeuge wie cyber-physische Systeme, Internet der Dinge, künstliche Intelligenz und digitale Zwillinge angepasst wird. Automatisierungspyramiden und cyber-physische Systeme werden im Folgenden beschrieben.

### Automatisierungspyramide

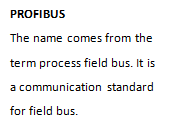
Die Automatisierungspyramide ist eine grafische Darstellung, die auf den Standard der International Society of Automation (ANSI/ISA) 95 zurückgeht. Sie wird häufig verwendet, um verschiedene Ebenen oder Hierarchieumgebungen zu veranschaulichen, die die Integration von Geschäftsfunktionen und Kontrollsystemen in herstellenden Unternehmen ermöglichen (Hollender, 2010). Sie dient als Leitfaden für die Organisation der Implementierung der Automatisierung im gesamten Unternehmen. In der heutigen Welt hängt der wirtschaftliche Erfolg eines Unternehmens u. a. von seiner Fähigkeit ab, schnell auf Kundenwünsche und Marktveränderungen zu reagieren. Daher ist ein effektives Kommunikationsdesign im Unternehmen wichtig und die Pyramide erleichtert die Umsetzung dieses Ziels. Daher ist die Gestaltung einer effektiven internen Kommunikation, aber auch mit dem Umfeld, für das Unternehmen wichtig und die Pyramide erleichtert die Umsetzung dieses Ziels.

Wenn Sie sich die Hierarchieebenen genauer ansehen, wird deutlich, dass die Kommunikationsaufgaben komplex sind und sich in ihren Anforderungen an Geschwindigkeit und Datenmenge unterscheiden. Dieser Aufbau unterscheidet sich geringfügig von der ursprünglichen Pyramide, denn er hebt den Informationsfluss und die Kommunikation mit der Cloud als grundlegenden Teil des Organisationssystems hervor. Es wird zwischen den hierarchischen Ebenen bzw. Levels unterschieden:

Automatisierungspyramide



Quelle: Rojas (2022)

**Level 0: Prozess- bzw. Feldebene**

Level 0 bildet die Basis der Pyramide und enthält Aktoren und Sensoren, die mit dem Produktionsprozess interagieren. Hier werden die Daten aufgezeichnet und verarbeitet, wobei die Reaktionen entsprechend der ausgewerteten Informationen erfolgen. Diese Geräte gewährleisten die Messung der Prozessvariablen, die Ansteuerung der Aktoren und die Verbindung mit übergeordneten Steuerungen. Die Kommunikation auf dieser Ebene dient der Bewältigung von Datenmengen, die mit kurzen Reaktionszeiten übertragen werden müssen, im Allgemeinen über **PROFIBUS-** oder Feldbusnetze und kleine AS-Interface-Subnetze (Aktor-Sensor-Schnittstelle). Außerdem muss Level 0 dafür sorgen, dass die Signale von den Sensoren die Steuerungen erreichen und dass relevante Informationen von den Steuerungen zu den Aktoren gelangen, von denen wiederum relevante Informationen an höhere Ebenen gesendet oder von diesen empfangen werden.

**Level 1: Steuerungsebene**

Auf dieser Ebene werden die Produktionsprozesse und deren Überwachung durch Geräte auf der Feldebene gesteuert, geregelt und manipuliert. Es besteht im Allgemeinen aus speicherprogrammierbaren Steuerungen (SPS) und Prozessleitsystemen (PLS); für einige spezielle Anwendungen werden in die SPS eingebettete Proportional-Integral-Differential-(PID)-Regler verwendet. Während die Automatisierung sequentieller oder binärer Systeme von SPS-Systemen übernommen wird, werden PLS für kontinuierliche Systeme eingesetzt und basieren im Allgemeinen auf Prozessen. Diese Geräte sind nach Bereichen oder Produktionszellen organisiert, die aus einem oder mehreren PLS bestehen, je nach Größe der Prozesse. Die Kommunikation auf dieser Ebene erfordert auch eine Datenübertragung mit kurzen Reaktionszeiten, weshalb PROFIBUS- oder Feldbusnetzwerke verwendet werden. Darüber hinaus muss sie eine Verbindung innerhalb einer Zelle, zwischen einzelnen Produktionszellen und anderen Ebenen sicherstellen. Da diese Ebene in der Regel nicht über Speicherkapazitäten verfügt, müssen die Daten auf höhere Ebenen übertragen und in Datenbanken oder in der Cloud gespeichert werden.

**Level 2: Leitebene**

Diese Ebene wird durch das SCADA-System (Supervisory Control and Data Acquisition; dt. Überwachung, Steuerung und Datenerfassung) abgedeckt. Sie bündelt alle Entscheidungen der unteren Ebenen, die sich sowohl auf die einwandfreie Funktion der Steuerungssysteme als auch auf die Überwachung der Erreichung der von den höheren Ebenen vorgegebenen kurzfristigen Produktionsziele beziehen. Um ihre Aufgabe zu erfüllen, verfügen diese Systeme über Mensch-Maschine-Schnittstellen (MMS; auch Human Machine Interface, HMI), die eine organisierte und systematische Visualisierung des Anlagenbetriebs ermöglichen. Dort können die Bediener:innen den Betrieb überwachen und notwendige Korrekturmaßnahmen ergreifen, um die gewünschte Leistung bei verschiedenen Produktions- und Wartungsaufgaben zu erreichen. Die Kommunikation auf dieser Ebene erfolgt über Ethernet-Netzwerke und WLAN-Netze, die den Zugriff auf Informationen aus untergeordneten Netzwerken sowie auf Computersysteme der höheren Ebene ermöglichen. Darüber hinaus sind wichtige Speicherkapazitäten durch dedizierte Datenbanken vorhanden, zusätzlich zu verschiedener Software für Anwendungen, die in der Industriewelt verwendet werden. Aus der IT-Perspektive ist dies der Ort, an dem die Integration von Geschäftsfunktionen und Kontrollsystemen stattfindet.

**Level 3: Betriebsleitebene**

Auf dieser Ebene erfolgt die Verwaltung und Bearbeitung von Lieferaufträgen, die Rechnungsstellung, die Terminverfolgung, die Kostenanalyse und die Produktionsplanung auf der Grundlage der Rohstoffbestandsberichte und der aktuellen Produktion. Diese Prozesse gewährleisten den täglichen Betrieb des Unternehmens. Um diese Aufgabe zu bewältigen, stehen den Betriebsleitern und Unternehmensmanagern Softwarelösungen wie das Manufacturing Execution System (MES) zur Verfügung. Die Kommunikation sowohl auf dieser als auch auf der höheren Ebene erfolgt über kabelgebundene und drahtlose lokale Netzwerke (LAN/WLAN).

**Level 4: Unternehmensebene**

Alle Prozesse, die das Überleben des Unternehmens auf dem Markt sichern, werden hier ausgeführt. Manager, Geschäftsführer und Unternehmensleiter analysieren alle Aspekte, die mit der internen Leistung des Unternehmens (Unternehmensführung, strategisches Personal und Produktion) und seiner Beziehung zum Umfeld (Marktanalyse und Investitionsplanung) zusammenhängen. Der Einsatz von Computersystemen, wie z. B. Enterprise Resource Planning (ERP), ermöglicht taktische und strategische Entscheidungen, einschließlich der Gestaltung von Werbung, Öffentlichkeitsarbeit, Verkaufsförderung und deren Beziehung zu Produktimage und Markenpositionierung.

Die auf höheren Ebenen verwendeten Computersysteme sind komplex, und die sie unterstützenden Kommunikationsnetze erstrecken sich über große Bereiche des Unternehmens. Die Verwaltung von Informationen und die Kommunikation über das Internet mit Kund:innen, Lieferanten, öffentlichen Verwaltungen und externen Mitarbeitenden ist von besonderer Bedeutung. Obwohl viele Benutzer:innen an ihnen teilnehmen und große Datenmengen verarbeitet werden, sind die Verarbeitungszeiten nicht von entscheidender Bedeutung.

### Cyber-physische Systeme

Cyber-physische Systeme sind Komponenten intelligenter Fabriken mit rechnergestützten und physischen Fähigkeiten, die es ihnen ermöglichen, mit Menschen zu kooperieren und Produktionsstrukturen, Koordinationsmittel, Management, Transport und Lagerung zu integrieren, so dass sie der Industrie durch Kommunikationsnetzwerke unter Verwendung des Internets der Dinge (IoT; Ynzunza et al., 2017) einen Mehrwert bieten. Sie bestehen aus verschiedenen technologischen Elementen, die entsprechend der zugewiesenen Aufgabe arbeiten und die bestehenden automatisierten Prozesse ersetzen oder ergänzen. Ding et al. (2019) hat diese Elemente in drei große Gruppen eingeteilt: Intelligente Objekte, cyber-physische Objekte und die Methode des digitalen Prozesszwillings. Um die Integration der verschiedenen Elemente in modernen Automatisierungssystemen zu erreichen, ist die Methode des digitalen Prozesszwillings für die Verwaltung von Information und Kommunikation zuständig (Martinez et al., 2021). Zu diesen Mechanismen oder Managementprozessen gehören das Industrielle Internet der Dinge, künstliche Intelligenz und digitale Zwillinge.

### Industrielles Internet der Dinge (IIoT)

Das Industrielle Internet der Dinge ist eine noch junge Kategorie industrieller Produktionssysteme, die durch technologische Fortschritte bei drahtlosen Sensornetzwerken, drahtloser Kommunikation mit geringem Stromverbrauch, eingebetteten Systemen und Identifizierungstechnologien vorangetrieben wird (Kim & Tran-Dang, 2019). Diese Systeme haben es ermöglicht, das Internet der Dinge in zahlreichen Überwachungs- und Steuerungsanwendungen in verschiedenen Bereichen zu implementieren, wobei Installation, Zuverlässigkeit, Wartung, Systeminteroperabilität und Skalierbarkeit mit großer Effizienz und wirtschaftlichem Nutzen erfolgreich eingesetzt werden. Kommunikationstechnologien sind die Schlüsselkomponente bei der Schaffung von IIoT-Systemen, die die Verbindung, die Kommunikation und den Datenaustausch zwischen allen Geräten und Maschinen ermöglichen. Auf diese Weise bieten die Dienste eine genauere und schnellere Entscheidungsfindung für die Industrie, die durch die Überwachung, Sammlung, Austausch und Analyse von Daten möglich wird (Kim & Tran-Dang, 2019).

### Künstliche Intelligenz (KI)

Die Analyse und Verwaltung der riesigen Menge an Informationen, die im modernen Fertigungsprozess erzeugt werden, ist eine Herausforderung. Künstliche Intelligenz hat sich als geeignetes Werkzeug für den Umgang mit großen Datenmengen erwiesen und hat die neuen Algorithmen des maschinellen Lernens überholt (Huang et al.,2021). Darüber hinaus ist es in der Automatisierungsbranche wichtig, Informationen effizient zu interpretieren, weshalb KI-basierte Management-Informationssysteme auch zur Vorhersage oder Verbesserung von Fertigungsprozessen eingesetzt werden. Ebenfalls ist die Anwendung von KI-Algorithmen zur Problemlösung für die Entscheidungsfindung geeignet. In dem Maße, wie sich die Leistung des Entscheidungssystems und der kooperativen Arbeit verbessert, wird auch die Leistung der Produktionssysteme optimiert. Dies ermöglicht die Implementierung von agilen Fertigungsprozessen auf der Grundlage von Management-Informationssystemen, was die Zusammenarbeit der Partner verbessert (Huang et al., 2021).

### Digitale Zwillinge

Digitale Zwillinge sind virtuelle Elemente, welche physische Elemente und ihr Verhalten in der realen Welt darstellen. Die Beschreibung erfolgt anhand digitaler Modelle. Digitale Zwillinge setzen sich aus fünf Teilen zusammen: Virtuell, physisch, Daten, Verbindung und Service (Martinez et al., 2021). Der virtuelle Teil ermöglicht Simulationen zur Entscheidungsfindung und Steuerung des Systems in der realen Welt. Diese effektiven und innovativen Werkzeuge ermöglichen die Entwicklung neuer Fertigungsprozesse und -funktionen, indem cyber-physische Systeme in Unternehmen in ihrem derzeitigen Zustand integriert und an die Prozessautomatisierung angepasst werden (Martinez et al., 2021).

### Fragen zur Selbstkontrolle

1. Welche der folgenden Aussagen sind zutreffend?

* *Ethernet ist ein Kommunikationsstandardprotokoll*
* ERP steht für Energy-Resource-Platform
* *Level 1 der Automatisierungspyramide ist die Steuerungsebene*
* Auf der Betriebsleitebene wird die Beziehung des Unternehmens zu seiner Umgebung analysiert

1. Bitte vervollständigen Sie den folgenden Satz.

Digitale Zwillinge *sind virtuelle Elemente*, welche *physische Elemente* und ihr Verhalten in der realen Welt darstellen. Die Beschreibung erfolgt anhand *digitaler Modelle*.

1.4 Herausforderungen und Trends

Die Industrie 4.0 hat sich noch nicht endgültig etabliert und einige Autoren behaupten, der Beginn der Industrie 5.0 stehe unmittelbar bevor. Beide haben ihre Grundlagen in cyber-physischen Systemen und dem industriellen Internet der Dinge gelegt (Ynzunza et al., 2017; Ozdemir & Hekim, 2018). Die Zahl der technologischen Instrumente und Geräte, aus denen sich der Stand der industriellen Automatisierung zusammensetzt, ist allerdings sehr hoch, und die Grenze zwischen Trends und Herausforderungen ist äußerst unscharf, da jeder Trend unterschiedliche Herausforderungen mit sich bringt, die überwunden werden müssen, um seine Umsetzung auf einem akzeptablen Niveau zu erreichen. Deshalb werden in diesem Abschnitt prädiktive Wartung, Cybersicherheit, Big Data, intelligente Fabriken, maschinelle Bildverarbeitungssysteme und autonome mobile Roboter als die wichtigsten Trends mit ihren jeweiligen Herausforderungen bei der Umsetzung vorgestellt.

### Prädiktive Wartung

Wenn man über prädiktive Wartung (auch vorausschauende Wartung) spricht, fällt es schwer, nicht an ihren Vorgänger, die präventive Wartung (auch vorbeugende Wartung), zu denken, die in vielen Unternehmen immer noch angewandt wird und aus einer starren Planung auf der Grundlage der geschätzten Zeiten für den Ausfall und den Austausch von Geräten besteht. Mit dem Aufkommen zahlreicher intelligenter Sensoren und der Überwachung des Maschinenzustands werden jedoch Variablen wie Temperatur, Vibrationen, Feuchtigkeit und Lärm in jeder Phase der Fertigung überwacht, so dass man sofort über den aktuellen Zustand jeder Komponente in der Produktionslinie informiert ist. Dies führt dazu, dass flexible und dynamische Wartungsanfragen erfüllt und beauftragt werden können, bevor das Problem einen kritischen Zustand erreicht. Die prädiktive Wartung vermeidet somit unnötige Verluste in der Nutzungsdauer der am Prozess beteiligten Maschinen, was zu Kosteneinsparungen führt und die Ausfallzeiten der Maschinen reduziert (Carvajal Soto et al., 2019; Ynzunza et al. 2017).

In der Praxis hat sich herausgestellt, dass die Umsetzung von Systemen zur prädiktiven Wartung anhand physikalischer Modelle oft schwierig ist und die Prädiktionsgüte nicht immer ausreichend ist. So hat sich beispielsweise die Implementierung von digitalen Zwillingen als effektiv erwiesen, aber sie basieren auf anspruchsvollen Modellen erster Prinzipien, was sie komplex macht. Daher werden alternative Methoden verwendet. So wurden Online-Fehlererkennungen unter Verwendung des IIoT auf der Grundlage von maschinellem Lernen und/oder künstlicher Intelligenz sowie hybride Lösungen unter Verwendung von digitalen Zwillingen auf der Grundlage von künstlicher Intelligenz und maschinellem Lernen vorgeschlagen, um die physikalischen Modelle zu ersetzen bzw. zu erweitern (Yokohawa, 2021; Carvajal Soto et al., 2019). Ein anderer Ansatz integriert sogar Geschäftsdaten mit den von den Sensoren gesammelten Informationen in einer dreistufigen Softwarearchitektur: Cloud, Fog und Edge, für die Entscheidungsfindung in einem dynamischen Programmiertool (Coito et al., 2020).

### Cybersicherheit

Die in der Industrie 4.0 geschaffenen und auf dem IIoT basierenden Netzwerke sind immer schneller, verfügen über eine größere Konnektivität und sind in hohem Maße von der Komplexität ihrer Software abhängig. Dies schafft einen unübersehbaren Nährboden für Cyberkriminelle, die sich in industrielle Systeme einhacken, Daten stehlen und Identitäten vorgeben wollen. Cyberangriffe sind nicht das Ziel dieser Hacker, sondern das Mittel, um eine Vielzahl von wirtschaftlichen, rechtlichen, politischen und militärischen Zielen zu verfolgen (Geers, 2015).

Auch wenn sich die Kund:innen beim Thema Cybersicherheit meist auf die Technologie konzentrieren, sagen Experten voraus, dass es auch anders gehen könnte. Kund:innen stellen oft fest, dass die Technologie rund um die Cybersicherheit die Sicherheitsbudgets überfordert, da sie mit Strategien für Disaster Recovery, HSE und die Versicherung von Industrieanlagen vermischt werden. Daher ist es oft notwendig, dass ein Unternehmen minimale Mittel in die Cybersicherheit investiert. Aus diesem Grund sind sie sich nicht bewusst, dass Cybersicherheit nicht mehr nur ein technisches Problem ist, sondern ein wirtschaftliches Risiko, das zu einem Hindernis wird, das direkte Maßnahmen erfordern kann. Die realen Kosten, die entstehen, wenn Cybersicherheitslösungen nicht berücksichtigt werden, und die ständige Zunahme der Bedrohungen haben die Aufmerksamkeit auf die Einführung strengerer Cybersicherheitsmaßnahmen gelenkt. Darüber hinaus wurden Verbesserungen bei der Schulung der Mitarbeitenden und der Information der Kund:innen und Lieferanten des Unternehmens vorgenommen, um diese Probleme zu bekämpfen (Yokohawa, 2021). Aus technologischer Sicht wurde auch eine Norm, ISA/IEC 62443, geschaffen, die sich mit Fragen der Sicherheit für industrielle Automatisierungs- und Steuerungssysteme befasst. Dieser Standard ermöglicht ein besseres Verständnis der Risiken in IIoT-basierten Netzwerken und das Design von Systemen mit einer höheren Wiederherstellungsgeschwindigkeit nach einem Angriff (Hassani et al., 2021).

### Big Data

Fortschrittlichere IIoT-Technologien, Multifunktionssensoren, Cloud Computing, systeminterne Interkommunikation und damit verbundene externe Informationen bedeuten die Produktion einer großen Menge an Daten, die in der Industrie 4.0 ständig und in Echtzeit gesammelt werden. Das ist nicht neu und wird auch in Zukunft eine der wichtigsten Herausforderungen und Trends in der Automatisierung sein, denn es liegt im Interesse der Unternehmen, das Potenzial dieser Technologie zu nutzen. In den automatisierten Produktionsprozessen spiegelt sich das Vorhandensein von Big Data in jeder Eingabe und Aktion wider, die sofort untersucht oder für eine spätere Analyse gespeichert werden können. Dies ermöglicht es Unternehmen, Fehler in einem Prozess zu finden, den Lebenszyklus ihrer Anlagen zu bewerten und Lücken in einem Verfahren zu finden. Unternehmen gewöhnen sich mehr und mehr an den Umgang mit Big Data und deren Integration mit IIoT und der Cloud. Dadurch können sie bessere Vorhersage- und Planungsmodelle erstellen, wie z. B. bei der Produktionsplanung und -steuerung und im Falle der integrierten Lieferkettenplanung zur Verbesserung von Produktivität und Gewinn (Zheng et al., 2021). Selbst große Unternehmen können Daten aus mehreren Produktionsstätten nutzen, um ein vollständigeres Bild ihrer Abläufe zu erhalten, und der Einsatz von KI und maschinellem Lernen (ML) kann den Umgang mit diesen Daten weiter verbessern.

### Intelligente Fabrik

Die intelligente Fabrik (auch Smart Factory) ist ein wichtiger Baustein der Industrie 4.0 und war bisher nicht leicht zu erreichen. Das liegt daran, dass es keine Anbieter gab, die die gesamte Technologie, die für die Umsetzung erforderlich war, zur Verfügung stellten. Eine echte intelligente Fabrik besteht aus integrierten Lösungen und vollständig vernetzten Fertigungssystemen, die die für die Produktion von Waren erforderlichen Daten ohne menschliches Zutun erzeugen, empfangen, verarbeiten und übertragen (Osterrieder et al., 2020). Heute bestehen die meisten Unternehmen, die sich für den Industrie-4.0-Ansatz entscheiden, aus einigen wenigen Komponenten der intelligenten Fabrik. Die Technologie ist profitabler geworden, da Startups verschiedene Lösungen für Technologiekomponenten anbieten, wie z. B. autonome mobile Roboter, Cybersicherheit, künstliche Intelligenz, Kommandozentralen und Videoanalyse, die früher oft lokale und personalisierte Lösungen erforderten. In diesem Sinne ist es von entscheidender Bedeutung, die wichtigsten Anforderungen und Herausforderungen zu identifizieren, die sich aus den neuen verfügbaren Technologien ergeben, um den Herstellern die nötige Anleitung für die Implementierung einer intelligenten Fabrik im Kontext der Industrie 4.0 zu geben (Shi et al., 2020).

### Bildverarbeitungssysteme und autonome mobile Roboter

Vor dem Hintergrund der hohen Produktions- und Materialkosten in der Industrie 4.0 sehen sich die Unternehmen gezwungen, die Arbeitseffizienz zu steigern und Qualitätsfehler zu reduzieren: Autonome mobile Roboter (AMRs) und Bildverarbeitungssysteme sind notwendige Elemente, um diese Ziele zu erreichen. Der Einsatz von autonomen mobilen Robotern nimmt in der Industrie zu, und sie haben eine Koexistenz mit Menschen erreicht, indem sie ihre Stärken und Grenzen teilen und sicher zusammenarbeiten. AMRs erhöhen die Effizienz bei der Automatisierung sich wiederholender Aufgaben, da sie schnell und ohne Pause arbeiten können, was die Produktivität erhöht und, da sie programmierbar sind, was die Flexibilität der Fertigung verbessert (Goel & Gupta, 2020; Fragapane et al., 2022). Bildverarbeitungssysteme sind unentbehrlich, um Fehler oder Defekte schnell zu erkennen, bevor sie sich auf die gesamte Produktionslinie auswirken. Bildverarbeitungssysteme sind Teil neuer Qualitätskontrollsysteme für Messzwecke, die zu erheblichen Verbesserungen von Qualität und Sicherheit führen und zusammen mit anderen visuellen Technologien wie Virtual Reality oder Augmented Reality eine wichtige Rolle in der Industrie 4.0 spielen (Alonso et al., 2019).

### Fragen zur Selbstkontrolle

1. Nennen Sie drei der wichtigsten Trends in der Industrie 4.0.

*Prädiktive Wartung*

*Cybersicherheit*

*Big Data*

*Intelligente Fabrik*

*Bildverarbeitungssysteme*

*Autonomen mobile Roboter.*

1. Welche der folgenden Aussagen sind zutreffend?

* Die Implementierung von Systemen zur prädiktiven Wartung ist einfach.
* *Cyberangriffe sind nicht das Ziel von Cyberkriminellen, sondern eher das Mittel, um andere Ziele zu verfolgen.*
* *Große Unternehmen können Daten aus mehreren Produktionsstätten verwenden, um sich ein vollständigeres Bild von ihrem Betrieb zu machen.*
* Autonome mobile Roboter in der Industrie haben aufgrund ihrer Stärken und Grenzen keine Koexistenz mit Menschen erreicht.

Zusammenfassung

Seit seinen Ursprüngen hat der Mensch nach Möglichkeiten gesucht, seine Arbeit mit möglichst geringem Aufwand zu erledigen. Deshalb hat die Technik eine fundamentale Rolle im menschlichen Leben gespielt und zur Erfindung von Maschinen geführt, die Aufgaben mit wenigen Bedienern und/oder ohne körperliche Anstrengung lösen. Die Bewässerungssysteme in Babylon sind die ersten Systeme, die bewusst automatisiert wurden. Die ersten wichtigen Beiträge stammen von den Griechen, angefangen bei den antiken Philosophen bis hin zur Schule von Alexandria, aus der Klepsydras und die Aeolipile hervorgingen. Dadurch wurden die Grundlagen der Mechanik entwickelt, während Pneumatik und Hydraulik die Basis für Regelmechanismen bildeten und zur Entwicklung der Dampfmaschine beitrugen. Als die industriellen Revolutionen aufkamen, wurde Automatisierung vor allem mit automatischen Anlagen oder Steuerungssystemen in der Fertigung, Montage oder anderen damit verbundenen Sekundärprozessen in Verbindung gebracht. Ihre Hauptaufgabe in der verarbeitenden Industrie besteht darin, das gewünschte Produktionsniveau aufrechtzuerhalten, die Qualität der Produkte zu sichern und die Sicherheit von Personal und Anlagen zu gewährleisten. Später ermöglichte die Elektrizität modernere Entwicklungen. Es folgte das Computerzeitalter mit der Entwicklung von SPS-Systemen und der Informationstechnologie. Die Industrie 4.0 brachte cyber-physische Systeme und das Internet der Dinge mit sich.

Ein wichtiges Hilfsmittel in der Automatisierung ist die Automatisierungspyramide, eine grafische Darstellung, die hilft, die verschiedenen Aufgaben in den meisten Produktionssystemen nachzuvollziehen. Ausgehend von der Prozess- bzw. Feldebene (Level 0) ist es einfach, über Kommunikationsmittel (PROFIBUS, Feldbus, AS-Interface, Ethernet, LANs und WLANs) mit den entsprechenden Systemen und Geräten (Sensoren, Aktoren, SPS, PIDs, PLS, SCADA, MES und ERP) zu den anderen vier Ebenen aufzusteigen (Steuerungsebene, Prozessleitebene, Betriebsleitebene, Unternehmensebene), um die Produktions-, Steuerungs-, Überwachungs- und Geschäftsaufgaben zu erfüllen. Zum Abschluss dieser Lektion werden die Herausforderungen und Trends der Automatisierung beleuchtet: Speziell in der Industrie 4.0 werden prädiktive Wartung, Cybersicherheit, Big Data, intelligente Fabrik, Bildverarbeitungssysteme und autonome mobile Roboter als die wichtigsten Trends beschrieben und die Herausforderungen, die sich bei ihrer Umsetzung ergeben, vorgestellt.

Lektion 2 – Einführung in speicherprogrammierbare Steuerungen

**Lernziele**

Nach der Bearbeitung dieser Lektion können Sie …

… die Hardware von speicherprogrammierbaren Steuerungen (SPS) verstehen.

… funktionale Elemente der internen SPS-Architektur unterscheiden.

… verschiedene Typen von SPS-Eingangs- und Ausgangsmodulen und -Geräten erkennen.

… die Kontaktplan- und Funktionsbausteinprogrammierung beschreiben.

… die Methoden der SPS-Programmierung erklären.

2. Einführung in speicherprogrammierbare Steuerungen

## Einführung

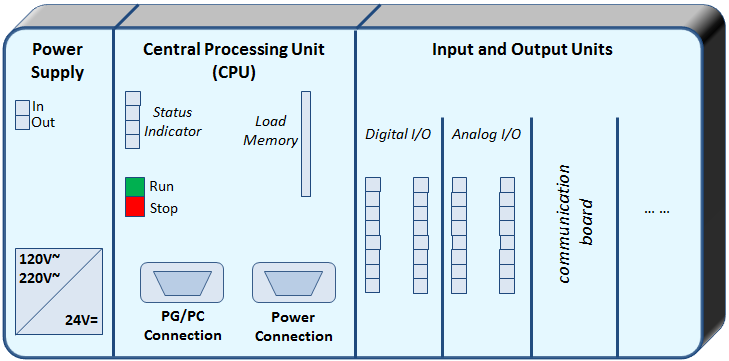
Speicherprogrammierbare Steuerungen (SPS) sind fortschrittliche, mikroprozessorbasierte Computergeräte, welche die Steuerung und Überwachung einer Vielzahl von industriellen Anlagen und vollständig automatisierten Systemen ermöglichen. Sie überwachen den Status der an ihre Eingänge angeschlossenen Geräte und treffen Entscheidungen basierend auf einem Programm, das die an ihre Ausgänge angeschlossenen Geräte steuert. (Dey & Sen, 2020).

Ursprünglich arbeiteten SPS-Systeme nur mit logischen Ein- und Ausgängen. Im Laufe der Zeit haben sich SPS-Systeme weiterentwickelt und können heutzutage sowohl digitale als auch analoge Signale verarbeiten, und einige verfügen sogar über Module zur Regelung. Diese leistungsstarken Geräte sind für die meisten Produktions-, Fertigungs- und Montageprozesse geeignet und erfordern dank ihrer einfachen Funktionsweise lediglich geringe Computerkenntnisse zur Bedienung (Metha & Reddy, 2015). Es ist von entscheidender Bedeutung, die Grundprinzipien von SPS-Systemen zu verstehen und zu wissen, wie sie in der Industrie und in Produktionsprozessen eingesetzt werden. In dieser Lektion werden wir SPS-Systeme von Grund auf vorstellen, beginnend bei der Hardware. Anschließend erläutern wir anhand der internen Architektur die Funktionseinheiten eines SPS-Systems sowie deren Funktionsweise. Wir werden uns auch mit Eingangs- und Ausgangssystemen befassen und in einem Abschnitt über Kontaktplan- und Funktionsbausteinprogrammierung zwei der gängigsten Programmiersprachen kennenlernen. Die Lektion schließt mit einem Abschnitt über Programmiermethoden ab, in dem es um die Beschreibung, den Steuerungsalgorithmus, die Anforderungen und das Logikschema als methodische Elemente geht.

## 2.1 Hardware

Entsprechend ihrer Grundfunktionen besteht die einfachste SPS aus einer Stromversorgungseinheit (Netzteil), einer Zentraleinheit (CPU) mit Speicher- und Verarbeitungseinheiten sowie Ein- und Ausgabeeinheiten (oder Signaleinheiten), wie in der folgenden Abbildung dargestellt. Das Netzteil ist verantwortlich für die Umwandlung der Hauptspannung (120-220 V) von Wechselspannung (VAC) in niedrige Gleichspannung (DC), die in einer SPS normalerweise 24 Volt Gleichstrom (VDC) beträgt (Mayol i Badía, 1988). Dieses Netzteil befindet sich normalerweise in Form eines externen Zusatzmoduls neben oder in der Nähe der CPU. In kleinen oder Mini-SPS-Systemen kann die Stromversorgung gelegentlich auch für die Versorgung von Feldgeräten verwendet werden, jedoch ist in der Regel eine externe Wechselstrom- oder Gleichstromversorgung erforderlich. Die CPU einer SPS setzt sich aus zwei grundlegenden Komponenten zusammen: dem Prozessor und dem Speicher. Die Bauweise der Module variiert. Sie können ein einzelnes Modul umfassen, das sowohl den Prozessor als auch den Speicher enthält, oder sie können aus getrennten Prozessor- und Speichermodulen bestehen. Es gibt auch Module in der Größe eines Racks oder Schrankes. Bei manchen Modellen beinhaltet das Modul die Stromversorgung, und bei Mini-SPS-Systemen enthält es normalerweise einen Teil des E/A-Systems (Mayol i Badía, 1988).

SPS-Hardware – Aufbau



Quelle: Rojas (2022), basierend auf Heinrich et al. (2020).

Es gibt verschiedene Module für E/A-Einheiten. Es gibt verschiedene Module für E/A-Einheiten. Diese Module können entweder digitale oder analoge Signale erfassen. Es gibt auch Funktionsmodule, die komplexere oder zeitkritische Prozesse bearbeiten (z. B. Zählermodule) oder Kommunikationsmodule, die Daten über Bussysteme oder WLAN verarbeiten (Heinrich et al, 2020). Um die CPU zu schützen, werden in diesen Modulen Maßnahmen wie Störungsunterdrückung, Pegelumwandlung, Kodierung und galvanische Isolierung der Signale durchgeführt. Der Signalzustand „1“ steht dabei für das positive oder höhere Potential und der Signalzustand „0“ für das Referenz- oder Massepotential. Ein offener Eingang oder ein Drahtbruch wird ebenfalls als Signalzustand „0“ interpretiert. Analoge Signale könne nicht direkt verarbeitet werden. Die analogen Module empfangen die Signale und wandeln sie zunächst in digitale Signale um (Heinrich et al., 2020).

Die CPU einer SPS kann an ein Programmiergerät (PG) oder einen PC angeschlossen werden, um das Programm des Anwenders auszulesen oder um Fehler zu beheben (Mayol i Badía, 1988). Der Netzwerkanschluss ermöglicht es, die Steuerung mit lokalen oder zentralen Netzwerken zu verbinden. Es gibt auch eine Vielzahl anderer Komponenten, die zusätzlich zur Basis-SPS verfügbar sind, wie zum Beispiel Bedieneinheiten.

Die Bediener:innen können mit dem System des Programmiergeräts über das Terminal oder die Programmierkonsole kommunizieren. Die grundlegenden Funktionen dieser Konsolen sind:

* Übertragung und Änderung von Programmen
* Überprüfung der Programmierung
* Informationen über die Funktionsweise der Prozesse

Es gibt Programmierkonsolen, die speziell für SPS-Systeme entwickelt wurden. Beispiele dafür sind Handheld-Geräte oder ein PC mit spezieller Software, die auf die Lösung von Programmier- und Steuerungsproblemen ausgerichtet ist (Mayol i Badía, 1988).

### Fragen zur Selbstkontrolle

1. Nennen Sie die drei Einheiten, aus denen die einfachste SPS besteht, entsprechend ihrer Grundfunktionen.

*Stromversorgungseinheit*

*Zentraleinheit (CPU) mit Speicher- und Verarbeitungseinheit*

*Eingangs- und Ausgangseinheiten oder Signaleinheiten*

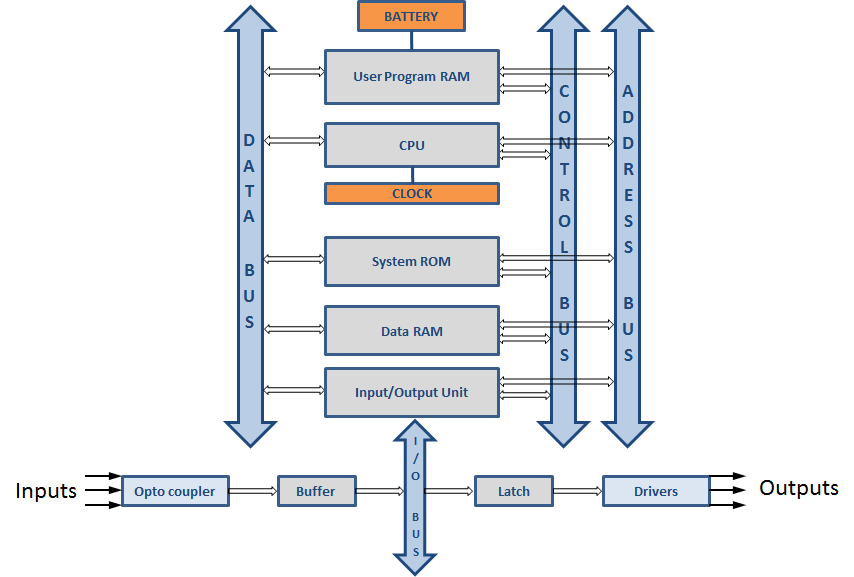
1. Bitte vervollständigen Sie den folgenden Satz.

Die Anwender:innen benötigen nur *geringe* Computerkenntnisse, um mit *SPS-Systemen* zu arbeiten, da ihre Funktionen *unkompliziert* sind.

## 2.2 Interne Architektur

Die grundlegende interne Architektur einer SPS besteht aus einer CPU, die den System-Mikroprozessor sowie die verschiedenen Speicher (Anwenderprogramm-RAM, System-ROM und Daten-RAM) und die E/A-Schaltkreise enthält (Metha & Reddy, 2015). Die CPU steuert und verarbeitet alle Vorgänge innerhalb der SPS. Nachfolgend sehen wir ein Beispiel für die grundlegende interne Architektur einer SPS:

SPS-Architektur

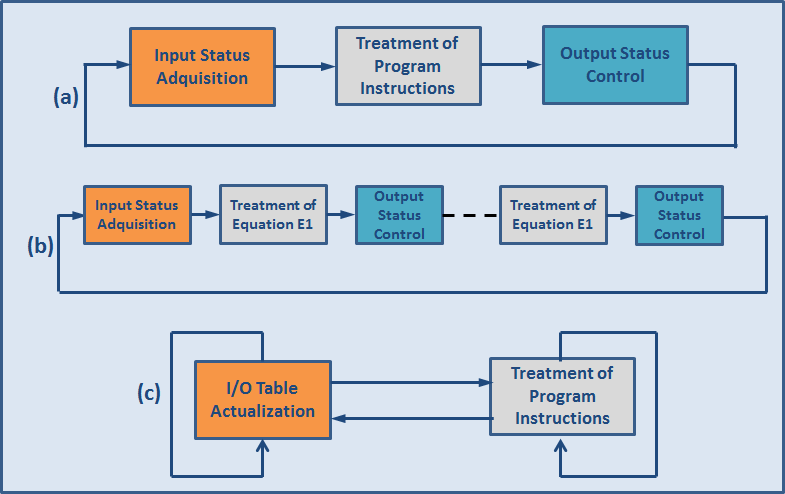


Quelle: Rojas (2022), basierend auf Metha & Reddy (2015).

Der Prozessor kommuniziert mit den verschiedenen Komponenten mittels eines Busses (bzw. einer Datenleitung), Adressen und Steuersignalen. Ein Bus kann aus Leiterbahnen auf einer Platine oder aus Drähten in einem Flachbandkabel bestehen, die als physische Leiter des elektrischen Signals dienen. Seine Hauptaufgabe besteht darin, die Anweisungen des Benutzerprogramms oder der Anwendung zu lesen und Lösungen anhand des Zustands der Eingänge und Ausgänge des Systems zu finden. Wie der Name schon sagt, wird der Datenbus verwendet, um Daten zwischen den einzelnen Komponenten auszutauschen. Der Zugriff auf verschiedene gespeicherte Daten erfolgt über den Adressbus und interne Steuerungsaktionen werden mittels Signalen über den Kommunikationsbus durchgeführt. Der E/A-Bus dient zur Kommunikation zwischen den E/A Modulen und der E/A-Einheit. Die Betriebsgeschwindigkeit der SPS wird durch einen internen Taktgeber bestimmt, der in der Regel eine Frequenz zwischen einem und acht Megahertz (MHz) hat und die Zeitsteuerung und Synchronisierung aller Systemkomponenten sicherstellt (Metha & Reddy, 2015).

Die Aufgaben innerhalb einer SPS werden in Zyklen ausgeführt, da die Informationsverarbeitung aufgrund der Beschaffenheit des Prozessors sequenziell erfolgt. Dieser zyklische Ablauf wird als Ausführungszyklus bezeichnet und durch eine Reihe von Operationen sowie eine Ausführungs- oder Zykluszeit definiert (Programmablaufzeit; Mayol i Badía, 1988). Die folgende Abbildung zeigt die verschiedenen Möglichkeiten, wie die definierten Operationen des Ausführungszyklus einer SPS ausgeführt werden können. Schema a () zeigt den Grundzyklus. Schema (b) stellt die Gruppierung von Eingängen/Ausgängen nacheinander dar, und Schema (c) zeigt unabhängige Zyklen der Ausführung und E/A-Erfassung. Diese Zyklen können nur geändert werden, wenn unter den Anweisungen, die dem Benutzer für die Programmierung zur Verfügung stehen, bedingte Sprünge, Sprünge zu Unterfunktionen oder Unterprogrammen, Unterbrechungen oder sofortige Aktualisierungen von E/A-Zuständen sind (Mayol i Badía, 1988).

SPS-Ausführungszyklus



Quelle: Rojas (2022), basierend auf Mayol i Badía (1988).

### Fragen zur Selbstkontrolle

1. Nennen Sie die drei verschiedenen Speicher, die in der CPU einer grundlegenden internen Architektur einer SPS enthalten sind.

*Anwenderprogramm-RAM*

*System-ROM*

*Daten-RAM*

1. Was ist die typische Frequenz des internen Taktgebers der SPS?

* Zwischen 100 Kilohertz (kHz) und 900 kHz
* *Zwischen einem und acht MHz*
* Zwischen 10 und 20 MHz

## 2.3 E/A

Um eine Maschine oder einen Prozess zu steuern, ist ein kontinuierlicher Informationsaustausch zwischen der SPS und dem jeweiligen Prozess erforderlich. „Eingänge“ bezieht sich auf alle Informationen, die vom Prozess gesammelt werden, während „Ausgänge“ Steuerungsmaßnahmen darstellen, die an der Maschine oder dem Prozess durchgeführt werden (Karaali, 2018). In der Automatisierungstechnik sind Signalgeneratoren und Leistungsverstärker die Eingangs- und Ausgangsgeräte zur Steuerung von Schaltungen oder Geräten. Manchmal überwachen sie die Inbetriebnahme von Steuerungssystemen mit Hilfe von Elementen, die vom Bediener manuell betätigt werden, wie Tasten, Schalter, Knöpfe oder Pedale. Sie können auch von externen Geräten wie Endschaltern, Fotozellen, Temperatursensoren, Drucksensoren, Zeitgebern und Relais eingestellt werden. Ausgangsgeräte sind für die Stromversorgung von Ausgangssignalen zuständig, die von Steuersystemen erzeugt werden, und sie werden auch verwendet, um Motoren oder Ventile durch Ein- und Ausschalten zu steuern. Im Allgemeinen werden diese Aktoren als Elemente beschrieben, die als Leistungsverstärker dienen, um das System auf eine bestimmte Weise zu beeinflussen. Diese können klassifiziert werden als (Karaali, 2018)

* + elektromechanische Aktoren, die mechanisch, manuell, pneumatisch, hydraulisch oder elektrisch gesteuert werden.
  + elektromagnetische Aktoren (Relais und Schütze); und
  + elektronische Aktoren (Dioden, Transistoren und Thyristoren).

Das E/A-System einer industriellen speicherprogrammierbaren Steuerung besteht aus einer Reihe von Modulen (oder Karten) und Trägerstrukturen für die Module und Montagerahmen, die die folgenden Funktionen erfüllen (Mayol i Badía, 1988):

1. Anpassung der Betriebsspannung der elektronischen Elemente der SPS an die der Feldgeräte und umgekehrt.
2. Angemessene elektrische Trennung zwischen Stromkreisen und Logikschaltungen.
3. Ermöglichung der Identifizierung von E/A-Geräten durch die physische Unterstützung der Adresse für die korrekte Ausführung der programmierten Steuersequenzen.

In modularen Geräten bieten Rahmen oder Racks mechanischen Halt für die Module und verleihen der Hauptplatine, auf der sich die Datenbusanschlüsse befinden, Steifigkeit und Schutz. Bei den Kompaktgeräten ist das gesamte System, einschließlich aller oder eines Teils der E/A, in einem einzigen Gehäuse untergebracht. Mini-SPS-Systeme werden oft in einer kompakten Form angeboten, welche die Zentraleinheit und einen Teil des E/A-Systems in einem einzigen Gehäuse enthält, aber diese können durch kompakte Einheiten oder E/A-Module erweitert werden.

E/A-Kanäle ermöglichen die Signalkonditionierung und -isolierung. Dadurch benötigen Sensoren und Aktoren keine zusätzlichen Schaltungen und können direkt angeschlossen werden. Im Eingangskanal wandelt die SPS das Signal mittels Signalkonditionierung in eine Spannung um, die mit den Pegeln des Mikroprozessors kompatibel ist. Bei größeren SPS werden diskrete oder Ein/Aus-Signale im Bereich von 5 Volt (V), 24 V, 110 V und 240 V als Eingänge gezählt, während kleine SPS in der Regel nur eine Form von Eingang haben (z. B. 24 V).

Die elektrische Isolierung von der äußeren Umgebung erfolgt durch „Optokoppler“ (auch Opto-Isolatoren genannt). Diese Geräte bestehen aus einer Fotodiode und einem Fototransistor. Wenn ein externer digitaler Impuls die Fotodiode anregt, erzeugt dieser Lichtemitter einen Impuls aus Infrarotstrahlung. Der Fototransistor erkennt diesen Impuls, indem er eine Spannung in diesem Schaltkreis erzeugt. Der Abstand zwischen der Fotodiode und dem Fototransistor sorgt für die elektrische Isolierung. Durch die optische Kopplung kann der externe digitale Impuls jedoch einen digitalen Impuls im internen Schaltkreis erzeugen (Mayol i Badía, 1988).

Ebenso werden Signale auf den Ausgangskanälen der SPS in einer Form bereitgestellt, die den direkten Anschluss an externe Schaltungen ermöglicht. Diese Signale werden als Relaistyp, Transistortyp oder Triac-Typ spezifiziert (Bolton, 2015):

* + **Relaistyp:** Das SPS-Ausgangssignal kann Ströme in der Größenordnung von einigen Amperen in einem externen Stromkreis schalten, der in der Regel zum Betrieb eines Relais verwendet wird. Mit dem Relais wird die SPS von der externen Schaltung isoliert, und die kleinen Ströme können wiederum größere Ströme verarbeiten. Die Relaisausgänge sind für das Schalten von AC und DC geeignet. Sie widerstehen Spannungsschwankungen und hohen Stoßströmen, sind aber relativ langsam im Betrieb.
  + **Transistortyp:** Dieser ändert den Strom durch den externen Stromkreis mit Hilfe eines Transistors. Der Schaltvorgang ist in diesem Fall wesentlich schneller, aber er unterstützt keine Überströme oder Rückwärts-Hochspannung und zerstört sich selbst, wenn diese auftreten. Außerdem ist er ausschließlich für Gleichstromschaltungen gedacht. Zum Schutz wird der eingebaute elektronische Schutz oder eine Sicherung verwendet. Die Isolierung erfolgt durch Optokoppler.
  + **Triac-Typ:** Dieser dient zur Steuerung externer Lasten, die an eine Wechselstromquelle angeschlossen sind. Überstrom kann ihn sehr leicht zerstören, daher sind zu seinem Schutz immer Sicherungen und zur Isolierung Optokoppler eingebaut. Sie arbeiten ausschließlich mit AC.

Daher kann das Signal am Ausgangskanal nach der Signalkonditionierung mit Relais, Transistoren oder Triacs auf 24 V, 100 Milliampere (mA), eine Gleichspannung von 110 V, 1 Ampere (A) oder vielleicht ein Triac-Signal 240 V, 1 A AC oder 240 V, 2 A AC geschaltet werden. Bei kleinen SPS-Systemen sind alle Ausgänge typischerweise von einem Typ, z. B. 240 V oder 1 A AC. Mit modularen SPS-Systemen kann jedoch je nach Auswahl der verwendeten Module eine breite Palette von Ausgängen erzielt werden (Bolton, 2015).

Es gibt eine Konvention, die beschreibt, wie Eingangsgeräte und Ausgangslasten mit den DC-E/A-Modulen der SPS verbunden werden (Metha & Reddy, 2015). Wenn das Eingangsmodul Strom an das Eingangsgerät liefert, wird es als Source-Eingangsmodul bezeichnet. Wenn das Eingangsmodul Strom vom Eingangsgerät erhält, wird es als Sink-Eingangsmodul bezeichnet. Ähnlich verhält es sich, wenn das Ausgangsmodul Strom an eine Ausgangslast liefert, dann spricht man von einem Source-Ausgangsmodul. Wenn das Ausgangsmodul Strom von der Ausgangslast erhält, wird es als Sink-Ausgangsmodul bezeichnet. Beachten Sie, dass der klassische Stromfluss von Plus zu Minus verwendet wird. Es ist wichtig, den Typ des verwendeten Eingangs- oder Ausgangsmoduls zu kennen, damit die Geräte oder Lasten richtig angeschlossen werden. So müssen Sensoren mit Stromzufuhr an Sink-Eingangsmodule angeschlossen werden, während Sensoren, die Strom benötigen, an Source-Eingangsmodule angeschlossen werden müssen. Wenn das Gerät oder die Last an das E/A-Modul angeschlossen ist und der Strom in die falsche Richtung fließen würde, funktioniert der Stromkreis nicht und das Modul könnte beschädigt werden (Metha & Reddy, 2015).

Zu den diskreten E/A gehören auch bitorientierte Ein- und Ausgänge. In ihnen wird in jedem Bit eine vollständige und unabhängige Information dargestellt, da sie zum Beispiel vor dem Fehlen oder Vorhandensein von Strom in einem Prozesskreis warnen oder den Status eines externen Kontakts anzeigen können (Petruzella, 2017). Zusätzlich zu den beschriebenen diskreten oder Ein/Aus-E/A können SPS-Systeme digitale Signale verarbeiten. Digitale Signale sind durch mehrstellige Bitfolgen gekennzeichnet und können je nach Wertebereich verschiedene Werte annehmen. Jedem Wertebereich wird durch Kodierung eine bestimmte Bedeutung zugewiesen, z. B. ein numerischer Wert. Deshalb gibt es auch digitale oder numerische E/A-Module, die es ermöglichen, Informationen auf der Ebene von Zahlen oder Daten zu erfassen oder zu erzeugen, d. h. sie verwenden ein komplettes Register des Datenspeichers der SPS. Darunter finden wir analoge E/A-Module, solche mit numerischen Codes und solche mit speziellen Einsatzzwecken (Mayol i Badía, 1988; Heinrich et al., 2020).

### Analoge Eingangs-/Ausgangsmodule

Dies sind Module, die für die Umwandlung einer analogen Größe vorgesehen sind. Die beiden Grundtypen sind Spannung und Strom. Die Module verfügen über vom Benutzer wählbare DIP-Schalter, mit denen festgelegt werden kann, ob jeder E/A für Strom oder für Spannung genutzt werden soll. Analoge Sensoren messen eine variable physikalische Größe (Temperatur, Durchfluss, Druck usw.) in einem bestimmten Bereich und erzeugen ein entsprechendes unterbrechungsfreies Spannungs- oder Stromsignal. Im Allgemeinen erfolgt die Umwandlung in einen Binärcode mit 11 oder 12 Bits, dem ein numerischer Wert entspricht, oder vom numerischen Wert in den Binärcode (Petruzella, 2017). Ein analoges Eingangsmodul verfügt in der Regel über einen einzigen Analog/Digital-Wandler (A/D-Wandler), und die Eingangsgrößen werden für die Umwandlung gemultiplext (Mayol i Badía, 1988). Für eine größere funktionale Effektivität werden diese Module normalerweise von einem eigenen Mikroprozessor gesteuert. Unter den von den Herstellern angebotenen analogen Modulen sind die am häufigsten verwendeten diejenigen mit vier, acht oder 16 Kanälen für Eingänge und vier Kanälen für Ausgänge, die einen Digital/Analog-Wandler pro Kanal enthalten. Die möglichen Funktionsbereiche sind die üblichen in der Signalpegel-Instrumentierung: 0 bis 5 V DC, 0 bis 10 V DC, -10 bis 10 V DC und 4 bis 20 mA, die auch für die Steuerung von Geschwindigkeitsreglern und motorisierten Ventilen geeignet sind (Mayol i Badía, 1988).

### E/A-Module mit numerischem Code

Diese Module werden für die Erfassung von Daten verwendet, die über Drehgeber, Daumenschalter, Hochgeschwindigkeitszähler und digitale elektronische Instrumente bereitgestellt werden, um numerische Informationen für die Anzeige zu generieren, z. B. Sieben-Segment-Anzeigen und andere elektronische Geräte (Petruzella, 2017). Diese Module bieten eine Schnittstelle für Anwendungen, die Geschwindigkeiten erfordern, welche die Kapazität des SPS-Programms übersteigen, d. h. sie verfügen über die notwendige Elektronik, um ihre Aufgabe in Echtzeit und unabhängig vom Prozessor zu erfüllen und diese Informationen zu speichern, damit der Prozessor sie später auslesen kann. Die Hersteller bieten numerische E/A-Module an, typischerweise für BCD (Binary-Coded Decimal), Gray- oder 9er-Komplementcodes, und verwenden aus wirtschaftlichen Gründen Multiplexing. Die Eingangsmodule erfassen die Informationen von jedem der Datenpunkte mit einer Abtastfrequenz von bis zu 100 kHz und übertragen sie in die Register des Datenspeichers des Prozessors oder führen den umgekehrten Vorgang aus, wenn es sich um Ausgangsmodule handelt (Petruzella, 2017).

### Module für besondere Zwecke

Die oben beschriebenen diskreten und digitalen E/A-Module decken zwar den Einsatz von SPS-Systemen in einem breiten Spektrum von Anwendungen – etwa 90 Prozent der Einsatzszenarien – ab, doch einige Anwendungen erfordern spezielle Funktionen. In solchen Fällen müssen bestimmte Arten von Signalen oder Daten verarbeitet werden, die zwar mit den oben genannten Elementen ausgeführt werden könnten, aber einen übermäßigen Einsatz von Material und Programmanweisungen erfordern würden.

Für diese Szenarien bieten die Hersteller verschiedene Spezialmodule an, die eine effiziente Verarbeitung ermöglichen. Diese Module können auch einen eingebauten Mikroprozessor enthalten, um der Schnittstelle Intelligenz zu verleihen, weshalb sie auch als intelligente oder Prozessmodule bezeichnet werden. Sie reduzieren die Anzahl der Systemkomponenten und entlasten den SPS-Prozessor. E/A-Module für besondere Zwecke sind zwar Teil großer SPS-Systeme, wurden aber zunehmend auch in Systeme mit mittlerer Kapazität integriert (Hughes, 2015).

**Thermoelement-Eingangsmodul**

Die analogen Module sind nicht in der Lage, Signale mit niedrigem Pegel direkt von den Messwertgebern zu empfangen und erfordern den Einsatz von Signalwandlern auf Instrumentenebene. Im Falle von Thermoelement-Temperaturwandlern bieten einige Hersteller Module an, die das schwache Signal (in der Größenordnung von Millivolt) direkt annehmen und so arbeiten, als wären es analoge Eingänge (Mayol i Badía, 1988).

**Schrittmotor-Steuerungsmodul**

Dieses Modul erzeugt die zur Steuerung eines Schrittmotors erforderlichen Impulszüge 10durch den Steuerverstärker, der Umsetzer oder Treiber genannt wird. Das Modul nimmt Daten aus dem Steuerungsprogramm in der SPS entgegen, die den Weg oder die Position, die Richtung, die Beschleunigung und die Verzögerung der Bewegung angeben. Sie verfügen in der Regel über manuelle Bewegungssteuerungseingaben, um die Positionierung unter Anfangsbedingungen durchzuführen (Petruzella, 2017).

**Servo-Steuerungsmodul**

Das Servo-Steuerungsmodul ermöglicht eine ein- oder mehrachsige Positioniersteuerung und bietet kurze Positionierzeiten, hohe Präzision, gute Zuverlässigkeit und hohe Wiederholgenauigkeit, womit es für Anwendungen geeignet ist, die präzise Hochgeschwindigkeitsbearbeitungs- und -verpackungsvorgänge umfassen. Daher bietet sie eine wirtschaftliche Alternative zum Einsatz der numerischen Steuerung bei kleinen Anwendungen, die nicht die hohe Leistung der computergesteuerten numerischen Steuerung (CNC) erfordern, wie z. B. bei Transfermaschinen, Werkzeugmaschinen und Verpackungsmaschinen (Mayol i Badía, 1988).

**Proportional-Integral-Differential-Steuermodule**

Das Proportional-Integral-Differential-Steuerungsmodul (PID-Steuerungsmodul) wird in Prozesssteuerungsanwendungen eingesetzt, bei denen eine hohe Präzision bei der Steuerung einer Regelfunktion nötig ist (Petruzella, 2017). Plötzliche Abweichungen oder Sprünge der Prozessvariablen in Bezug auf den Referenzpunkt können die Produktqualität beeinträchtigen, einen übermäßigen Energieverbrauch verursachen oder sogar zu einem Verlust der Systemkontrolle führen, was eine schnelle Reaktion des Steuerungsalgorithmus erfordert. Steuerungsalgorithmen sind Programme, die komplexe mathematische Berechnungen durchführen. Das PID-Modul verhindert, dass die CPU die Prozesssteuerung übernimmt, da diese außerhalb stattfindet. Die Prozessvariable wird über einen Analogeingang ermittelt und nach der Verarbeitung mit dem Referenzpunkt verglichen. Das resultierende Fehlersignal wird direkt durch die PID-Komponenten verarbeitet, um die Steuergröße zu erhalten und sie auf das System anzuwenden. Dieses Design verhindert, dass die CPU durch komplexe Berechnungen überlastet wird und führt nur Überwachungsfunktionen für diesen Teil des Prozesses aus. Die Grundfunktion des Moduls besteht darin, die notwendigen Steuerungsmaßnahmen zu ergreifen, um die gewünschte Prozessvariable innerhalb der festgelegten Grenzen zu halten. In jedem Fall programmiert der Prozesstechniker die notwendigen Parameter des Reglers im PID-Modul, und dieses führt alle Berechnungen durch, ohne dass Programme im Speicher der SPS erstellt werden müssen (Mayol i Badía, 1988; Petruzella, 2017).

**ASCII-Modul**

Im Allgemeinen beschränkt sich die Kommunikation einer SPS auf den Informationsaustausch zwischen verschiedenen Prozessoren desselben Herstellers oder mit intelligenten Terminals, die in der Lage sind, das gleiche Protokoll zu erzeugen, das sie verwenden. Um den Datenaustausch mit nicht-intelligenten Peripheriegeräten zu ermöglichen, bieten die Hersteller ASCII-Module mit einem oder mehreren Kommunikationskanälen an, die in Bezug auf die Übertragungsgeschwindigkeit, die Informationsstruktur und die Steuer- oder Protokollcodes konfigurierbar sind (Mayol i Badía, 1988). Mit diesen Modulen lassen sich vom Benutzer geschriebene BASIC- und C-Programme ausführen. Diese Programme bieten eine schnelle und einfache Schnittstelle zwischen externen Geräten und dem SPS-Prozessor, da sie prozessorunabhängig sind. So können typische Anwendungen wie Schnittstellen für Drucker, Bildschirme, Barcode-Leser und Roboter programmiert werden. (Petruzella, 2017).

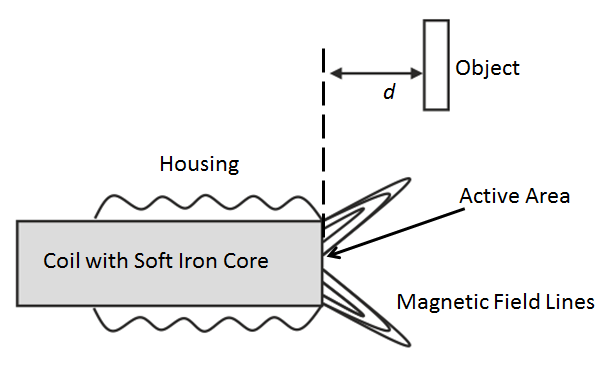
**Remote-E/A-*Module***

Remote-E/A-Module werden als Lösung für die Verteilung von Ein- und Ausgängen in großen Systemen oder hochgradig verteilten Systemen vorgestellt (Bolton, 2015). In großen Systemen ist es nicht möglich, alle Komponenten der Zentraleinheit und des Systems im selben Rack unterzubringen. Daher müssen sogenannte E/A-Expander verwendet werden, mit denen der Systembus vom Rack der CPU auf andere E/A-Strukturen erweitert werden kann. Die Verbindung zwischen den Racks erfolgt über ein mehradriges Kabel in Parallelschaltung, wodurch die Abstände zwischen den Racks begrenzt sind. Es ist kaum möglich, die Länge der Kabel zu erhöhen, da die Gefahr besteht, dass dies Störungen auf dem Systembus verursacht. Wenn sich viele Ein- und/oder Ausgänge in beträchtlicher Entfernung von der Haupt-SPS befinden, ist es sinnvoll Ein-/Ausgangsmodule in der Nähe der Prozesseingänge und -ausgänge zu installieren. Ein oder mehrere lokale serielle Verbindungsmodule sind in der Zentraleinheit installiert. Sie sind über ein Kommunikationskabel verbunden, ein einfaches abgeschirmtes Twisted-Pair-Kabel mit Remote-Strukturen und einem Remote-Verbindungsmodul, das als Controller für die Kommunikation von diesem Rack aus fungiert. Eine weitere Alternative besteht darin, die Haupt-SPS als Master-SPS zu konfigurieren, die Eingangs-/Ausgangsdaten von bzw. zu mehreren Slave-SPS-Einheiten empfängt bzw. sendet. Die Slave-SPS-Systeme enthalten nicht das Steuerungsprogramm, und das Master-SPS führt den gesamten Steuerungsprozess durch. Auch in hochgradig verteilten Systemen, in denen eine große Anzahl von Signalen gesteuert wird und E/A-Geräte über große Flächen verstreut sind, können serielle E/A-Schnittstellenmodule an entfernten Orten in der Nähe der Geräte eingesetzt werden, deren Signale gesteuert werden sollen (Bolton, 2015).

### E/A-Geräte

Dieser Unterabschnitt beschreibt kurz einige typische Eingangs- und Ausgangsgeräte, die mit SPS-Systemen verwendet werden. Dazu gehören digitale und analoge Eingangsgeräte, wie Näherungsschalter, Lichtschranken, Drehgeber, Dehnungsmessstreifen, Thermistoren und Thermoelemente. Als Ausgangsgeräte werden Relais und Motoren behandelt.

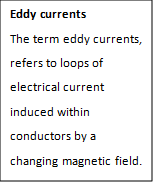
Induktiver Näherungsschalter



Quelle: Rojas (2021), basierend auf Heinrich et al. (2020).

**Näherungsschalter**

Näherungsschalter sind berührungslose elektronische Schalter, welche die benötigten Signale liefern, nämlich Einschaltpositionen, Endpositionen und Füllstände, oder als Impulsgeber für die Zählung oder Geschwindigkeitserfassung dienen (Pallas, 2005). In der Industrie erfordern die meisten automatisierten Prozesse den Einsatz von Näherungsschaltern als Übermittler von Informationen zur Steuerung. Von den bekannten Positionsdetektoren haben sich induktive und kapazitive Näherungsschalter für die berührungslose Erkennung einer Vielzahl von Materialien bewährt.

Der induktive Näherungsschalter besteht aus einer Spule mit einem Weicheisenkern, der durch einen Schwingkreis ein Magnetfeld erzeugt. Dieses Feld entsteht an einem Ende, der so genannten aktiven Fläche. Wenn ein Objekt aus einem leitfähigen Material in die Nähe der aktiven Fläche kommt, gerät es in dieses Magnetfeld und erzeugt **Wirbelströme** in dem Objekt. Dadurch wird dem Sensor Energie entzogen, wodurch die Schwingungsamplitude des Schaltkreises abnimmt. Somit ist die Amplitude der Schwingung groß, wenn sich kein Objekt vor der aktiven Fläche befindet, und sie ist klein, wenn ein Objekt vorhanden ist (Grundprinzip der zwei Positionen), was als binäres Schaltsignal wirkt (Pallas, 2005).

**Lichtschranken**

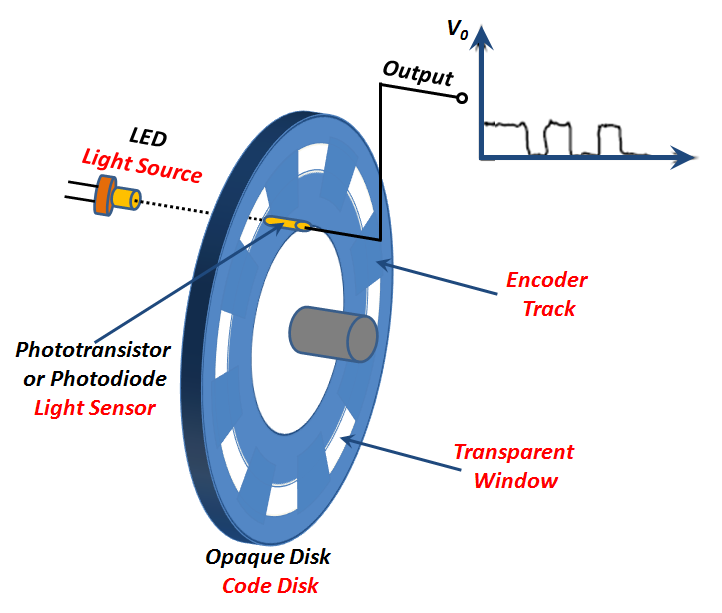
Lichtschranken verwenden in der Regel Lichtsender, die von Empfängern aufgefangen und in Schaltsignale umgewandelt werden. Lichtschranken werden je nach ihrer Funktionsweise in zwei Gruppen unterteilt: Einweg-Lichtschranken und Reflexions-Lichtschranken. Wir behandeln hier nur Einweg-Lichtschranken.

Bei Einweg-Lichtschranken befinden sich Sender und Empfänger gegenüberliegend in eigenen Gehäusen (Heinrich et al., 2020). Das Prinzip besteht darin, die Unterbrechung des Lichtstrahls zwischen dem Sender und dem Empfänger auszuwerten, unabhängig davon, wo die Unterbrechung stattfindet. Einweg-Lichtschranken ermöglichen große Reichweiten, mit exakt reproduzierbaren Schaltpunkten. Darüber hinaus bieten die Empfänger eine Empfindlichkeitseinstellung über ein Mehrgangpotentiometer. Bei diesem System werden alle Objekte, die den Lichtstrahl vollständig unterbrechen, immer erkannt. Die zu erkennenden Objekte müssen die Größe der Lichteintrittsöffnung des Empfängers vollständig abdecken. Die Funktionssicherheit von Einweg-Lichtschranken wird bei reflektierenden Oberflächen nicht beeinträchtigt, und wenn bei transparenten Objekten Probleme auftreten, kann die Erkennung durch Anpassung der Empfindlichkeit korrigiert werden (Heinrich et al., 2020).

**Drehgeber**

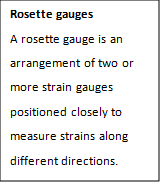
Drehgeber sind Sensoren zur Messung von Winkelgeschwindigkeiten und -verschiebungen in der industriellen Automatisierung. Dank ihrer Konstruktion sind sie verschleißfrei und ermöglichen im Allgemeinen Positionierungen und Geschwindigkeiten mit hoher Auflösung und Genauigkeit. Diese Eigenschaften haben sie für die Überwachung und Steuerung der Leistung von Robotermanipulatoren und Werkzeugmaschinen in vielen Fertigungs- und Produktionsprozessen unentbehrlich gemacht. Drehgeber wandeln Drehbewegungen in eine digitale Ausgabe um, häufig durch optoelektronische Abtastung von Impulsen, die von einer fest mit der Welle verbundenen Scheibe erzeugt werden. Je nach Art und Interpretationsmethode ihrer Ausgabe werden Drehgeber entweder als Inkrementalgeber oder als Absolutwertgeber klassifiziert (De Silva, 2016).

Schema Inkrementalgeber



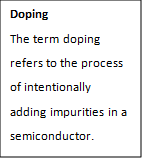
Quelle: Rojas (2021) basierend auf De Silva (2016).

**Dehnungsmessstreifen**

Als einzelner Sensor, mit dem Kraft, Drehmoment und Druck gemessen werden können, sollten Dehnungsmessstreifen (auch DMS) in Betracht gezogen werden. Sie sind einer der am häufigsten verwendeten Sensoren zur Messung von Axialkraft und Gewicht. Dabei wird die Beziehung zwischen den Verformungen des Messgeräts und der Kraft oder dem Gewicht, die diese Verformungen verursachen, ausgenutzt. Um den Druck zu messen, können Messgeräte verwendet werden, die an einer elastischen Membran in der Mitte eines Gehäuses befestigt sind. Wenn der Druck auf beiden Seiten der Membran ungleich ist, biegt sie sich und erzeugt eine messbare Dehnung in den Messgeräten. Zur Bestimmung des Drehmoments müssen die Messgeräte auf dem Material entsprechend der Richtung des zu messenden Drehmoments angeordnet werden, oder es werden **Dehnungsmessstreifen-Rosetten** verwendet. Auf diese Weise kann die vom Material erlittene Verformung mit dem Drehmoment, das die Verformung verursacht, in Beziehung gesetzt werden.

Dehnungsmessstreifen basieren auf dem piezoresistiven Prinzip: Sie werden im Allgemeinen in Form eines mäanderförmig angeordneten Drahtes gebaut, um eine größere Länge zu erreichen, und auf eine flexible Trägerfolie aufgebracht (Morris & Langari, 2020). Die Längenänderungen der Dehnungsmessstreifen sind winzig und liegen zwischen 0,1 µm und 10 µm. Das Hookesche Gesetz gibt die Längenänderung an, die sich aus der Anwendung einer Kraft (F) auf einen Dehnungsmessstreifen ergibt, wenn dieser in der elastischen Zone bleibt. Der Widerstand erhöht sich dabei, wenn der Draht gedehnt wird (Zug) und verringert sich, wenn er zusammengedrückt wird (Druck). In jedem Fall wird die Widerstandsänderung im Allgemeinen mit einer Wheatstonebrücke ausgewertet.

**Thermistoren**

Thermistoren sind wärmeempfindliche Sensoren, die aus Halbleitermaterialien hergestellt werden, deren elektrische Leitfähigkeit zwischen der des Leiters und der des Isolators liegt (Heinrich et al., 2020). Es gibt zwei Arten von Thermistoren: Eine hat PTC-Widerstände (Positive Temperature Coefficient; Kaltleiter), die andere hat NTC-Widerstände (Negative Temperature Coefficient; Heißleiter). Die Basis der Thermistoren hängt von der Temperaturbeständigkeit des Halbleiters ab, da sich die Anzahl der Ladungsträger bei Temperaturänderungen ändert. Mit steigender Temperatur nimmt auch die Anzahl der Ladungsträger zu, wodurch sich der Widerstand verringert. Das bedeutet, dass es sich bei den meisten Thermistoren um NTC-Thermistoren handelt. Diese Abhängigkeit variiert mit dem Vorhandensein von Verunreinigungen, und wenn die **Dotierung** stark ist, erhält der Halbleiter in einem begrenzten Temperaturbereich metallische Eigenschaften mit PTC-Eigenschaften. Diese Sensoren haben einen Widerstand, der stark variieren kann, von *500 Ω* bis zu mehreren Mega-*Ω*. Der nutzbare Temperaturbereich liegt zwischen *250* und *650 ºC –* dieser Bereich kann jedoch nicht mit einem einzigen Thermistor erreicht werden. Stattdessen deckt jeder Thermistor ein kleines Intervall ab. Thermistoren werden jedoch häufig in Anwendungen eingesetzt, die eine hohe Impedanz, einen bestimmten Temperaturbereich und eine kurze Reaktionszeit erfordern (Heinrich et al., 2020).

**Thermoelemente**

Ein Thermoelement ist die Verbindung von zwei homogenen und unterschiedlichen Leitern, die seitlich isoliert und an einem Ende, der so genannten Messstelle, zusammengefügt sind. Thermoelemente als Sensoren beruhen auf dem Seebeck-Effekt oder dem thermoelektrischen Effekt, bei dem ein elektrisches Potential oder eine Spannung aufgrund eines Temperaturgefälles entlang eines elektrischen Leiters auftritt. Diese Spannung, die proportional zur Temperaturänderung am Anschlusspunkt ist, kann für Messzwecke verwendet werden.

Thermoelemente sind wichtige Sensoren und die gängigste Methode zur Temperaturmessung in der Industrie. Sie wurden in der Industrie standardisiert, damit diejenigen mit den besten Eigenschaften verwendet werden und die Beziehung zwischen der erzeugten elektromotorischen Kraft (EMK) und der Temperatur bekannt ist (Morris & Langari, 2020). Bevor ein Thermoelement an einen Eingang im Analogmodul einer SPS angeschlossen werden kann, muss seine kleine Ausgangsspannung verstärkt werden. Außerdem ist ein Schaltkreis erforderlich, um die Umgebungstemperatur auszugleichen, da der von der Thermoelement-Verbindung gelieferte EMK-Wert davon beeinflusst wird. Um eine Signalverarbeitungseinheit zu vermeiden, die eine Verstärkung und Kompensation durchführt, sowie Filter, um die Auswirkungen von Störungen durch das 50-Hz-Netz zu reduzieren, wird ein Thermoelement-Eingangsmodul verwendet. (Metha & Reddy, 2015).

**Relais**

Dabei handelt es sich um ein elektromagnetisches Gerät, die aus einem automatischen Schalter besteht, der von einem elektrischen Schaltkreis gesteuert wird und bei dem ein oder mehrere Kontakte mit Hilfe einer Spule und eines Elektromagneten betätigt werden (Brunete et al., 2020). Wenn das Befehlssignal den Elektromagneten auslöst, fließt Strom durch die Spule und erzeugt ein Magnetfeld, das mit einem oder mehreren Kontakten interagiert. Das Ergebnis ist, dass sich das Magnetfeld öffnet und schließt, wodurch andere unabhängige Stromkreise geöffnet oder geschlossen werden können. Dadurch kann ein Stromkreis mit höherer Leistung (Kraftkreis) gesteuert werden als der Stimulatorkreis (Steuerkreis), der nur eine kleine Spannungsquelle benötigt, um das Relais zu aktivieren, welche durch einen SPS-Ausgang gegeben werden kann. Den Relais sind mehrere Kontakte zugeordnet, die entweder Schließer (NO) sind, wenn der Kontakt schließt, wenn Strom durch die Spule fließt, oder Öffner (NC), wenn der Kontakt öffnet, wenn Strom durch die Spule fließt (Brunete et al., 2020).

**Motoren**

Der Gleichstrommotor ist eine elektromechanische Maschine, die durch die Umwandlung von elektrischer Energie in mechanische Energie betrieben wird. Dies erfolgt durch die Wirkung eines Magnetfelds, das dazu führt, dass sich der Motor dreht (Bolton, 2015). Er besteht aus einem rotierenden Element, das „Rotor“ oder „Anker“ genannt wird, und einem festen Element, das „Stator“ oder „Anker“ genannt wird. Der Rotor, in der Regel ein Zylinder aus elektromagnetischem Material, enthält einen Kern und viele eng beieinander liegende Schlitze, die Spulen oder Wicklungen tragen, um Gleichstrom durch den Kommutator zu liefern, der abwechselnd mit festen Bürsten in Kontakt kommt. Wenn ein Strom durch die Ankerspule fließt, werden magnetische Kräfte erzeugt, die auf den Rotor wirken und zu einer Drehung führen. Der Stator besteht aus einer Reihe fester Magnetpole um den Rotor herum, die ein Magnetfeld bilden. Die Pole können Permanentmagnete oder Spulen aus Kupferdraht auf einem Eisenkern sein. Das Feld seinerseits interagiert mit den Rotorspulen und erzeugt das Motordrehmoment, das die Rotation aufrechterhält. Die Geschwindigkeit des Motors wird durch Änderungen des Ankerstroms gesteuert. Dies wird durch eine elektronische Schaltung erreicht, die den Durchschnittswert der Ankerspannung und damit den Strom variiert, indem sie die Zeit variiert, in der die konstante Gleichstromversorgung eingeschaltet ist. Dies wird Pulsweitenmodulation (PWM) genannt und ermöglicht es der SPS, die Drehgeschwindigkeit eines Motors zu steuern, indem sie die elektronischen Schaltkreise kontrolliert, die diese Modulation verarbeiten (Bolton, 2015).

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie die drei Kategorien von Aktoren, die als Leistungsverstärker dienen.

*Elektromechanische Aktoren*

*Elektromagnetische Aktoren*

*Elektronische Aktoren*

1. Bitte geben Sie an, welches Signal, das von den SPS-Ausgangskanälen bereitgestellt wird, zur Steuerung externer Lasten verwendet wird, die an Wechselstromquellen angeschlossen sind.

* Relais-Typ
* Transistor-Typ
* *Triac-Typ*

1. Bitte vervollständigen Sie den folgenden Satz.

Die *E/A-Module mit numerischem Code* werden für die Erfassung von Daten, die durch *Drehgeber* bereitgestellt werden, und zur Erzeugung von *numerischen Informationen* für die Anzeige verwendet.

## 2.4 Kontaktplan- und Funktionsbausteinprogrammierung

Obwohl jeder Hersteller seine eigene Programmiersprache für seine SPS-Modelle anbietet, können Programme im Allgemeinen in drei Darstellungsarten eingegeben werden: Funktionsbausteinsprache (FBS), Kontaktplan (KOP) und Anweisungsliste (AWL), die die am häufigsten verwendeten Standardsprachen darstellen (Hughes, 2015). In diesem Abschnitt erhalten Sie eine kurze Einführung in die wichtigsten grafischen Programmiersprachen. Dazu gehören die Programmierung mit Kontaktplan, die Darstellung der wichtigsten logischen Funktionen durch ihre Verwendung und die Programmierung mit der Funktionsbausteinsprache. AWL wird nicht behandelt, da es sich um eine textbasierte Programmiersprache handelt.

### Kontaktplan (KOP)

Kontaktplan ist eine grafische Sprache, welche den elektrischen Schaltplänen sehr ähnelt, die verwendet wurden, um die fest verdrahteten logischen Abläufe darzustellen, die vor dem Aufkommen der SPS zur Prozesssteuerung verwendet wurden. Mittels Symbolen (die Kontakte, Magnetschalter, Verbindungen usw. darstellen), die einfach kombiniert und mit der entsprechenden Adresse einer Eingangs- oder Ausgangsvariablen identifiziert werden, kann der Status einer Ausgangsvariablen definiert werden. Die verwendeten Symbole entsprechen der amerikanischen Konvention gemäß den NEMA-Normen für die Darstellung von elektrischen Schaltplänen (Mayol i Badía, 1988). Diese Sprache drückt also die Steuersequenzen auf grafische Weise aus, ähnlich wie in der verdrahteten Relaistechnik.

Die folgende Tabelle enthält die Befehlssymbole, die in Kombinationen verwendet werden, um grundlegende Funktionen in Kontaktplan auszudrücken.

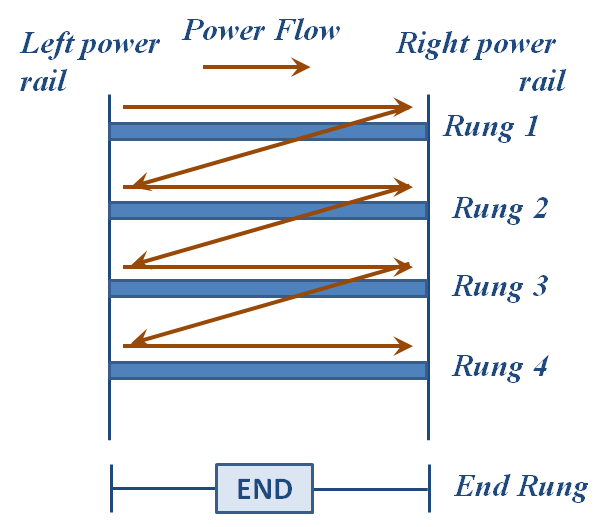
|  |  |  |
| --- | --- | --- |
| **Kontaktplan: Symbole** | | |
| **Symbol** | **Bedeutung** | **Variable** |
|  | Schließer | Diskreter E/A oder interne Variable |
|  | Öffner | Komplementäre diskrete Variable |
|  | Ausgang | Diskreter Ausgang oder interne Variable |

Quelle: Rojas (2022)

Die folgenden Konventionen werden für das Zeichnen in Kontaktplan verwendet (Bolton, 2015):

* + Die Schaltungen werden zwischen Stromschienen angeschlossen, die durch die vertikalen Linien im Plan dargestellt werden. Der Strom fließt durch die Sprossen, ausgehend von der linken Senkrechten.
  + Die Abläufe im Steuerungsprozess werden durch Sprossen auf der Leiter definiert.
  + Der Kontaktplan wird von links nach rechts und von oben nach unten gelesen. Die folgende Abbildung zeigt den von der SPS ausgeführten Programmablauf. Die letzte Sprosse des Programms muss deutlich angegeben werden, damit die SPS bei der Ausführung des Programms den gesamten Kontaktplan bis zum Ende durchläuft und dann wieder am Anfang beginnt und so eine Schleife bildet. Ein Block mit dem Wort „END“ oder „RET“ kennzeichnet die letzte Sprosse, die das Ende oder die Rückkehr anzeigt. Im Durchschnitt erfolgt der Programmablauf mit einer Ausführungsgeschwindigkeit von einer Millisekunde pro 1000 Byte Programm und liegt damit typischerweise zwischen 10 ms und 50 ms, abhängig von der Anzahl der Ausführungen im Programm.

Kontaktplan – Programmablauf



Quelle: Rojas (2022), basierend auf Bolton (2015).

* + Ein Eingang ist eine Steuerungsaktion, wie z. B. das Schließen der Kontakte eines Schalters, und ein Ausgang ist die Darstellung eines Geräts, das mit dem SPS-Ausgang verbunden ist, z. B. ein Motor. Jede Sprosse beginnt mit einem oder mehreren Eingängen und endet mit mindestens einem Ausgang. Die Ausgaben werden nicht sofort mit dem Programmablauf aktualisiert, sondern alle Ergebnisse werden gespeichert, so dass alle Ausgaben anschließend gleichzeitig aktualisiert werden.
  + Jedes elektrische Gerät wird in seinem normalen Zustand dargestellt. So wird jeder Öffner (bis er durch ein Objekt geöffnet wird) im Kontaktplan als geschlossen angezeigt. Ebenso wird jeder Schließer als offen angezeigt.
  + Ein bestimmtes Gerät beeinflusst den Status mehrerer Geräte und kann auf mehr als einer Sprosse erscheinen (z. B. ein Relais, das ein oder mehrere Geräte einschaltet). Dieses Gerät muss in jeder Situation, in der es auftaucht, mit denselben Buchstaben und/oder Zahlen beschriftet werden.
  + Speicherplatzadressen im Speicher einer SPS identifizieren alle Ein- und Ausgänge. Für ihre Beschreibung wird die vom Hersteller der SPS festgelegte Notation verwendet (Bolton, 2015).

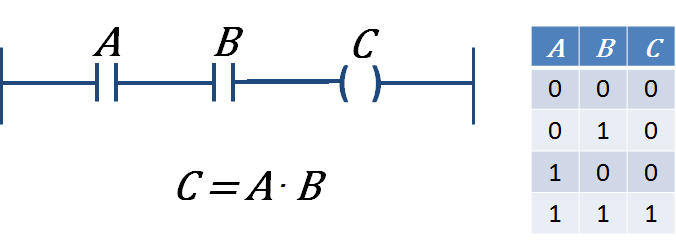
### Logische Funktionen

In der Steuerungstechnik können viele Lösungen zur Automatisierung einfach aufgebaut und direkt entworfen werden. Bei komplexeren Automatisierungsanforderungen werden jedoch kombinatorische Schaltungen benötigt, und die Prinzipien der Aussagenlogik werden durch logische Funktionen angewandt, um den Gesamtentwurf der implementierten Lösung zu vereinfachen. Logische Funktionen basieren auf dem binären Zahlensystem, so dass alle Elemente zwei Zustände haben können, wie z. B. ein Relais, das aktiviert oder deaktiviert sein kann, oder ein Ventil, das offen oder geschlossen sein kann. Die wichtigsten logischen Funktionen sind Konjunktion, Disjunktion, Inversion und deren negierten Ausprägungen (Heinrich et al., 2020).

**Konjunktion**

Die Konjunktion, auch logisches UND genannt, wird durch den Punkt-Operator (**·**) dargestellt. Sie hat zwei oder mehr Eingänge, und die Ausgangsvariable nimmt den Wert 1 (logischer High-Pegel) an, wenn ihre Eingänge gleich 1 sind. Andernfalls ist der Ausgang 0 (logischer Low-Pegel). Die Konjunktion wird in der folgenden Abbildung dargestellt, die eine UND-Darstellung mit zwei Eingängen, ihre logische Gleichung und ihre **Wahrheitstabelle** enthält.

Konjunktion und Wahrheitstabelle



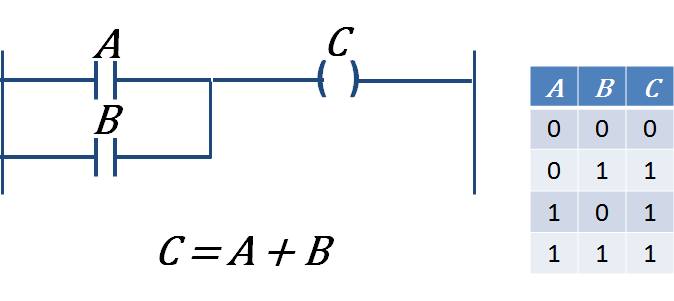
Quelle: Rojas (2022)

Der Kontaktplan beginnt mit einem Schließer mit der Bezeichnung „Eingang A“, der z. B. eine Lichtschranke darstellt, und einem Schließer mit der Bezeichnung „Eingang B“, der z. B. einen Schalter darstellt. Die Zeile endet dann mit dem Ausgang C, der z. B. einen Motor darstellt. Es kann nur dann eine Ausgabe am Ausgang geben, wenn sowohl die Kontakte von Eingang A als auch die von Eingang B geschlossen sind. Die in Reihe geschalteten Kontakte stellen die logische UND-Verknüpfung dar. Das heißt, Kontakte auf einer horizontalen Sprosse im Kontaktplan (Metha & Reddy, 2015).

**Disjunktion**

Die Disjunktion, auch logisches ODER genannt, wird durch den Plus-Operator *(+)* dargestellt. Sie kann zwei oder mehr Eingänge haben, wobei die Ausgangsvariable den Wert 1 (logischer High-Pegel) annimmt, wenn einer ihrer Eingänge gleich 1 ist. Der Ausgang ist 0 (logischer Low-Pegel), wenn alle seine Eingänge gleich 0 sind. Die Disjunktion wird in der folgenden Abbildung dargestellt, die die ODER-Darstellung mit zwei Eingängen, ihre logische Gleichung und ihre Wahrheitstabelle enthält (Hughes, 2015).

Disjunktion und Wahrheitstabelle

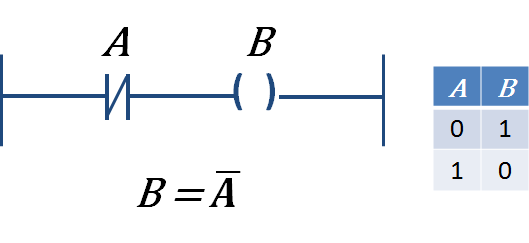


Quelle: Rojas (2022)

**Inversion**

Die Inversion, auch logischer Umkehrer oder logisches NICHT genannt, wird durch den Komplement-Operator *( ̅ )* dargestellt. Sie hat nur einen Eingang und liefert den entgegengesetzten Zustand am Ausgang, d. h. wenn die Eingangsvariable den Wert 1 (logischer High-Pegel) hat, ist ihr Ausgang 0 (logischer Low-Pegel) und umgekehrt. Die Inversion wird durch die folgende Abbildung dargestellt, die die NICHT-Darstellung im Kontaktplan, ihren logischen Ausdruck und ihre Wahrheitstabelle enthält (Hughes, 2015).

Inversion und Wahrheitstabelle

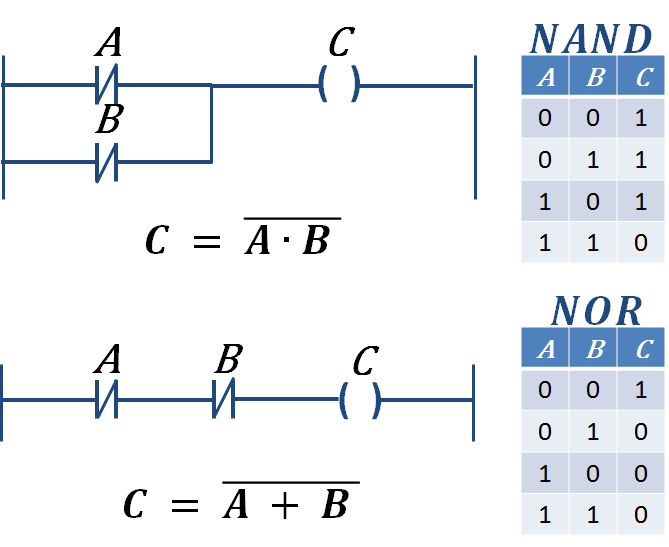


Quelle: Rojas (2022)

**Negierte Konjunktion und Disjunktion**

Die negierte Konjunktion und Disjunktion, die auch als logisches NAND (NICHT-UND) und NOR (NICHT-ODER) bezeichnet werden, sind komplementäre Ausprägungen des ursprünglichen UND bzw. ODER. Im Allgemeinen werden sie durch die Verwendung von UND- und ODER-Gattern, gefolgt von einem NICHT-Gatter, realisiert. Alternativ erhält man die gleichen Ergebnisse, wenn man an jedem Eingang ein NICHT-Gatter anbringt und ihm jeweils die entgegengesetzten Gatter folgen lässt (z. B. ein ODER-Gatter für die NAND-Funktion und ein UND-Gatter für die NOR-Funktion; Bolton, 2015). Ähnliche Ergebnisse werden mit der Kontaktplandarstellung erzielt. Die folgende Abbildung zeigt die negierte Konjunktion bzw. Disjunktion in ihrer Kontaktplandarstellung mit ihren Wahrheitstabellen.

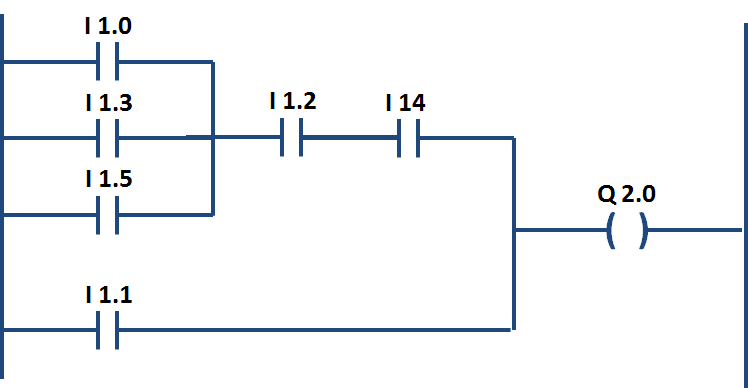
Negierte Konjunktion bzw. Disjunktion – Kontaktplandarstellung



Quelle: Rojas (2022)

Ein Beispiel für einen Kontaktplan kann wie folgt dargestellt werden: Verwenden wir eine bitorientierte Konfiguration unter Verwendung der Siemens SPS-Notation. Jedes Eingangs- oder Ausgangsmodul besteht aus Bytes mit Informationen für die SPS. Jedes seiner Bits ist nummeriert und definiert eine Adresse, die aus dem Byte und dem Bit besteht. Zusätzlich werden die Bezeichner I oder Q angegeben, um anzuzeigen, dass es sich um einen Eingang oder Ausgang handelt. Zum Beispiel geben I 3.5 und Q 2.4 die Adresse des fünften Bits im dritten Byte des Eingangsmoduls und des vierten Bits im zweiten Byte des Ausgangsmoduls an (Karaali, 2018). Gehen wir nun von der Verwendung von sechs Eingängen des ersten Bytes des Moduls aus (von I1.0 bis I1.5), die wie folgt angeschlossen sind: Die ersten drei Eingaben, I1.0, I1.3 und I1.5, bilden eine Disjunktion. Ihr Ergebnis wird mit den Eingängen I1.2 und I1.4 verbunden. Das Gesamtergebnis dieser Operation wird mit dem Eingang I1.1 zu einer zweiten Disjunktion verbunden. Schließlich erhalten wir die Ausgabe Q2.0, die zum zweiten Byte des Ausgangsmoduls gehört. Die folgende Abbildung zeigt das vorherige Beispiel in einem Kontaktplan. Nach der Analyse des Kontaktplans entspricht die Reihenschaltung der betroffenen Eingänge dem logischen UND und die Parallelschaltung dem logischen ODER, wie bereits erwähnt.

Kontaktplandarstellung



Quelle: Rojas (2022)

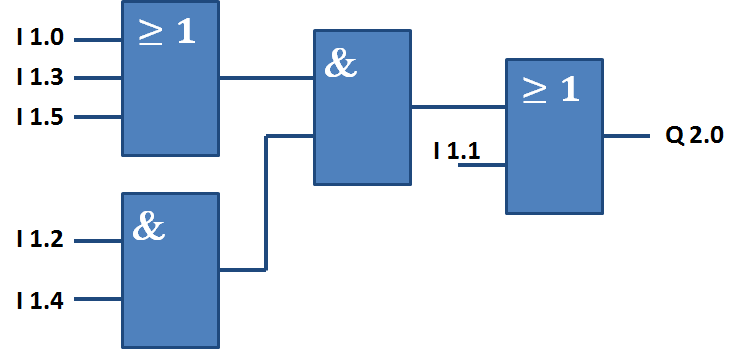
### Funktionsbausteinsprache

Eine Funktionsbausteinsprache (FBS) ist eine grafische Sprache, in der ein:e Benutzer:in Elemente (SPS-Funktionsblöcke) so programmiert, dass sie wie ein elektrischer Schaltkreis miteinander verbunden erscheinen. Dieses Funktionsblockdiagramm basiert auf standardisierten Symbolen, die für logische Funktionen stehen, die miteinander verbunden sind, um eine Steuerungsaufgabe zu realisieren. Für Logikausgänge ist es nicht erforderlich, eine Ausgangsspule zu integrieren. Stattdessen wird der Ausgang als Variable dargestellt, die den Ausgang des Blocks bezeichnet.

Das Logikfunktionsdiagramm ist besonders einfach für Techniker, die an die Arbeit mit Logikgatterschaltungen gewöhnt sind, da sie äquivalente Symbole verwenden. Zusätzlich zu den Standard- und anbieterspezifischen Logikfunktionen können Benutzer:innen ihre eigenen Funktionsblöcke mit Hilfe der FBS des IEC 1131-3-Standards konstruieren, basierend auf den Anforderungen des Steuerungsprogramms.

Die folgende Abbildung zeigt beispielsweise das vorherige Beispiel in einem Funktionsblockdiagramm. Der erste Disjunktionsblock erhält die Eingänge I1.0, I1.3 und I1.5. Dann werden die Eingänge I1.2 und I1.4 mit dem ersten Konjunktionsblock verbunden: Die Ausgänge dieser beiden Blöcke sind mit einem zweiten Verzweigungsblock verbunden, und dessen Ausgang ist mit einem zweiten Verzweigungsblock neben dem Eingang I1.1 verbunden. Schließlich erhalten wird die Ausgabe Q2.0, die zum zweiten Byte des Ausgangsmoduls gehört.

FBS-Darstellung



Quelle: Rojas (2022)

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie drei der wichtigsten logischen Funktionen, die in kombinierten SPS-Schaltungen verwendet werden.

*Konjunktion*

*Disjunktion*

*Inversion*

*Die negierten Ausprägungen davon.*

1. Bitte geben Sie an, welche der folgenden SPS-Sprachen eine textbasierte Programmiersprache ist.

* Die Funktionsbausteinsprache (FBS)
* Der Kontaktplan (KOP)
* *Die Anweisungsliste (AWL)*

## 2.5 Programmiermethoden

Aus den obigen Ausführungen lässt sich folgern, dass die Programmierung der SPS mit einer der vorgestellten Sprachen keine allzu schwierige Aufgabe ist. Um ein Problem erfolgreich zu lösen, ist es dennoch wichtig, es zu definieren und zu verstehen. Denn eine adäquat beschriebene Steuersequenz erleichtert das Schreiben von Anweisungen für die Automatisierung. Um Fehler zu vermeiden, gibt es daher unabhängig vom jeweiligen Automatisierungsproblem einige Schritte, die zuvor durchgeführt werden sollten.

Zunächst sollten die erforderlichen Arbeiten und deren Kriterien definiert werden. Beispielsweise hilft es nicht, einfach zu sagen, dass ein bestimmter Verbundstoff aus einer bestimmten Anzahl und Menge von Inhaltsstoffen hergestellt werden soll. Besser ist es, anzugeben, dass der Verbundstoff mit einer Rate von m Tonnen pro Tag und bei einer maximalen Luftfeuchtigkeit von 10 Prozent produziert werden soll.

Nachdem eine Aufgabe definiert wurde, muss festgelegt werden, wie diese ausgeführt werden soll, d. h. es ist ein Steuerungsalgorithmus für die Maschine oder den Prozess zu erstellen. Es muss festgelegt werden, welche Phasen oder Teilaufgaben in welcher Reihenfolge durchgeführt werden müssen, um die gewünschte Steuerung zu erreichen. Diese Phase der Problemdefinition erfordert bereits eine Bewertung der Feldgeräte, die als Eingangs- und Ausgangsvariablen fungieren können. Bei dieser Bewertung werden die Einschränkungen berücksichtigt, die bestehende Geräte dem vorgeschlagenen Steuerungsalgorithmus auferlegen können.

Ob es sich um eine neue Anwendung oder die Umstrukturierung einer bereits im Betrieb befindlichen Anwendung handelt, beeinflusst die Art und Weise, wie die Vorbereitung der SPS-Programmierung durchgeführt wird.

### Umstrukturierung eines Systems

Wenn es um die Umstrukturierung des Systems geht, ist das Problem im Allgemeinen begrenzt, da die meisten Anforderungen perfekt definiert sind: Deren Nichteinhaltung wird die Entscheidung, die Systeminstallation zu modernisieren, definitiv beeinflusst haben.

Für diese Anwendungen können die folgenden Schritte befolgt werden:

1. Untersuchen und Verstehen der Aufgabe, die in dem aktuellen Prozess oder der Maschine ausgeführt wird.
2. Analysieren des bisherigen Algorithmus und der Steuerlogik zur Optimierung und Berücksichtigung neuer Anforderungen.
3. Zuweisen von E/A-Adressen an Feldgeräte, die die Eingangs- und Ausgangsvariablen bilden, sowie Zuweisung von Adressen an interne Variablen.
4. Übertragen der aktuellen Logikpläne (nach der Optimierung) in die Programmiersprache der verwendeten SPS.

### Neue Anwendungen

Im Falle neuer Anwendungen wird die Erfahrung des Programmierers mit ähnlichen Anwendungen einen Einfluss haben, da Programmieraufgaben subjektiv sind. In jedem Fall ist es besser, eine Arbeitsmethode zu befolgen, wie etwa die folgenden Schritte:

1. Funktionale und detaillierte Beschreibung des Systems erstellen.
2. Steuerungsverfahren bis zur Optimierung definieren.
3. Fluss- oder Phasendiagramm der Abläufe erstellen, die das Steuerungsverfahren bestimmen.
4. Ein- und Ausgangsgeräten E/A-Adressen zuweisen, ebenso wie den internen Variablen.
5. Logikpläne erstellen, die das Flussdiagramm im verständlichen Format für den Programmierer darstellen.
6. Diagramme in die für die SPS gewählte Programmiersprache übertragen.

Die Steuerungsaufgabe wird in der Regel in einem schriftlichen Dokument beschrieben, das darauf abzielt, sie so verständlich und klar wie möglich darzustellen. Die Erstellung eines Fluss- oder Phasendiagramms aus dieser Beschreibung ermöglicht eine grafische Synthese der darin definierten Abläufe. Durch die Erstellung des Diagramms wird man mit dem Steuerungssystem vertraut und man kann die Hauptsteuerungsaufgabe (den Kern des Prozesses) sowie die Neben- oder Hilfssequenzen identifizieren. Anhand des Flussdiagramms kann der Programmierer jede Sequenz in dem logischen Format seiner Wahl ausdrücken.

### Fragen zur Selbstkontrolle

1. Bitte geben Sie an, wann es erforderlich ist, ein Fluss- oder Phasendiagramm der Abläufe zu erstellen.

* Bei der Umstrukturierung eines bereits in Betrieb befindlichen Systems
* *Bei der Implementierung einer neuen Anwendung*
* Beide sind korrekt

1. Bitte vervollständigen Sie den folgenden Satz.

Zur Lösung eines SPS-*Programmier*problems ist es notwendig, *eine Aufgabe* zu definieren und *die Art und Weise* festzulegen, in der sie ausgeführt werden kann.

Zusammenfassung

Speicherprogrammierbare Steuerungen gelten als zentrale Instrumente der Automatisierungstechnik. Für das Verständnis in diesem Bereich ist es unerlässlich, zu wissen, wie diese Geräte aufgebaut sind, wie sie funktionieren und wie sie zur Entwicklung von Automatisierungsaufgaben in Produktion und Fertigung eingesetzt werden. Im Abschnitt über die Hardware werden die Komponenten einer einfachen SPS beschrieben und wie diese bei der Ausführung der programmierten Steuerungsaufgaben zusammenwirken. Zudem werden die verschiedenen Arten von Modulen beschrieben, die mit der SPS verwendet werden können, sowie die Programmiergeräte, die benutzt werden können. Der Abschnitt über die interne Architektur beschreibt die CPU mit ihrem Mikroprozessor, ihre Speicher und ihre Eingangs-/Ausgangsschaltungen sowie die Arbeitsgeschwindigkeit und die zyklische Art und Weise, wie eine SPS ihre Aufgaben ausführt. E/A-Systeme, die die Eigenschaften von Elementen beschreiben, die als Ein- und Ausgänge für die SPS gelten, werden im folgenden Abschnitt beschrieben, zusammen mit der Art und Weise, wie E/A-Kanäle für die Signalkonditionierung und Isolierung sorgen. Außerdem wird auf die wichtigsten E/A-Module eingegangen, die von einer SPS verwendet werden, und es werden verschiedene E/A-Geräte vorgestellt, die üblicherweise zur Durchführung von Überwachungs- und Steuerungsaufgaben verwendet werden. Im folgenden Abschnitt werden Kontaktplan und die Funktionsbausteinsprache als die wichtigsten grafischen Programmiersprachen vorgestellt, die mit SPS-Systemen verwendet werden. Außerdem enthält der Abschnitt eine Darstellung der wichtigsten logischen Funktionen, die in den kombinatorischen Schaltungen einer SPS mit diesen Sprachen verwendet werden. Schließlich werden im Abschnitt über Programmiermethoden die Schritte vorgestellt, die helfen, Fehler zu minimieren, wenn eine Systemumstrukturierung oder eine neue Anwendung zur Lösung eines Automatisierungsproblems erforderlich ist.

# Lektion 3 – Batch-Automatisierung

**Lernziele**

Nach der Bearbeitung dieser Lektion …

… verstehen Sie die Grundlagen von Batch-Prozessen.

… kennen Sie die drei Kriterien für die Kategorisierung von Batch-Prozessen.

… können Sie die Automatisierungsfunktionen unterscheiden, die für Batch-Prozesse benötigt werden.

… die drei idealen Reaktorsysteme identifizieren.

… die drei grundlegenden Konfigurationen der Batch-Destillation unterscheiden.

# 3. Batch-Automatisierung

## Einführung

## Die ersten Produktionssysteme wurden automatisiert, um die höchstmögliche Produktionsrate zu den niedrigsten Kosten bei möglichst wenigen menschlichen Eingriffen zu erreichen. Infolgedessen standen durchgehende Fließbänder und die Massenproduktion im Mittelpunkt der Entwicklung (Smith, 2002). Batch-Prozesse oder Laborprozesse in größerem Maßstab wurden jedoch nie verworfen: Sie wurden für neue Produktionsanlagen und für die Herstellung von Spezial- und Feinchemikalien benötigt, wobei die Anforderungen und der Schwerpunkt zunehmend auf hoher Qualität lagen (Barker & Rawtani, 2004). Sie gewannen an Bedeutung, als sich die Fertigung von der Massenproduktion zu einer stärker kundenorientierten Produktion verlagerte, welche die Bedeutung der Herstellung von Produkten in aufeinanderfolgenden Schritten, auch bekannt als Batch-Prozesse, hervorhebt (Heinrich et al., 2020). Diese Lektion führt in die Grundlagen der Automatisierung von Batch-Prozessen und ihre wichtigsten Anwendungen ein.

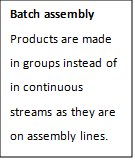
## 3.1 Grundlagen

Produktionssysteme umfassen alle Prozesse, die materielle Güter und Energie produzieren, die Umwandlung eines Materials oder Produkts mit Hilfe von Energie und Informationen sowie alle Montageprozesse und damit verbundene sekundäre Aktivitäten (Heinrich et al., 2020). Die Prozesse können je nach Arbeitsbereich und Produktionsverfahren klassifiziert werden. Smith (2014) klassifiziert die Prozesse als kontinuierlich, Batch und Semi-Batch, während Barker & Rawtani (2004) sie als kontinuierlich, diskret und Batch klassifizieren. In der vorliegenden Darstellung werden beide Sichtweisen berücksichtigt und Prozesse wie folgt klassifiziert:

* **Kontinuierlicher Prozess:** Dieser ist dadurch gekennzeichnet, dass ein ununterbrochener – also „kontinuierlicher“ – Material- oder Produktfluss aufrechterhalten wird. Produktionsanlagen arbeiten ohne Unterbrechung und verarbeiten durchgehend Materialien zu Produkten. Die Produktion steht nur selten still; hin und wieder sind kleinere Unterbrechungen zu Wartungszwecken erforderlich (Barker & Rawtani, 2004; Smith, 2014).

1. **Diskreter Prozess:** Dieser zeichnet sich dadurch aus, dass die Produktion von Produkten in diskreten Mengen bzw. nach Einheiten erfolgt. Die Produkte behalten nach der Verarbeitung ihre Form und können in der Regel gekennzeichnet werden, um sie von anderen Produkten zu unterscheiden. Die Produkte, die aus denselben Rohstoffen hergestellt werden, umfassen eine große Anzahl von Einheiten. Die Produktion bewegt sich zwischen den Arbeitsstationen in Gruppen von Teilen oder in bestimmten Mengen von Produkten (Barker & Rawtani, 2004; Hawkins & Fisher, 2006).
2. **Batch-Prozess:** Dieser liegt vor, wenn ein Produkt am Ende des Prozesses aus einer bestimmten Menge an Material oder einer Charge besteht. Die Produktionsanlagen arbeiten unter unterschiedlichen Bedingungen, während das Produkt den Herstellungsprozess durchläuft. Die Verarbeitung einer Charge erfolgt in einem definierten Zeitintervall, in dem sowohl für kontinuierliche als auch für diskrete Prozesse charakteristische Aktivitäten durchgeführt werden. Diese Prozesse wiederholen sich im Allgemeinen zyklisch (Barker & Rawtani, 2004; Smith, 2014).
3. **Semi-Batch-Prozess:** Dieser ist insofern einzigartig, als der größte Teil des Prozesses kontinuierlich abläuft, andere Teile jedoch in Chargen, weshalb man sie auch als semi-kontinuierlich bezeichnen könnte (Smith, 2014).

### Batch-Prozesse

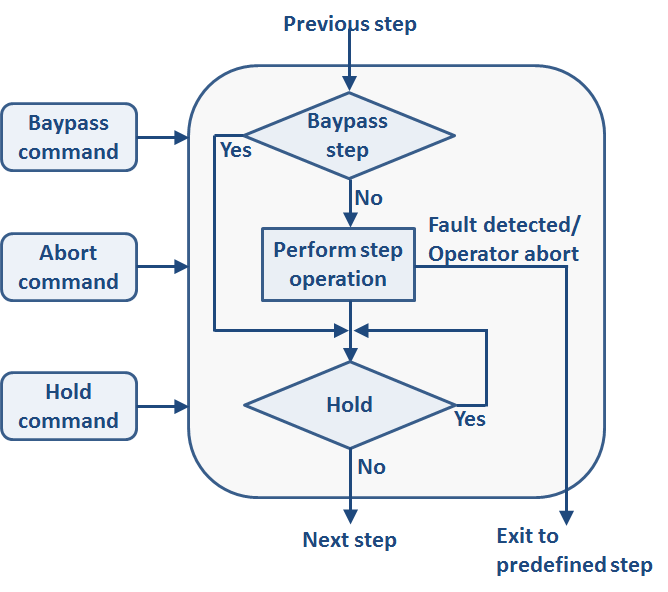
Im Allgemeinen werden Batch-Prozesse als Prozesse definiert, bei denen im Voraus festgelegte Mengen von Einsatzstoffen einer Reihe von Prozessaktivitäten unterzogen werden. Diese Aktivitäten werden in geordneter Weise mit einer oder mehreren Anlagen über einen abgegrenzten Zeitraum hinweg durchgeführt, um schließlich eine bestimmte Menge des fertigen Produkts zu erhalten. Nachfolgende Chargen des Produkts werden in der gleichen Abfolge von Schritten und mit den gleichen Mengen an Rohstoffen hergestellt (Barker & Rawtani, 2004). In ähnlicher Weise werden an einer **Batch-Montagestation** alle Teile und Komponenten bereitgestellt, die für die Ausführung der Aufgabe benötigt werden. Innerhalb jeder Charge agiert die Station wie ein Fließband, das jeweils ein Produkt bearbeitet und den Prozess so oft wiederholt, wie es für die Fertigstellung der Charge erforderlich ist (Thomopoulos, 2014).

Nach Barker & Rawtani (2004) ist bei Batch-Prozessen Folgendes üblich:

* sie arbeiten mit diskreten Mengen von Produkten oder Rohstoffen
* sie ermöglichen die Verfolgung dieser diskreten Mengen von Produkten oder Rohstoffen
* sie umfassen die Übertragung diskreter Produkte von einem Verarbeitungsbereich zu einem anderen
* sie ermöglichen die gleichzeitige Verarbeitung mehrerer Produkttypen, sofern die Produkte durch die Anordnung der Anlagen getrennt sind
* sie folgen den Verarbeitungsanweisungen oder Rezepten für jede Ladung des zu verarbeitenden Rohmaterials
* ihre Logik in Bezug auf die Verarbeitung ist komplexer als die von kontinuierlichen Prozessen
* sie enthalten Standardschritte, die fehlschlagen können, so dass für den Fall eines Fehlers besondere Schritte vorgesehen sind

Die folgende Abbildung zeigt einen typischen Batch-Prozess-Schritt.

Typischer Batch-Prozess-Schritt



Quelle: Rojas (2022), basierend auf Barker & Rawtani (2004).

Batch-Prozesse sind im Allgemeinen flexibel und können eine Reihe von Produkten innerhalb einer Anlage herstellen (Smith, 2014). Produktchemiker erstellen Anweisungen in einer Form, die einem Kochrezept ähnelt: Die Liste der Zutaten wird jedoch als „Formel“ oder „Rezeptur“ bezeichnet und die Anweisungen werden „Verfahren“ oder „Prozessanweisungen“ genannt. Chemiker geben die Formel oft auf der Grundlage einer Standard-Chargengröße an, z. B. 500 Kilogramm (kg), die dann zur Berechnung der Verhältnisse zur Größe der Produktionsanlagen verwendet wird. Ähnlich wie bei Rezepten gehen Chemiker oft schrittweise vor, um klar auszudrücken, was mit den Rohstoffen getan werden muss, um eine Produktcharge zu erhalten (Smith, 2014).

### Klassifizierung von Batch-Prozessen

Batch-Prozesse können anhand von drei Kriterien kategorisiert werden. Jede dieser Kategorien wird hier beschrieben.   
**Kategorisiert nach Formel und Verfahren**

Diese Batch-Prozesse sind mit dieser Kategorie verbunden:

* **Zyklischer Batch-Prozess:** Charakterisiert durch die Verwendung einer konstanten Formel, die sicherstellt, dass die Verarbeitungsmengen von einer Charge zur nächsten gleich bleiben. Das Verfahren verwendet den gleichen Prozess zur Herstellung jeder Charge. Ein Beispiel für eine zyklische Charge ist die Katalysatorregeneration für einen Reformer (Smith, 2014).
* **Mehrstufiger Batch-Prozess:** Charakterisiert durch den Einsatz einer jeweils anderen Formel pro Charge, müssen die Parameter jedes Mal neu festgelegt werden. In manchen Fällen werden die Parameter aus einer vorherigen Charge wiederholt, aber der Bediener muss deren Werte überprüfen, bevor eine neue Verarbeitungscharge beginnt. Wie im vorherigen Fall nutzt das Verfahren die gleiche Logik zur Herstellung jeder Charge. In diesem Zusammenhang ist der Begriff „gleich“ tolerant gegenüber kleineren Änderungen. Zu den Parametern gehört in der Regel auch eine logische Variable, die die auszuführende Aktion bestimmt. Das funktioniert hervorragend bei einer begrenzten Anzahl von Änderungen, wird aber kompliziert, wenn die Anzahl groß ist. Ein Beispiel für einen mehrstufigen Batch-Prozess ist der Batch-Zellstoffkocher (Smith, 2014).
* **Flexibler Batch-Prozess:** Wie beim mehrstufigen Batch-Prozess ist diese Art der Verarbeitung dadurch gekennzeichnet, dass für jede Charge eine andere Formel verwendet wird. Jedes Mal muss eine Reihe von Parametern angegeben werden. Das Verfahren kann in diesem Fall unterschiedliche Logiken zur Herstellung jeder Charge verwenden. Ein Beispiel für diese Art von Batch-Prozess ist der Emulsionsreaktor (Smith, 2014).

**Kategorisiert nach Menge der hergestellten Produkte**

Diese Batch-Prozesse sind mit dieser Kategorie verbunden (Barker & Rawtani, 2004):

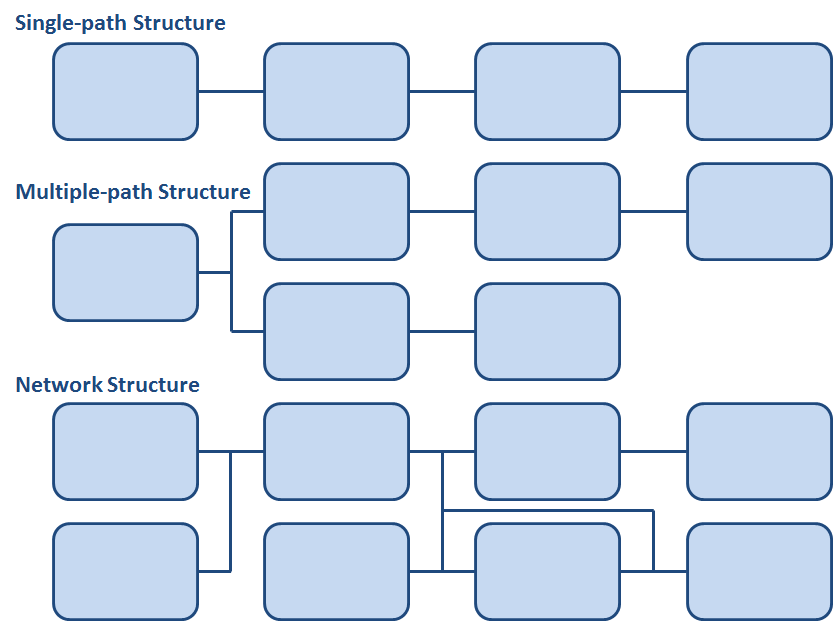
* **Ein-Produkt-Batch-Prozess:** In jeder Charge werden identische Produkte hergestellt, d. h. es werden die gleichen Arbeitsschritte durchgeführt und die gleichen Mengen an Rohstoffen verwendet.
* **Mehrstufiger Batch-Prozess:** In jeder Charge werden ähnliche, aber nicht identische Produkte hergestellt, d. h. die gleichen Arbeitsschritte werden mit unterschiedlichen Mengen an Rohstoffen und/oder unter unterschiedlichen Verarbeitungsbedingungen durchgeführt.
* **Multi-Produkt-Batch-Prozess:** In jeder Charge werden unterschiedliche Produkte hergestellt, so dass unterschiedliche Arbeitsschritte oder Methoden mit unterschiedlichen Mengen an Rohstoffen und unter unterschiedlichen Verarbeitungsbedingungen durchgeführt werden.

**Kategorisiert nach Anlagenstruktur**

Diese Batch-Prozesse sind mit dieser Kategorie verbunden (Barker & Rawtani, 2004):

* **Einweg-Batch-Prozess:** Bei dieser Prozessart wird die Charge nacheinander über eine vorher festgelegte Route von einer Produktionseinheit zur nächsten befördert.
* **Mehrweg-Batch-Prozess:** Der Aufbau dieser Prozessart ermöglicht es, dass mehrere Chargen gleichzeitig aktiv sind und die Produktionseinheiten unterschiedliche physikalische Eigenschaften haben können.
* **Netzwerk-Batch-Prozess:** Bei dieser Prozessart wird die Reihenfolge der Produktionseinheiten vor oder während der Chargenproduktion festgelegt oder zugewiesen. Beim Netzwerkprozess wird die geeignete Route zum Zeitpunkt der Herstellung auf der Grundlage von Beschränkungen, wie z. B. Anlagenkapazitäten und Rezeptanforderungen, festgelegt.

Klassifizierung von Batch-Prozessen nach Anlagenstruktur



Quelle: Rojas (2022)

### Notwendige Automatisierungsfunktionen für Batch-Prozesse

Batch-Prozesse erfordern einen umfangreichen Satz an Automatisierungsfunktionen, insbesondere die komplexeren, wie flexible Batch-Prozesse, Multi-Produkt-Batch-Prozesse und Netzwerk-Batch-Prozesse (Smith, 2014). Zu den zahlreichen Funktionen gehören

* Rezeptverwaltung,
* Sequenzlogik,
* Zustandsplaner,
* Zeitplanung,
* diskrete Gerätetreiber,
* grundlegende Regelungssteuerung (einfache PID-Schleifen und/oder erweiterte Steuerung),
* Produktionssteuerung und
* Sicherheits- und Prozessverriegelungen.

Für diese Funktionen in einer Batch-Anlage ist jedoch eine grundlegende Regelungssteuerung unerlässlich. Aufgaben wie Temperatur- oder Druckregelung werden normalerweise mit Hilfe von PID-Reglern (Proportional-Integral-Differential-Reglern) in einfachen Regelkreisen durchgeführt. Da die Produktionsprozesse immer komplexer werden, werden bei diesen Arten von Variablen in der Regel einfache Regelkreise genutzt und in verbesserte, fortschrittliche Steuerungssysteme integriert (Smith, 2014):

**Kaskadenregelung**

Zwei Regler bilden eine „Kaskade“, wenn der Bezugspunkt eines untergeordneten Reglers, Folgeregler genannt, durch den Ausgang eines übergeordneten Reglers, Führungsregler genannt, bestimmt wird (Shinskey, 1996). Nur der Sollwerteingang des Führungsreglers kann unabhängig eingestellt werden: Der Ausgang des Folgereglers geht immer in den Prozess, während jeder Regler sein entsprechendes Rückführsignal erhält. Diese Regelungsart wird üblicherweise zur Temperaturregelung von Behältern mit Umwälzsystemen im Bereich der Wärmeübertragung eingesetzt. Neben anderen sind Kaskaden von Temperatur zu Durchfluss und Druck zu Durchfluss üblich, da Durchflussmessungen in den meisten Prozessen weit verbreitet sind (Smith, 2014).

**Override-Regelung**

Um die Batch-Zykluszeit zu verkürzen und gleichzeitig die Produktionsleistung zu erhöhen, werden Batch-Prozesse in der Regel bis an ihre Grenzen ausgereizt. Dies bedeutet, dass der Prozess mit der maximal zulässigen Temperatur für die Kühlwasserrückführung betrieben wird, wobei der Druck neben anderen kritischen Prozessvariablen nahe an den von den Behältern akzeptierten Höchstwerten liegt. Eine Möglichkeit, diese Betriebsart zu erreichen, ist die Verwendung der Override-Regelung (dt. auch Begrenzungsregelung) (Smith, 2014). Auch bei dieser Regelungsart sind zwei Regler im Einsatz: der Hauptregler, der die Regelgröße auf dem Sollwert hält, wenn eine voreingestellte Stellgröße außerhalb ihrer Grenzen arbeitet, und der Override-Regler. Nähert sich die Regelgröße zu irgendeinem Zeitpunkt den Grenzwerten, übernimmt der Override-Regler die Regelung und der Hauptregler wird außer Kraft gesetzt (Blevins & Nixon, 2011).

**Planmäßige Abstimmung**

Diese Abstimmung ist bei Batch-Prozessen üblich und besteht in der Anpassung der Reglerkoeffizienten (z. B. eines PID-Reglers), die entweder auf dem Auftreten eines bestimmten Ereignisses, wie z. B. dem Beginn der Beschickung eines Reaktors, oder auf der Zeit im Batch basiert (Smith, 2014).

**Modellbasierte Regelungen**

Regelungssysteme, die die Verwendung eines Prozessmodells erfordern, wie z. B. die modellprädiktive Regelung (Model Predictive Control, MPC), haben sich in industriellen Anwendungen als überaus erfolgreich erwiesen (Caccavale et al., 2011). So können z. B. bei stark endothermen oder exothermen Reaktionen einige Variablen durch Energiebilanzen geschätzt werden, die dann im Regelungsschema oder in der Prozessverriegelung verwendet werden. Der Einsatz von MPC für die Regelung von Batch-Prozessen ist jedoch nur in begrenztem Umfang möglich (Smith, 2014).

**Mehrgrößenregelung**

Die Zahl der Prozesse mit mehreren Eingängen und mehreren Ausgängen ist zwar gering, ihre wirtschaftlichen Auswirkungen sind jedoch erheblich. Daher ist es wichtig, diese Art von Prozessen korrekt zu steuern (Acedo Sánchez, 2003). Die Regelung von Mehrgrößenprozessen mit einfachen PID-Regelkreisen ist aufgrund von Totzeiten, Wechselwirkungen und Begrenzungen schwierig. Die Temperatur ist eine wesentliche Größe in den meisten Batch-Prozessen. Wenn die Temperatur mit einer anderen Regelgröße in Wechselwirkung steht, muss das Regelungsschema geeignet sein, den Auswirkungen dieser Wechselwirkung entgegenzuwirken (Smith, 2014).

### Fragen zur Selbstkontrolle

1. Bitte geben Sie an, ob die folgenden Aussagen richtig oder falsch sind.

* Ein charakteristisches Merkmal des Regelungsschemas der planmäßigen Abstimmung ist die Änderung des Reglers, wenn sich die Regelgröße einem Grenzwert nähert. *Falsch*
* Die Wechselwirkung ist einer der Gründe, warum Proportional-Integral-Differential (PID)-Regler in Mehrgrößenprozessen schwierig einzustellen sind. *Richtig*
* Bei der Kaskadenregelung werden die Parameter eines Reglers in Abhängigkeit vom Auftreten eines bestimmten Ereignisses angepasst. *Falsch*
* Die modellprädiktive Steuerung (MPC) ist eine Art der modellbasierten Regelung *Richtig*
* Bei der Override-Regelung kann nur der Sollwert des Primärreglers unabhängig eingestellt werden. *Falsch*

1. Bitte wählen Sie aus, welche Batch-Prozess-Kriterien zu mehrstufigen Batch-Prozessen gehören.

* Anlagenstrukturkriterien
* Kriterien der hergestellten Produktmenge
* *Kriterien für Formeln und Verfahren*

## 3.2 Anwendungen

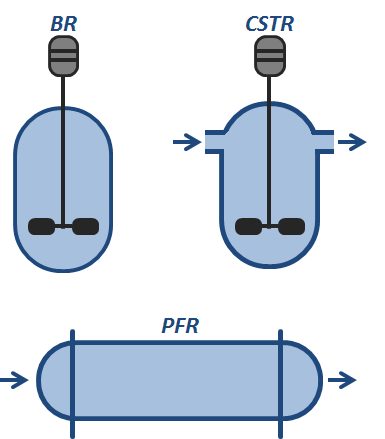
Wie bereits im vorigen Abschnitt erwähnt, werden Batch-Prozesse hauptsächlich in verschiedenen Bereichen der chemischen Prozessindustrie eingesetzt, insbesondere bei der Herstellung von Pharmazeutika, Lebensmitteln, Kosmetika, Polymeren und Farben, die als Spezialchemikalien gelten, oder bei der Herstellung von konfigurierten Konsumgütern (Dimian et al., 2014). Bei diesen Prozessen werden komplexe chemische Schritte wie Reinigung und Trennung in kleinen Produktionsmaßstäben durchgeführt, die in der Regel 10.000 Tonnen/Jahr nicht überschreiten. Alternativ wurde angemerkt, dass diese Batch-Prozesse Teil eines größeren kontinuierlichen Prozesses oder eines Semi-Batch-Prozesses sein könnten. In diesem Fall werden die Schritte entweder als Abfolge von Batch-Reaktionen mit anschließenden kontinuierlichen Trennungen oder umgekehrt organisiert (Bequette, 2003; Smith, 2014). Daher ist der Einsatz von Reaktoren und/oder Destillationskolonnen als Batch-Verfahren in diesem Bereich von großer Bedeutung.

### Der chemische Batch-Reaktor

Chemische Reaktionen können fast überall beobachtet werden, doch Reaktionen, bei denen Produkte entstehen, müssen unter kontrollierten Bedingungen ablaufen. Hier kommt ein Apparat ins Spiel, der als chemischer Reaktor bezeichnet wird (Caccavale et al., 2011). Chemische Reaktoren unterscheiden sich im Allgemeinen durch ihren Aufbau und ihre Abmessungen. Ihre Funktionsweise wird jedoch hauptsächlich durch die Qualität des Gemischs und die Betriebsweise beschrieben. Aus diesen Merkmalen wird ein mathematisches Modell abgeleitet. Ihre quantitative Beschreibung dient als Grundlage für Simulationen, die eine Vielzahl von Aufgaben ermöglichen (z. B. statische und dynamische Analysen oder die Entwicklung von Basisstrategien; Bequette, 2003; Smith, 2014).

Die Analyse chemischer Batch-Reaktoren beginnt üblicherweise mit der Betrachtung der drei Typen idealer chemischer Reaktoren mit einfachen abstrakten Darstellungen der tatsächlichen Apparate, welche die oben beschriebenen wesentlichen Merkmale zusammenfassen (Caccavale et al., 2011). Je nach Qualität des Gemischs werden diese Modelle als „ohne Vermischung“ oder „perfekte Vermischung“ und je nach Betriebsart als „kontinuierlich“ oder „diskontinuierlich“ klassifiziert. Von den drei idealen Reaktoren handelt es sich nur bei einem, dem idealen Strömungsrohrreaktor, um einen kontinuierlichen Reaktor ohne Vermischung. Für die beiden anderen Reaktoren wird eine perfekte Vermischung angenommen: Der kontinuierliche ideale Rührkessel (KIK) und der diskontinuierliche Batch-Reaktor (BR). Die drei idealen Reaktoren sind in der folgenden Abbildung schematisch dargestellt.

Ideale Reaktoren – Schematisch

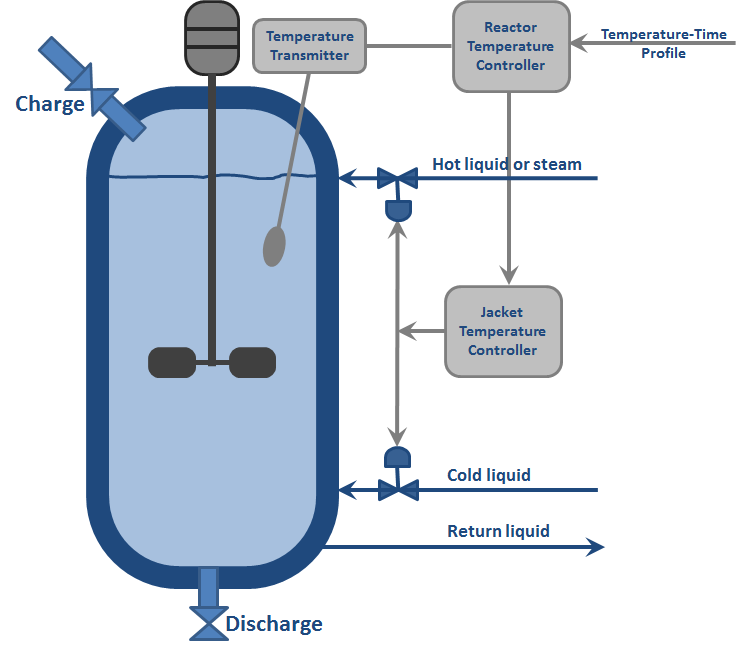


Quelle: Rojas (2022), basierend auf Caccavale et al. (2011)

### Der ideale Batch-Reaktor

Batch-Reaktoren gehören zur Grundausstattung in der chemischen Prozessindustrie. Sie bestehen aus einem Behälter mit Wärmeübertragungs- und Mischvorrichtungen sowie Rohrleitungen für die Zufuhr der Reaktanten (auch: Edukte) und die Entnahme der Produkte (Dimian et al., 2014). Im Gegensatz zu kontinuierlichen Reaktoren, in denen der Prozess unter stationären Bedingungen abläuft, ist der Betrieb eines Batch-Reaktors inhärent dynamisch, so dass sich die Eigenschaften der Reaktanten im Laufe der Zeit ständig ändern. Es ist jedoch zu beachten, dass der Batch-Reaktor nicht räumlich variiert, da die Homogenisierung mischbedingt erfolgt (Luyben, 1999; Bequette, 2003). Dadurch ergeben sich für einige Anwendungen kinetische Vorteile gegenüber kontinuierlichen Reaktoren, insbesondere wenn Reaktionen mit langsamen Geschwindigkeitskonstanten gefordert sind. Bei Batch-Reaktoren gibt es keine Strömung in den oder aus dem Behälter. Zu Beginn wird der Reaktor mit einem konstanten Flüssigkeitsvolumen V, einem Reagenz A und einer Anfangskonzentration CAO (Anzahl Mol pro Liter) beschickt. Um das gewünschte Temperatur-Zeit-Profil im Reaktor zu erreichen, sind in der Regel Aufheiz- und Abkühlvorgänge erforderlich. Um die Reaktionstemperatur in der Reaktionsmasse zu erreichen, muss dem Mantel Wärme zugeführt werden. Um die exotherme Reaktionswärme abzuführen, wird Kühlmittel zugeführt. Der Reaktionstemperaturregler verwendet die gewünschte Temperatur-Zeit-Kurve als zeitlich veränderliches Referenzsignal (Luyben, 1999; Bequette, 2003). Die folgende Abbildung skizziert die Temperaturregelung eines Batch-Reaktors.

Batch-Reaktor – Temperaturregelung



Quelle: Rojas (2022)

Mit der Zeit laufen im Reaktor nacheinander Reaktionen erster Ordnung ab. Die gewünschte Komponente, B erhält man durch die Reaktion der Komponente A. Komponente B kann weiter reagieren, um eine unerwünschte Komponente C zu erzeugen. Alle diese Reaktionen sind irreversibel, A kann man also nicht durch die Reaktion der Komponente B erhalten, obwohl B durch die Reaktion der Komponente A gewonnen wird (Bequette, 2003).

A−→− k1 B−→− k2 C*A→ k1 B→ k2 C*

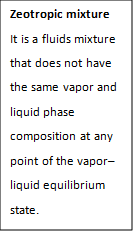
Hier ist k1 die spezifische Reaktionsgeschwindigkeit für die Umwandlung von A in B*;* k2 ist die spezifische Reaktionsgeschwindigkeit für die Umwandlung von B in C. Da das gewünschte Produkt die Komponente B ist, ist es wichtig zu wissen, wie lange die Reaktion dauern wird, um die maximale Menge an B zu erhalten, ohne dass eine Umwandlung in C erfolgt (Luyben, 1999; Bequette, 2003).

Da die spezifischen Reaktionsgeschwindigkeiten temperaturabhängig sind, muss sorgfältig darauf geachtet werden, das optimale Temperaturprofil zu wählen. Wenn k1 stärker von der Temperatur abhängig ist als k2 oder die Temperaturabhängigkeit von sowohl k1 und k2 gleich sind, muss die höchstmögliche Temperatur beibehalten werden, um die Reaktion der Komponente A zur Bildung der Komponente B zu erreichen. In beiden Fällen ist es wichtig, die Reaktion zum richtigen Zeitpunkt zu stoppen, um die maximale Menge an B zu erhalten. Wenn k1 weniger temperaturabhängig ist als k2, sollte das optimale Temperaturprofil mit einer hohen Temperatur beginnen, die die erste Reaktion auslöst, dann aber sinken, um den Verlust großer Mengen der Komponente B zu vermeiden. (Luyben, 1999).

Die Sicherheit ist aufgrund der hohen Temperaturen ein zentrales Thema bei der Entwicklung und dem Betrieb von Batch-Reaktoren. Besonders wichtig ist dies bei Feinchemikalien, bei denen die Behandlung exothermer Effekte und die Reaktionskinetik oft vernachlässigt werden können. Ein hilfreiches Instrument ist dabei die Simulation von Szenarien, mit deren Hilfe mögliche negative Ereignisse bereits in der Konzeptionsphase erkannt werden können (Blevins & Nixon, 2011).

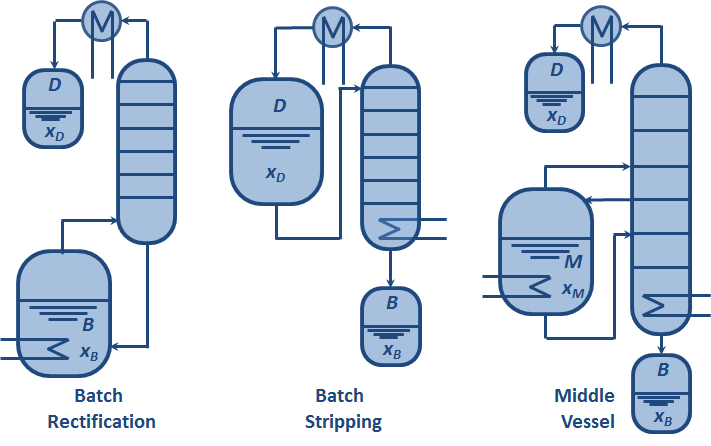
### Batch-Destillation

Gemäß Dimian et. al. (2014) wird die Batch-Destillation mit diesen drei Grundkonfigurationen durchgeführt:

1. Destillation mit Batch-Rektifikation
2. Destillation mit Batch-Stripping
3. Destillation mit Rektifikation und Stripping

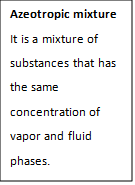
Die Destillation mit Batch-Rektifikation ist die in der Industrie am häufigsten verwendete Konfiguration. Sie verwendet eine Rektifikationskolonne, die mit dem Bodenbehälter verbunden ist. Die Destillation beginnt nach dem Einfüllen der Mischung in den Destillierkolben. Bei einem **zeotropen** **Gemisch** erfolgt die Trennung der Komponenten am Kolonnenkopf in aufsteigender Reihenfolge der Siedepunkte. Verschiedene Auffangbehälter sammeln Produktfraktionen mit guter Reinheit, während nicht spezifikationsgerechte Fraktionen in die nachfolgenden Chargen zurückgeführt werden (Dimian et al., 2014). Die Abbildung unten zeigt die drei grundlegenden Batch-Destillationsaufbauten.

Konfigurationen für die Batch-Destillation



Quelle: Rojas (2022), basierend auf Dimian et al. (2014).

Bei der Batch-Stripping-Destillation wird eine umgekehrte Konfiguration verwendet, bei der das Gemisch in den Kondensator am oberen Ende der Destillationskolonne gegeben wird. Die Trennung der Komponenten beginnt mit der schwersten Komponente und wird in umgekehrter Reihenfolge der Flüchtigkeiten am unteren Ende der Kolonne fortgesetzt. Nach Sørensen und Skogestad (1996) ist diese Anordnung am besten geeignet, wenn viele schwere Komponenten entfernt werden müssen, da sie die Dauer des Vorgangs minimiert.

Bei der Destillation mit Rektifikation und Stripping wird ein Mittelbehälter verwendet, und das Verfahren funktioniert ähnlich wie das Gegenstromprinzip bei der kontinuierlichen Destillation. Nach Meski und Morari (1995) können mit dieser Konfiguration die Einschränkungen der konventionellen Batch-Rektifikation überwunden werden, da eine höhere Leistung bei geringerem Energieverbrauch erzielt wird. Für weitere Anwendungen im Zusammenhang mit Mehrbehälter-Batch-Kolonnen und der Trennung von zeotropen und **azeotropen Gemischen** siehe Skogestad et al. (1997) und Warter et al. (2004).

### Beginn der Batch-Destillation

Für den Start der Batch-Destillation sind folgende drei Schritte erforderlich (Diwekar, 2012):

1. Die anfangs statische Charge wird bis zum Siedepunkt vorgeheizt.
2. Die Kolonne wird unter Berücksichtigung der Verstopfung des Kondensators befüllt.
3. Die Kolonne wird ohne Destillatentnahme in Betrieb genommen, bis ein stabiler Zustand erreicht ist.

Die Beschickung wird über die gesamte Kolonne verteilt, in der die im dritten Schritt beschriebene vollständige Rückflussbedingung hergestellt wird. Dies wird als „Kapazitätseffekt“ bezeichnet, an den die Anlaufzeit Teq gebunden ist. Die Anlaufzeit ist definiert als die Zeit, die die Kolonne von der Beschickung bis zum Erreichen des Gleichgewichtszustandes benötigt. Die erste Inbetriebnahme erfolgt in der Regel unter vollem Rückfluss.

Der zweite Schritt kann auf zwei verschiedene Arten erfolgen (Diwekar, 2012):

1. Der Zulauf erfolgt von oben, so dass die Zusammensetzung in jeder Platte und im Kessel die gleiche ist wie die Zusammensetzung des Zulaufs.
2. Die Kolonne wird ohne Rückfluss in Betrieb genommen und der Destillierapparat wird mit dem Zulauf beschickt. Auf diese Weise wird sichergestellt, dass die Zusammensetzung in jeder Kammer mit der des Stroms übereinstimmt, dessen Wert der Zusammensetzung des Zulaufs entspricht. Diese Methode wurde von Luyben (1971) vorgeschlagen. Sie wird in der Praxis jedoch nicht allgemein angewandt.

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie drei Bereiche, in denen Batch-Prozesse angewendet werden.

*Herstellung von Arzneimitteln*

*Herstellung von Lebensmitteln*

*Herstellung von Kosmetika*

*Herstellung von Polymerprodukten*

*Herstellung von Farbprodukten*

1. Bitte vervollständigen Sie den folgenden Satz.

Der einfache Batch-Reaktor besteht aus *einem Behälter*, der mit *Wärmeübertragungs-* und *Misch*vorrichtungen ausgestattet ist.

Zusammenfassung

Batch-Prozesse sind wichtig, weil sie notwendig sind, um neue Produktionsanlagen zu testen und/oder um Spezial- und Feinchemikalien herzustellen, bei denen Qualität und Anforderungen immer wichtiger werden. Daher ist es für das Verständnis dieses Bereichs unerlässlich, die grundlegenden Konzepte und Anwendungen von Batch-Prozessen zu kennen und zu wissen, wie sie funktionieren und wie sie automatisiert werden können. Der Abschnitt über die Grundlagen beschreibt die Prinzipien, aus denen Batch-Prozesse bestehen, ihre drei Hauptklassifizierungskriterien und die verschiedenen Klassifizierungen basierend auf diesen Kriterien. Anschließend werden die für Batch-Prozesse erforderlichen Automatisierungsfunktionen vorgestellt. Hervorgehoben wird sowohl die Bedeutung der grundlegenden Regelungstechnik als auch die Notwendigkeit der Kenntnis fortgeschrittener Regelungssysteme, wenn der Produktionsprozess komplexer wird. Sodann werden im Abschnitt Anwendungen verschiedene Bereiche der chemischen Prozessindustrie vorgestellt, in denen Batch-Prozesse und insbesondere deren komplexe Reinigungs- und Trennprozesse eingesetzt werden. Schließlich werden chemische Reaktoren und Destillationskolonnen als grundlegende Komponenten dieser Anwendungen vorgestellt. Sie sind entweder allein oder als Teil eines komplexen oder Semi-Batch-Prozesses ein wesentlicher Bestandteil dieser Anwendungen.

Lektion 4 – SCADA-Systeme

**Lernziele**

Nach der Bearbeitung dieser Lektion können Sie …

… die vier Funktionen nachvollziehen, die von SCADA-Systemen ausgeführt werden.

… die verschiedenen Komponenten von SCADA-Systemen erkennen.

… zwischen den von SCADA-Systemen verwendeten Kommunikationstechnologien unterscheiden.

… die drei von SCADA-Systemen verwendeten Schnittstellen identifizieren.

4. SCADA-Systeme

## Einführung

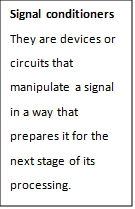
Mit dem Wachstum der Chemie-, Petrochemie-, Öl-, Gas-, Stahl- und Elektroindustrie wurde es immer schwieriger, die Kontrolle und den Überblick über die Anlagen und Maschinen zu behalten. Daher wurde ein System benötigt, mit dem der Zustand der Anlagen vor Ort und aus der Ferne kontrolliert und überwacht werden konnte. Dies führte zur Entwicklung von Steuerungs- und Datenerfassungssystemen mit der Bezeichnung Supervisory Control and Data Acquisition (SCADA; Zhang, 2010; Dey & Sen, 2020). Diese Lektion bietet einen Überblick über diese SCADA-Systeme, ihre Komponenten, Kommunikationstechnologien und verwendeten Schnittstellen.

## 4.1 Überblick

In den meisten Industriezweigen gibt es einzelne Systeme und Geräte, die autonom arbeiten, während ihre Parameter in der Regel gemessen und an eine zentrale Einrichtung übermittelt werden (Gardner, 2020). Die Geräte werden vor Ort von Controllern gesteuert, die überall in der Anlage vorhanden sind. Bei Bedarf können die wichtigsten Messwerte dieser Geräte von den Bediener:innen an einem zentralen Leitstand überwacht werden. Ausgestattet mit all diesen Informationen, können die Bediener:innen Entscheidungen hinsichtlich der Anlagenleistung treffen. Mit anderen Worten: Zentrale Computersysteme kommunizieren elektronisch mit den einzelnen Anlagen, Geräten und Systemen, um die Anlage zu überwachen. Sie sind auch in der Lage, die Betriebsparameter der Anlagen aus der Ferne einzustellen. Darüber hinaus verwalten diese Systeme die gesammelten Daten und erstellen historische Dateien als Grundlage für die Problemlösung und die Bewertung der langfristigen Effizienz. Dies ist die Aufgabe eines SCADA-Systems (Gardner, 2020). Bei den heutigen SCADA-Systemen werden vorzugsweise Fernkommunikationssysteme oder offene Steuerungssysteme verwendet. Dies schließt jedoch nicht aus, dass bei Bedarf auch Kurzstreckenkommunikation eingesetzt wird und/oder bestimmte geschlossene Steuerungsmechanismen verwendet werden (Zhang, 2010). Zusammenfassend kann man sagen, dass das SCADA-System eine Kombination aus Hardware und Software ist, die große Datenmengen erzeugt, die an eine zentrale Stelle transportiert werden müssen. Dort werden die Daten für die Sammlung, die Analyse, die Darstellung, die Entscheidungsfindung und die anschließende Kontrolle verwendet, die sich in vier verschiedene Funktionen zusammenfassen lassen, die im Folgenden aufgeführt sind (Zhang, 2010; Dey & Sen, 2020):

### Datenerfassung

Sensoren, Messgeräte, Transmitter, Steuerungen, Aktoren, Schalter und Ventile sind nur einige der vielen Geräte oder Feldgeräte, aus denen sich Produktions- und Fertigungssysteme zusammensetzen, die in der Regel von SCADA-Systemen überwacht werden (Zhang, 2010). Es gibt Sensoren, die den Input des Systems messen, z. B. die Flüssigkeit, die in einen Reaktor fließt, und andere, die den Output messen, z. B. die Temperatur, auf der das Endprodukt des Reaktors gehalten wird. Wenn das zu messende Ereignis einfach ist und durch Ein/Aus-Signale erkannt werden kann, wie z. B. das Öffnen oder Schließen eines Ventils oder Relais, können sie auch digital oder diskret sein. Ähnlich werden Analogsensoren zur Messung komplexer Zustände eingesetzt, bei denen eine kontinuierliche und genaue Erfassung von Spannungs- oder Stromsignalen wichtig ist (z. B. Temperatur eines Produktgemischs oder die Konzentration am Ende eines Prozesses).

Die Datenerfassung in SCADA-Systemen sollte in der Regel in Echtzeit erfolgen, d. h. die Daten müssen so erfasst werden, dass ein Computer sie ohne Verzögerung sammeln oder verarbeiten kann. Außerdem benötigen sie in der Regel Eingangsschalter oder Scanner, **Signalaufbereiter** und Analog-Digital-Wandler, damit die Datensignale korrekt übertragen und direkt vom Computer interpretiert werden können. Diese Funktion kann auch Teil eines Prozesssteuerungssystems, eines Datenaufzeichnungssystems oder sogar eines Prozessüberwachungs- und/oder Alarmsystems sein. Die gewonnenen Informationen können zum Beispiel dazu verwendet werden, einen industriellen Prozess mit Hilfe einer geeigneten Software direkt digital zu steuern (Zhang, 2010).

### Datenkommunikation

SCADA-Systeme werden zur Überwachung verschiedener Systeme von einer zentralen Station aus eingesetzt. Für den Transport aller auf der Feldebene erfassten Daten ist daher mindestens ein Kommunikationsnetz erforderlich. Die Kommunikation zwischen dem zentralen Standort und den entfernten Standorten kann kabelgebunden oder drahtlos über lokale Netzwerke (LAN) oder das Internet erfolgen (Dey & Sen, 2020). Frühe SCADA-Netzwerke hatten aufgrund der häufigen Verwendung von Modems oder Erdkabeln in der Regel eine geringe Bandbreite für die kabelgebundene Übertragung. Die drahtlose Übertragung könnte wiederum VHF/UHF-, Mikrowellen- oder Spreizspektrumfunkverbindungen umfassen. Für Anwendungen, die eine geringe Datenrate erzeugen und eine hohe Übertragungsgeschwindigkeit erfordern, wurden DSL (Digital Subscriber Lines) und ISDN (Integrated Services Digital Network) eingesetzt. Heute übertragen die meisten Systeme SCADA-Daten über SONET per Ethernet und IP.

Um den Zugriff auf SCADA-Daten über das offene Internet zu verhindern, werden diese Daten in der Regel verschlüsselt. Anschließend werden sie in einem proprietären Protokollformat über LAN oder WAN übertragen. Heutzutage werden sie jedoch in einem offenen Standardprotokollformat gesendet. Die Ausgabe der Sensoren wird von den Feldkomponenten zur Übertragung an die zentrale SCADA-Komponente kodiert. Im Gegenzug werden in Protokollformaten kodierte Steuerbefehle von der Zentrale an die Feldkomponenten gesendet, die diese dekodieren und die Steueraktion an die entsprechenden Feldgeräte, z.B. Sensoren und/oder Aktoren, weiterleiten (Dey & Sen, 2020).

### Datendarstellung

SCADA-Systeme erfordern, dass dem Bediener an zentraler Stelle ein Überblick über die gesamte Anlage gegeben wird, damit er deren Zustand überwachen kann. Auf Wunsch des Anwenders muss das System in der Lage sein, Details wie z.B. kommentierte Fließbilder anzuzeigen und herkömmliche Anlagenausrüstungen wie z.B. digitale Zähler, Füllstandsanzeigen und/oder analoge Druckmesser zu emulieren (Zhang, 2010; Gardner, 2020). Die Feldgeräte werden kontinuierlich überwacht. Das SCADA-System muss den Bediener alarmieren, wenn eine Alarmsituation auftritt. Dies ist der Fall, wenn eine Prozessvariable außerhalb ihres normalen Betriebsbereichs arbeitet. Die Alarmtafeln müssen die aktuellen Messwerte der kritischen Variablen, ihren Arbeitspunkt sowie die oberen und unteren Toleranzgrenzen anzeigen. Zur besseren Visualisierung für den Bediener könnte der Alarmstatus auch farblich gekennzeichnet werden (Gardner, 2020). Abgesehen von der Bereitstellung direkter Informationen muss es dem menschlichen Bediener auch ermöglichen, auf eine Datenbank zuzugreifen, die Trends, Balkendiagramme, Logistikinformationen, Diagnosedaten, geplante Instandhaltungsarbeiten und Managementinformationen bereitstellt (Zhang, 2010).

### Systemsteuerung

Komplexe, moderne SCADA-Systeme müssen nicht nur in der Lage sein, den Produktions- oder Fertigungsprozess zu überwachen, sondern auch alle notwendigen Variablen automatisch zu regeln. Wenn der Druck in einer Gasleitung zu hoch wird oder die Temperatur in einem Ofen über das normale Maß ansteigt, muss das System automatisch Regelungsmaßnahmen ergreifen, wie z. B. das Öffnen eines Ablassventils in der Gasleitung oder die Verringerung der Wärmezufuhr im Ofen (Zhang, 2010; Dey & Sen, 2020). Die Regelungsmaßnahmen des SCADA-Systems können in der Zentrale eingerichtet werden, insbesondere wenn komplexe Steuerungsalgorithmen erforderlich sind. Wenn jedoch die Zuverlässigkeit der Kommunikationsverbindungen begrenzt ist oder wirtschaftliche Gründe dies rechtfertigen, wird ein automatisches Regelungssystem an einem entfernten Standort eingerichtet (Zhang, 2010). Darüber hinaus müssen SCADA-Systeme in der Lage sein, adäquat auf Variationen in mehreren Inputs in einen Prozess zu reagieren, unabhängig davon, ob diese als Störung des Steuerungssystems betrachtet oder als Teil eines multivariaten Steuerungsschemas verwendet werden. Bei Ausfall eines automatischen Steuerungssystems muss das SCADA-System in der Lage sein, die Prozesssteuerung aufrechtzuerhalten, indem der Bediener diese Aufgabe von einer zentralen Stelle aus manuell übernimmt (Dey & Sen, 2020).

### Fragen zur Selbstkontrolle

1. Bitte geben Sie an, ob die folgenden Aussagen richtig oder falsch sind.

* Eine Anforderung an die Datenkommunikationsfunktion des SCADA-Systems ist es, dem Bediener an zentraler Stelle einen Überblick über die gesamte Anlage zu geben. *Falsch*
* Alle erforderlichen Variablen zu kontrollieren oder regulieren ist ebenfalls eine Funktion des SCADA-Systems. *Richtig*
* Signalkonditionierer, Eingangsschalter oder Scanner gehören zu den Geräten, die für die Datendarstellung des SCADA-Systems erforderlich sind. *Falsch*
* SCADA-Systeme nutzen DSL (Digital Subscriber Line) und ISDN (Integrated Services Digital Network) als Teil der Datenerfassungsfunktion. *Falsch*

1. Bitte vervollständigen Sie den folgenden Satz.

Sensoren können *digital oder diskret* sein, wenn das zu *messende* Ereignis einfach ist und nur durch Ein/Aus-Signale *erkannt* werden kann.

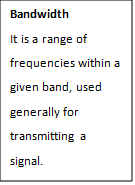
## 4.2 Komponenten

SCADA-Systeme bestehen in der Regel aus mehreren Subsystemen, deren Aufgabe es ist, Daten zwischen mehreren dezentralen Stationen und einer zentralen Station oder einem Host zu übertragen. Die Definition der Systemstruktur ist weit gefasst. Sie reicht von einfachen lokalen Überwachungs- und Steuerungssystemen bis hin zu großen verteilten Überwachungs- und Steuerungssystemen (Zhang, 2010). Unabhängig von der Größe des SCADA-Systems, mit dem wir uns befassen, besteht es aus vier Grundkomponenten: Zentralrechner oder Master-Station, Felddatenschnittstellengeräte, Kommunikationsinfrastruktur und Feldinstrumentierung.

### Zentralrechner oder Master-Station

Der Zentralrechner bzw. die Master-Station des SCADA-Systems, die sich normalerweise in einer zentralen Steuerungszentrale befindet, besteht aus großen Datenbanken, Benutzerschnittstellen und dem Masterterminal (Boyer, 2004). Große Datenbanken werden verwendet, um alle in der Anlage oder im Feld gesammelten Daten sowie die durch lokale Verarbeitung gewonnenen Daten zu speichern. Alle diese gespeicherten Daten enthalten Informationen über die Quelle und den Zeitpunkt, wann sie aufgetreten sind. Benutzerschnittstellen sind intuitive Eingabe- und Ausgabegeräte, die dazu dienen, dem Bediener Ergebnisse in einem lesbaren Format zu präsentieren und von ihm Eingabebefehle entgegenzunehmen und an das System zurückzusenden. Diese Schnittstellen sind für die Funktion der Datendarstellung zuständig. Es kann sich um Monitore mit Tasten oder Tastaturen und/oder Touchscreens handeln. Das Masterterminal (MTU) ist das Zentrum des Systems und für das Sammeln von Daten von entfernten Standorten sowie für das Senden von Befehlen oder Operationen verantwortlich. Dabei kann es sich um einen einzelnen Computer oder eine Gruppe von Servern handeln (Zhang, 2010). Teil der MTU können auch Überwachungsrechner, Engineering-Workstations und Bedienstationen sein (Gardner, 2020). Die Überwachungscomputer sammeln, archivieren und analysieren die von den Felddatenschnittstellengeräten empfangenen Daten. Sie enthalten eine übergeordnete SCADA-Software, die für die Darstellung der Informationen über die Benutzerschnittstellen verantwortlich ist. Diese Rechner können miteinander vernetzt sein, wobei einige auf die Überwachung beschränkt sind, während andere die aktive Steuerung des Produktions- oder Fertigungsprozesses ermöglichen. Die Engineering-Workstation steuert das gesamte Prozessleitsystem (PLS) und verfügt über spezielle Software für dessen Programmierung und Implementierung mit unbegrenzten Überwachungsmöglichkeiten. Die Bedienstationen beschränken sich, wie der Name schon sagt, auf die Überwachung, Bedienung und Steuerung der Anlagen und Parameter. Es besteht keine Möglichkeit, die Programme zu ändern. In komplexen und großen SCADA-Systemen werden verschiedene Sub-Master-Stationen (Sub-MTUs) eingesetzt. Diese sammeln Informationen von entfernten Standorten und senden die Daten an die Master-Station (MTU) des SCADA-Systems zurück (Dey & Sen, 2020).

### Felddatenschnittstellengeräte

Felddatenschnittstellengeräte sind Mikroprozessorsteuerungen, welche die Verbindung zwischen den Messgeräten auf der Feldebene und der Master-Station des SCADA-Systems ermöglichen, das für die Überwachung und Steuerung der Anlage verantwortlich ist (Gardner, 2020). Sie liefern Details über den Betrieb der installierten Instrumente und kommunizieren mit dem Zentralrechner in einem Format, das mit dem Protokoll oder der Software des SCADA-Systems kompatibel ist (Zhang, 2010). Im Allgemeinen gibt es zwei Arten von Geräten: Fernwirkeinheiten (engl. Remote Terminal Units, RTUs) oder speicherprogrammierbare Steuerungen (SPS).

RTUs sind autonome Spezialgeräte, die an verschiedenen Standorten Daten erfassen, Prozesse steuern und verwalten. Ursprünglich galten diese Geräte als dumm, da ihre einzige Funktion darin bestand, Feldgeräte miteinander zu verbinden, E/A zwischen Feldgeräten und SPS zu multiplexen und Informationen an den Zentralrechner zu übertragen (Gardner, 2020). Die Automatisierung dieser Geräte erfolgt über Befehle, die in der Regel lokal in den SPS-Systemen gespeichert werden. Eine zentrale Speicherung wird als nicht praktikabel angesehen, da die typische **Bandbreite** der Kommunikationsverbindung zur Master-Station begrenzt ist (Zhang, 2010). Heutige RTUs gelten als intelligente E/A-Geräte mit integrierten Logikfunktionen. Die Kommunikation zwischen RTUs erfolgt auf Peer-to-Peer-Basis. Wenn eine RTU nicht direkt mit der Master-Station kommunizieren kann, kann eine andere RTU als Repeater-Station fungieren und die wichtigsten Daten speichern und senden. Die RTUs sammeln die Daten von den Sensoren in Echtzeit und geben die Quelle und den Zeitpunkt des Ereignisses an. Sie senden die Informationen jedoch nur dann an die Zentrale, wenn sie von der MTU angefordert werden (Dey & Sen, 2020).

Ebenso sind SPS als Felddatenschnittstellengeräte wesentlich vielseitiger, konfigurierbarer und kostengünstiger als ihre spezialisierten Gegenstücke (Gardner, 2020). Obwohl SPS-Systeme über komplexere Steuerungsfunktionen als RTUs verfügen, können sie sich auch als Steuerungs-Blackbox verhalten, ähnlich wie RTUs, jedoch mit der Möglichkeit des Zugriffs über eine robuste Benutzerschnittstelle, wie sie für SPS typisch ist.

Während SPS-Systeme aus der industriellen Automatisierung stammen, haben SCADA-Systeme ihren Ursprung im Bereich der Telemetrie, wo RTUs keine Steuerprogramme benötigten. Die RTUs mussten daher nur grundlegende Informationen von einer entfernten Quelle empfangen. Ihre lokalen Steueraktionen beschränkten sich auf die Aktivierung der Relaisschaltlogik. Mit zunehmender Nutzung und Funktionsverschmelzung mussten SCADA-Systeme das SPS-Programm schließlich über ein Fernsignal beeinflussen, um ihre Überwachungsfunktion zu erfüllen. Dies wurde durch einfache lokale Steuerungsprogramme erreicht, die in der RTU gespeichert wurden. Diese Programme ermöglichen es der RTU, die SPS zu überwachen und sogar lokale Steuerungsaufgaben von diesem Gerät aus durchzuführen. Ebenso wurden Kommunikationsmodule in die SPS integriert, damit diese ihren Status und den ihres Steuerungsprogramms melden konnten. Aufgrund dieser Fortschritte ist es heute schwierig, zwischen SPS und RTU zu unterscheiden. Die in beiden Fällen verwendete Terminologie ist austauschbar (Zhang, 2010).

### Kommunikationsinfrastruktur

An dieser Stelle wird die Kommunikationsinfrastruktur benötigt, um die Verbindung zwischen dem Zentralrechner und den dezentralen Einheiten zu gewährleisten. In den meisten industriellen Anwendungen werden hierfür Netzwerke verwendet (Zhang, 2010). Die in der Zentrale definierten Überwachungs- und Steuerbefehle werden in der Regel als einfache Daten an die RTU/SPS gesendet. Diese stellt eine Kommunikationsverbindung zur RTU/SPS her, so dass die Feldgeräte die Befehle empfangen können. Die Verifizierungsmechanismen moderner SCADA-Systeme stellen sicher, dass das entsprechende Gerät den gesendeten Befehl empfängt. Dabei werden mehrere Ebenen der Bestätigung verwendet.

Nach Zhang (2010) werden in SCADA-Netzwerken in der Regel zwei Kommunikationsmodelle verwendet: das Master-Slave-Modell und das Peer-to-Peer-Modell.

**Master-Slave-Kommunikationsmodell**

Beim Master-Slave-Modell hat die Master-Station die vollständige Kontrolle über das Kommunikationssystem und verwendet zu diesem Zweck eine Punkt-zu-Punkt- oder Mehrpunkt-Netzwerkanordnung. Nach Dey & Sen (2020) kann die Kommunikation zwischen einer Master-Station und einer Slave-Station auf drei Arten erfolgen: über den nachrichtenbasierten Polling-Modus, über den Standard-Polling-Modus oder über den Ausnahme-Polling-Bericht.

Im nachrichtenbasierten Polling-Modus ist die Kommunikation mit den einzelnen Slave-Stationen weder zeitlich noch in Bezug auf die Häufigkeit entscheidend. In diesem Modus kann ein:e Benutzer:in festlegen, wann und wie oft die Kommunikation zwischen der Master-Station und jeder Slave-Station hergestellt werden muss. Um dieses Ziel zu erreichen, bietet diese Methode dem Benutzer volle Flexibilität mit Hilfe der Kontaktplanlogik. Die Kommunikation zwischen der Master-Station und einer bestimmten Slave-Station beginnt erst, wenn in der Kontaktplanlogik ein Nachrichtenbefehl (MSG) an die Adresse der entsprechenden Slave-Station aktiviert wurde. Daher sind die Kommunikationsereignisse mit jeder Slave-Station und deren Häufigkeit vollständig benutzerdefiniert. Dieser Modus wird nicht für SCADA-Systeme empfohlen, die eine ununterbrochene Kommunikation zwischen der Master-Station und den Slave-Stationen erfordern (Dey & Sen, 2020).

Der Standard-Polling-Modus wiederum wird verwendet, wenn das SCADA-System groß ist und es wichtig ist, dass die Master-Station mit allen Slave-Stationen kommuniziert. Dieser Modus wird auch verwendet, wenn das SCADA-System den Slave-Stationen erlaubt, Nachrichten zu initiieren. Darin konfiguriert ein:e Benutzer:in zunächst alle Slave-Stationen, und von dort aus fragt die Master-Station alle mit ihr verbundenen Slave-Stationen im Turnus ab. Zu diesem Zweck sendet die Master-Station ein oder mehrere 4-Byte-Polling-Pakete an die Adressen der einzelnen Slave-Stationen. Slave-Stationen werden von der Master-Station in der Reihenfolge abgefragt, in der sie in einer Abfrageliste erscheinen. Als Antwort auf die Abfrage sendet die Slave-Station ein Datenpaket oder ein Paket, das angibt, dass sie zu diesem Zeitpunkt keine Daten zu senden hat. Die Abfrage erfolgt kontinuierlich und asynchron. Sie ist unabhängig von den Nachrichtenauslösebefehlen (MSG) in der Kontaktplanlogik der Master-Station. Wenn z. B. die Master-Station eine Slave-Station abfragt und ein MSG-Befehl in der Kontaktplanlogik ausgelöst wird, muss die Master-Station die Abfrage der aktuellen Slave-Station abschließen und die Nachricht wird dann übertragen, bevor mit der nächsten Station in der Abfrageliste fortgefahren wird. Wenn mehrere MSG-Befehle gleichzeitig gesendet werden, können mindestens vier Nachrichtenpakete zwischen den Abfragen von zwei aufeinanderfolgenden Slave-Stationen in der Abfrageliste gesendet werden. Wenn die Adresse der entsprechenden Slave-Station in der Abfrageliste erscheint und von der Master-Station angesprochen wird, können die gesamten Nachrichten abgeschlossen werden. Sind MSG-Befehle an verschiedene Slave-Stationen adressiert, werden die Nachrichten nacheinander in der Reihenfolge abgearbeitet, in der die Slave-Stationen in der Abfrageliste erscheinen.

Wenn in diesem Modus eine einzelne Nachricht pro Abfrageumlauf eingestellt ist, wird für jede abgefragte Station eine einzelne Nachricht aus der entsprechenden Sendewarteschlange gesendet. Wenn jedoch mehrere Nachrichten pro Abfrageumlauf eingestellt sind, sendet jede abgefragte Station kontinuierlich alle Nachrichten in ihrer Sendewarteschlange, bis diese leer ist. Außerdem wird auf der Master-Station eine Liste der aktiven Knoten erstellt und bei jedem Umlauf aktualisiert, wenn die Slave-Stationen auf die Abfrage antworten oder nicht antworten. Darüber hinaus ist die Liste der aktiven Knoten eine Information für die mit der Master-Station verbundene Benutzerschnittstelle, ob der Kommunikationsstatus für alle Slave-Stationen gut (oder schlecht) ist. Für SCADA-Systeme, bei denen der Anwender in der Lage sein muss, zu begrenzen, wann und wie oft die Master-Station mit jeder Slave-Station kommunizieren muss, wird dieser Modus nicht empfohlen (Dey & Sen, 2020).

Schließlich initiiert im Kommunikationsmodus mit Ausnahme-Polling-Bericht die Slave-Station die Datenübertragung zum Master. In diesem Fall wertet jede Slave-Station alle Änderungen ihrer Eingangsdaten aus, indem sie ihre Eingänge kontinuierlich überwacht. Wenn eine Slave-Station eine Änderung in den Daten feststellt, leitet sie eine Datenübertragung an die Master-Station ein und informiert diese über die Änderung der von dem betreffenden Slave erfassten Daten. Der Vorteil dieser Technik besteht darin, dass keine häufige Abfrage aller Slaves erforderlich ist, wodurch der Master von dieser Aufgabe entlastet wird und sich auf andere wichtige Funktionen konzentrieren kann, die seine Aufmerksamkeit erfordern (Dey & Sen, 2020).

**Peer-to-Peer-Kommunikationsmodell**

Beim Peer-to-Peer-Kommunikationsmodell gibt es keinen Master, der die Kommunikation kontrolliert, was zu einem Wettbewerb um den Zugang zum Übertragungsmedium zwischen den einzelnen Stationen führt (Zhang, 2010). In diesem Fall wird für die Kommunikationssteuerung häufig das Konkurrenzverfahren Carrier Sense Multiple Access mit Collision Detection (CSMA/CD) verwendet. Diese Art der Steuerung ist notwendig, da Kollisionen unvermeidbar sind und die Stationen damit umgehen müssen. Wenn z. B. eine RTU eine Kommunikation mit einem Peer auf der gleichen Ebene aufbauen muss, antwortet sie immer mit der Zieladresse ihres Peers und nicht mit der Zieladresse des Zentralrechners, wenn sie vom Zentralrechner in einem Poll abgefragt wird. Dieses Verfahren wird in Gruppen von Stationen mit gleichem Status und sogar in Master-Slave-Netzwerken verwendet. In der Regel wird das Kommunikationsmedium vor der Datenübertragung abgehört, um Kollisionen zu vermeiden. SCADA-Systeme verwenden Wiederherstellungsverfahren, um Kollisionsprobleme zu lösen. Bei niedrigen Übertragungsraten ist dieser Ansatz im Allgemeinen erfolgreich. Wenn der Datenverkehr jedoch 30 % der Kanalkapazität überschreitet, wird die Kommunikation unregelmäßig und unzuverlässig und das System bricht zusammen. Zur Aufrechterhaltung der Kontrolle über die Kommunikation wird diese Technik nur in Netzwerken eingesetzt, in denen für alle RTUs und/oder SPS-Systeme mit Zugangsbedarf dieselben Medien auf einer gemeinsamen Kabelverbindung oder innerhalb derselben Funkreichweite garantiert werden können. Wie beim Kommunikationsmodus „Abfrage durch Ausnahme“ werden auch beim CSMA/CD-Verfahren unnötige Datenübertragungen durch Ausnahmeberichte reduziert (Zhang, 2010).

### Feldinstrumentierung

Schließlich werden die RTUs und/oder SPS-Systeme mit der Feldinstrumentierung verbunden, einer der wesentlichen Bestandteile von SCADA-Systemen im Allgemeinen (Dey & Sen, 2020). Die Instrumentierung ihrerseits besteht im Wesentlichen aus Sensoren und Aktoren, die an den überwachten und gesteuerten Arbeitsplätzen und Prozessen angebracht sind, um Informationen zu sammeln und die lokale Leistung in den verschiedenen Phasen des Produktions- oder Fertigungsprozesses zu steuern. Diese Instrumente wandeln in der Regel physikalische Größen in elektrische Signale auf Feldebene um. Sie werden insbesondere gebildet durch verschiedene Arten von Sensoren, z. B. Temperatur-, Durchfluss-, Druck- und Energieverbrauchssensoren, Positionsgeber, Messumformer und Stellglieder wie Schalter, Relais, Ventile usw., sowie durch lokale Steuerungen und spezifische Instrumente, z. B. Motorsteuergeräte (Zhang, 2010; Dey & Sen, 2020).

Die Felddaten werden von den RTUs und SPS-Systemen in ein für die Master-Station des SCADA-Systems akzeptables Format umgewandelt. Heute gibt es außerdem intelligente Feldgeräte oder Intelligent Electronic Devices (IEDs), die sowohl über Eingänge als auch über Ausgänge direkt mit der Master-Station des SCADA-Systems kommunizieren können. IEDs senden oder empfangen E/A-Signale als Teil ihres normalen Betriebs, aber zusätzlich zu ihren Steuersignalen können sie auch Leistungs- und Diagnoseinformationen liefern. Steuerventile empfangen z. B. 4 bis 20 mA-Signale, um das Ventil zu positionieren, aber wenn sie intelligent sind, können sie auch die Auslenkung der Ventilspindel, den Steuerluftdruck oder den Signalluftdruck übertragen, um ihren aktuellen Zustand zu beschreiben. Außerdem können Sie die Seriennummer des Modells und die Marke angeben und, falls erforderlich, sogar eine Anfrage zur Wartung oder zum Austausch des Geräts stellen. Diese Art von Informationen ist für die Unterstützung von Instandhaltungsplanungssystemen, für die Verbesserung der Zuverlässigkeit des automatisierten Systems als Ganzes und für die Lösung von Problemen, die während des Produktions- oder Fertigungsprozesses auftreten können, von Bedeutung. Darüber hinaus können einige intelligente Instrumente über integrierte Anzeigen verfügen, die vor Ort Folgendes anzeigen: Messwerte, Trend- und Balkendiagramme, Diagnosen und Fehlermeldungen (Gardner, 2020).

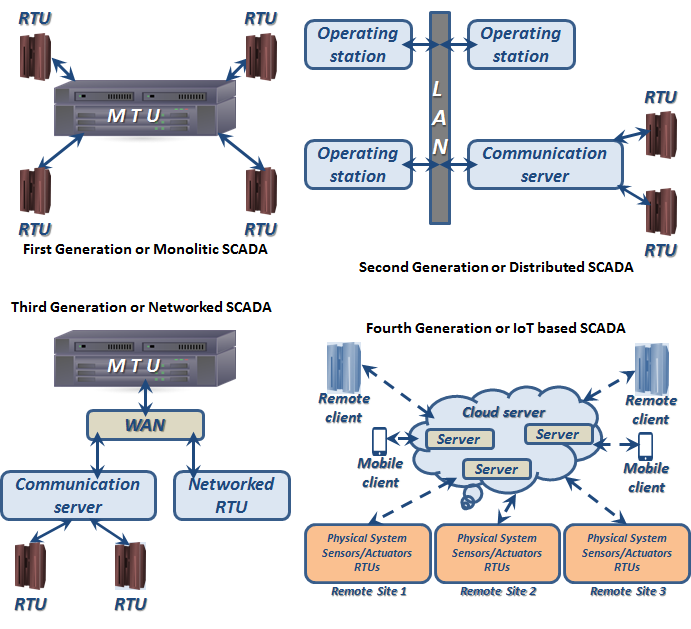
### SCADA-Architektur

SCADA-Systeme repräsentieren eine Technologie, die 50 Jahre alt ist. Doch obgleich die grundlegenden Komponenten, wie oben beschrieben, die gleichen sind, hat sich die Architektur dieser Systeme im gleichen Tempo wie die Mess-, Steuer- und Kommunikationstechnik verändert und weiterentwickelt (Dey & Sen, 2020). Ziel der technologischen Entwicklung war schon immer die Erfüllung der Anforderungen der Industrie an intelligentere, sicherere und zuverlässigere Systeme. Dies hatte zur Folge, dass die Architektur der SCADA-Systeme vier Generationen durchlaufen hat, wie im Folgenden beschrieben:

Die erste Generation, die aus monolithischen SCADA-Systemen bestand, wurde auf der Basis von Großrechnersystemen entwickelt und entfernte sich vollständig vom Netzwerkgedanken. Daher handelte es sich im Allgemeinen um kleine, wenig sichere und unabhängige Systeme, die nicht in der Lage waren, die verschiedenen Regelungssysteme, aus denen sie sich zusammensetzten, miteinander zu verbinden (Yadav & Paul, 2021). Diese Systeme verwendeten proprietäre Kommunikationsprotokolle, die in der Regel von RTU-Anbietern entwickelt wurden. Diese Protokolle ermöglichten der Master-Station den Zugriff auf die an die RTU angeschlossenen Sensoren und Aktoren zwecks Abfrage, Datenaustausch und Steuerung. Primitive WANs wurden auch nur für die Kommunikation der Master-Station mit den RTUs im Feld entwickelt. Der Datenschutz und die Sicherheit des Dauerbetriebs der Systeme der ersten Generation wurden durch Redundanz sichergestellt. Zu diesem Zweck wurden ein Haupt- und ein Backup-System verwendet, die identisch und auf Busebene miteinander verbunden waren. Der Hauptrechner wurde ständig vom Backup-Rechner überwacht, der bei einem Ausfall alle Aktivitäten des SCADA-Systems übernahm, während der Hauptrechner repariert wurde (Dey & Sen, 2020).

Die Verbesserungen in der LAN-Technologie und die Miniaturisierung der Systeme führten zur zweiten Generation der verteilten SCADA-Systeme. Sie verfügten über mehrere Stationen und mehrere Systeme, von denen jedes eine bestimmte Funktion erfüllte, einschließlich der Verteilung der Verarbeitung und des gegenseitigen Austauschs von Informationen in Echtzeit. Die Stationen dieser Generation waren in der Regel Minicomputer, die im Vergleich zu den Großrechnern der vorherigen Generation sehr preiswert waren. Einige dieser Stationen dienten als Kommunikationsbasis für die RTUs, andere wurden als Datenbankserver oder Rechenprozessoren und wieder andere als integrierte Benutzerschnittstellen eingesetzt. Bei den LANs dieser Generation wurden proprietäre Protokolle verwendet, die von den Anbietern der spezialisierten Stationen entwickelt worden waren. Diese LANs bieten eine höhere Systemzuverlässigkeit durch Kanäle mit höheren Übertragungsgeschwindigkeiten und Echtzeit-Traffic-Management. Alle an das LAN angeschlossenen Stationen oder Geräte waren aufgrund der Sicherheit, die die verteilte Architektur bietet, ständig online. Da diese LANs proprietär waren, hatten die Stationen, aus denen sie zusammengesetzt waren, keine Möglichkeit zur Kommunikation mit externen Geräten, obwohl die SCADA-Systeme grundsätzlich verteilt waren. Durch die Verteilung der Funktionen des SCADA-Systems auf die an das Netz angeschlossenen Stationen oder Geräte wurde nicht nur die Verarbeitungseffizienz erhöht, sondern auch die allgemeine Zuverlässigkeit und Redundanz des Systems verbessert (Dey & Sen, 2020; Yadav & Paul, 2021).

**SCADA-Architekturen**

  
Quelle: Rojas (2022), basierend auf Dey & Sen (2020).

Aufgrund des starken Anstiegs der Prozessautomatisierung durch Steuerungssysteme und der rasanten Industrialisierung wurde die dritte Generation, das so genannte Netzwerk-SCADA, entwickelt. Vernetzte SCADA-Systeme zeichnen sich durch ihre Komplexität aus, die mit dem vorherrschenden Bedürfnis nach einem offenen, herstellerunabhängigen System zusammenhängt. Dies bedeutet, dass jedes Gerät problemlos durch ein anderes ersetzt werden kann, unabhängig vom Hersteller. Diese Generation hat das bestehende proprietäre, herstellerabhängige SCADA-System in ein SCADA-System mit offener Systemarchitektur überführt, das standardisierte Kommunikationsprotokolle verwendet (Dey & Sen, 2020). Dank der Einführung offener Standards können auch Computer und Peripheriegeräte von Drittanbietern das Netzwerk nutzen. Außerdem hat die Verwendung des Internetprotokolls für die Kommunikation zwischen der Master-Station und den RTUs zu einer wesentlichen Verbesserung geführt, welche die Landschaft der vernetzten SCADA-Systeme verändert hat (Yadav & Paul, 2021).

Die vierte Generation von SCADA-Systemen, die auf dem Internet der Dinge (Internet of Things, IoT) basiert, nutzt IoT-Innovationen und den Zugang von SCADA-Systemen zum Cloud Computing, um die Kosten zu senken, was erhebliche wirtschaftliche Vorteile mit sich bringt (Yadav & Paul, 2021). Im Vergleich zu früheren Generationen haben diese Technologien die Kosten für die Infrastruktur von SCADA-Systemen erheblich gesenkt, die Wartung erleichtert und die Implementierung und Integration verbessert. Die Möglichkeit, Daten über das IoT zu manipulieren, zu visualisieren und auf sie zuzugreifen, erhöht die Robustheit von SCADA-Systemen. Die IoT-Technologie bietet mit Hilfe der verfügbaren offenen Netzwerkprotokolle wie Transport Layer Security (TLS) zudem ein sehr spezifisches, transparentes und verwaltbares Sicherheits-Framework. Diese Protokolle erleichtern die Erkennung und Behebung möglicher Schwachstellen, indem sie die Verwaltung der Sicherheitsgrenzen vereinfachen. Außerdem ermöglichen sie die Ausweitung oder Replikation dieser Grenzen auf den Rest des Netzwerks. Cloud Computing ermöglicht die Anbindung entfernter Server an ein Netzwerk und damit die Einrichtung eines zentralen Datenspeichers. Zusätzlich zu IoT und Cloud Computing verfügen SCADA-Systeme der vierten Generation über eine Vielzahl von Werkzeugen wie Datenmodellierung oder plattformunabhängige Kommunikationsdienste. Aktuelle SCADA-Software ermöglicht z. B. die Datenmodellierung auf der Grundlage objektorientierter Programmierung. Dadurch lassen sich Probleme wie die Eins-zu-eins-Zuordnung von Daten aus verschiedenen Arten von Datenbanken, Steuerungen und/oder Sensoren vermeiden (Dey & Sen, 2020).

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie die vier Grundkomponenten der SCADA-Systeme.

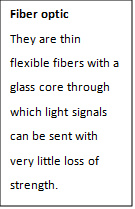
* *Der Zentralrechner oder die Master-Station*
* *Die Felddatenschnittstellengeräte*
* *Die Kommunikationsinfrastruktur*
* *Die Feldinstrumentierung*

1. Geben Sie die Anzahl der Generationen an, die die Architektur der SCADA-Systeme durchlaufen hat.

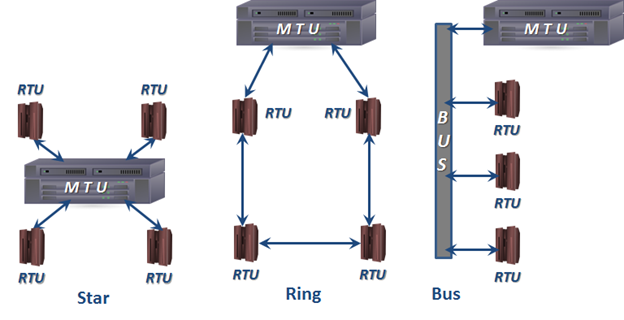
* Eine
* *Vier*
* Drei
* Zwei

## 4.3 Kommunikationstechnologien

Zwischen den beteiligten Einheiten oder Knoten muss eine Verbindung bestehen, damit eine Kommunikation stattfinden kann. Unabhängig von der Art des verwendeten Netzwerksystems sind die verschiedenen Knoten physisch oder logisch miteinander verbunden, und die geometrische Anordnung der Verbindungen, ob kabelgebunden, drahtlos oder beides, wird als Netzwerktopologie bezeichnet (McIver McHoes & Flynn, 2011). Zu den typischen geometrischen Anordnungen dieser Topologie gehören die Stern-, Ring-, Bus-, Baum- und Hybrid-Topologie. Die physikalische Topologie eines Netzwerks spiegelt jedoch nicht unbedingt seine logische Topologie wider. Beispielsweise kann ein Netzwerk per Software so konfiguriert werden, dass es logisch als Ring funktioniert, unabhängig davon, ob seine physikalische Verbindung eine Sterntopologie aufweist. Um Verwirrung zu vermeiden, wird immer dann, wenn von einer Topologie die Rede ist, davon ausgegangen, dass die logische Struktur und die physikalische Struktur des Netzwerks identisch sind. Die in SCADA-Systemen üblicherweise verwendeten Topologien für die Datenkommunikation zwischen MTU und RTU sind Stern, Ring und Bus (Dey & Sen, 2020).

Die Sterntopologie ermöglicht eine einfache Orientierung, da die MTU die Routen aller RTUs kennt, den Zugang zum Netzwerk einfach kontrollieren und bei Bedarf bestimmten ausgewählten RTUs Vorrang einräumen kann (McIver McHoes & Flynn, 2011). In dieser Topologie muss die MTU extrem zuverlässig und in der Lage sein, den gesamten Datenverkehr im Netzwerk zu verarbeiten, unabhängig von der Datenmenge, denn wenn sie ausfällt, fällt das gesamte Netzwerk aus. Außerdem können die RTUs in der Sterntopologie nicht miteinander kommunizieren, obwohl sie alle mit der MTU kommunizieren können (Dey & Sen, 2020). Bei der Ring- oder Daisy-Chain-Topologie sind alle Knoten in einer geschlossenen Schleife verbunden, beginnend mit der MTU. Alle RTUs können nacheinander gekreuzt werden, wobei nur die erste und die letzte RTU mit der MTU verbunden sind (McIver McHoes & Flynn, 2011). In dieser Topologie kann jede Station mit ihrem Nachbarn kommunizieren. Durch die Peer-to-Peer-Kommunikation und die Möglichkeit, Nachrichten zu empfangen, zu speichern und weiterzuleiten, kann jede von der MTU gesendete Nachricht über eine oder mehrere RTUs an eine andere RTU weitergeleitet werden, die keine direkte Verbindung zur MTU hat. Diese Methode wird häufig bei SCADA-Systemen mit großer geografischer Entfernung zwischen MTU und RTU verwendet (Dey & Sen, 2020). In der Bustopologie sind alle Knoten an eine einzige Kommunikationsleitung angeschlossen, die sich über die gesamte Länge des Netzwerks erstreckt und alle RTUs über Kabel miteinander verbindet, während sich die MTU als Controller in der Regel in einem Extrem befindet (McIver McHoes & Flynn, 2011). In dieser Topologie kann jede RTU Nachrichten von jeder anderen RTU senden/empfangen, da die Nachrichten über die gesamte Kommunikationsleitung in beide Richtungen zirkulieren können. Da sich alle RTUs und die MTU die Kommunikationsleitung teilen, kann es zu Kollisionen kommen, so dass immer nur eine dieser Stationen erfolgreich Nachrichten senden kann. Besonderes Interesse an dieser Kommunikationstopologie haben in letzter Zeit die Entwickler von SCADA-Systemen gezeigt, die **Glasfaserkabel** für die Datenübertragung verwenden (Dey & Sen, 2020). Die folgende Abbildung zeigt die drei Topologien, die normalerweise für die Kommunikation von SCADA-Systemen verwendet werden.

**SCADA-Kommunikationstopologien**

  
Quelle: Rojas (2022), basierend auf Dey & Sen (2020).

### SCADA-Kommunikationsprotokolle

Eine der Prioritäten für die korrekte Implementierung von SCADA-Systemen ist eine effektive Kommunikation zwischen den verschiedenen Geräten, aus denen sie bestehen. Diese Kommunikation kann auf der einen Seite zwischen MTU und RTU (oder SPS, IED) und/oder auf der anderen Seite zwischen einer RTU und Feldgeräten erfolgen (Dey & Sen, 2020). Damit die Kommunikation zwischen den Komponenten eines SCADA-Systems korrekt funktioniert, werden Protokolle benötigt, um Fehler zu vermeiden. Ein Kommunikationsprotokoll ist ein Satz von Regeln und Verfahren, die den RTUs und MTUs die Darstellung und den Austausch von Daten über eine Kommunikationsverbindung ermöglichen. Schutzrelais und Feldgeräte verwendeten ursprünglich Wählleitungsmodem-Schnittstellen oder lokale RS-232-Verbindungen für die Fernkommunikation. Im Laufe der Zeit und mit der Zunahme der an der Kommunikation beteiligten Komponenten, die mit dem Wachstum der Industrie einherging, sind sie jedoch zur Vermeidung von Skalierungsproblemen zu fortschrittlicheren Protokollen übergegangen (Yadav & Paul, 2021). Ursprünglich waren die SCADA-Protokolle herstellerspezifisch und nicht interoperabel. RP-570 und Conitel sind Beispiele dafür. Wenn in immer größeren SCADA-Systemen jede Komponente ein anderes proprietäres Protokoll verwendet als die anderen Komponenten, können sie nicht mehr miteinander kommunizieren (Dey & Sen, 2020). Einige offene Standards sind aus diesem Grund und im Streben nach Interoperabilität und Kosteneffizienz entstanden. Darüber hinaus hat die Nutzergemeinschaft die Industrie dahingehend beeinflusst, eine von allen akzeptierte Standardarchitektur zu schaffen, die eine echte Interoperabilität zwischen verschiedenen Anbietern ermöglicht. So entstanden die Referenzmodelle Open Systems Interconnection (OSI) und Transmission Control Protocol/Internet Protocol (TCP/IP). (McIver McHoes & Flynn, 2011). Von diesen Modellen wurde das OSI-Referenzmodell am häufigsten auf der Ebene der industriellen Automatisierung eingesetzt. Dieses Modell wurde von der Internationalen Organisation für Normung (International Organization for Standardization, ISO) spezifiziert und besteht aus sieben Schichten, wie in der folgenden Tabelle dargestellt. Mit dem Ziel, das OSI-Referenzmodell zu vereinfachen, wurde ein EPA-Referenzmodell (Enhanced Performance Architecture) entwickelt, das auf den Schichten eins, zwei und sieben des OSI-Modells basiert und die Grundlage für Protokolle darstellt, die eine flexible und geeignete Kommunikation mit einfachen Geräten wie RTUs, IEDs, Relais usw. ermöglichen.

|  |  |  |
| --- | --- | --- |
| **Schichten und Beschreibung des OSI-Modells** | | |
| **SCHICHT** | **NAME** | **FUNKTION** |
| 7 | Anwendungsschicht | Benutzerrolle; Variablenaustausch |
| 6 | Präsentationsschicht | Konvertierung in ein für das Gerät geeignetes Format |
| 5 | Sitzungsschicht | Aufbau, Auflösung und Überwachung einer Sitzung |
| 4 | Transportschicht | Bildung, Wiederholung und Klassifizierung von Paketen |
| 3 | Netzwerkschicht | Adressierung anderer Netzwerke und Datenflusskontrolle; Kommunikationsrouten |
| 2 | Datenübertragungsschicht | Zugriffsverfahren, Kollisionsmanagement, Fehlererkennung und -beseitigung |
| 1 | Physikalische Schicht | Physikalische Übertragungsmethode; Fehlerprüfung auf Bit-Ebene |

Quelle: Rojas (2022)

Nach Yadav & Paul (2021) können Kommunikationsprotokolle in zwei Arten unterteilt werden, in kabelgebundene und drahtlose. Es folgt eine kurze Beschreibung der in der Industrie am häufigsten verwendeten kabelgebundenen SCADA-Protokolle. Für ausführlichere Beschreibungen von SCADA-Protokollen, einschließlich drahtloser SCADA-Protokolle, wird der interessierte Leser auf die Literatur verwiesen.

### Kabelgebundene SCADA-Kommunikationsprotokolle

Von den für SCADA-Systeme verfügbaren kabelgebundenen Kommunikationsprotokollen werden zunächst die Protokolle IEC 60870-5-101, DNP3 und Foundation Fieldbus beschrieben, da sie unter den offenen Standards am weitesten verbreitet sind (Yadav & Paul, 2021). Andere gängige Protokolle wie Modbus, Profibus, IEC 61850 und HART werden im Anschluss behandelt.

Bei dem IEC 60870-5-Protokoll handelt es sich um eine Reihe von Standard-SCADA-Protokollen für Fernwirkung, Fernschutz und Telekommunikation im Bereich der elektrischen Energiesysteme und -dienste (Dey & Sen, 2020). Die aus fünf Teilen bestehende Normenreihe IEC 60870-5 wurde von der dritten Arbeitsgruppe der Internationalen Elektrotechnischen Kommission (International Electrotechnical Commission, IEC), dem Technical Committee 57, in den Jahren 1990 bis 2009 entwickelt. Die fünf Teile dieser Reihe sind: (Dey & Sen, 2020):

1. Übertragungs-Frame-Formate.
2. Übertragungsprozeduren.
3. Struktur der Anwendungsdaten.
4. Definition und Codierung der Informationselemente.
5. Grundlegende Anwendungsfunktionen.

Diese Protokollreihe verwendet das EPA-Modell als Grundlage und definiert eine Basisfunktionalität für eine zusätzliche Anwenderschicht (Basisfunktionen im Zusammenhang mit dem Fernwirk-Framework), die zwischen der OSI-Anwendungsschicht (OSI-Schicht 7) und dem Anwendungsprogramm angesiedelt ist, was zu einem vierschichtigen Referenzmodell führt. Sie haben auch andere Varianten entwickelt, die auf dem Fernwirk-Framework basieren, z. B. T101, T102, T103 und T104, die Details wie Datenobjekte und Funktionscodes auf einer bestimmten Anwendungsebene charakterisieren (Yadav & Paul, 2021). Darüber hinaus enthält die IEC 60870-5-101-Variante keine Sicherheit auf der Datenübertragungsschicht und keine Anwendungsschicht, so dass das Referenzmodell in diesem Fall auf drei Schichten reduziert ist.

Das Distributed Network Protocol (DNP3) ist ein Telekommunikationsstandard. Er wurde ursprünglich für die Kommunikation zwischen einer MTU und anderen IED-Geräten definiert. Es unterstützt auch die Kommunikation mit Polling und/oder Ausnahmemethode zwischen mehreren Mastern, mehreren Slaves oder Peer-to-Peer (Zhang, 2010). DPN3 wurde zwischen 1990 und 1993 von der Firma Harris, Distributed Automation Products (ursprünglich Westronic, Inc.) entwickelt und im Jahr 1993 der Öffentlichkeit zur Verfügung gestellt. Seitdem wird es von der DNP3 Users Group verwaltet, die 1995 das DPN Technical Committee gründete (Dey & Sen, 2020). Der Grund für seine Entwicklung war das Erreichen einer offenen Interoperabilität, die durch Standards für die Kommunikation zwischen MTU und RTU oder speicherprogrammierbaren Steuerungen (SPS) unterstützt wird. Die wichtigsten Elemente des DNP3-Protokolls sind die Auflösungen der Datenverbindungsschicht, die transportspezifischen Funktionen, die Anwendungsauflösungen und die Datenverbindungsbibliothek. Dieses Protokoll ist vom EPA-Modell abgeleitet, in dem eine Pseudo-Transportschicht zwischen der OSI-Datenverbindungsschicht und der Anwendungsschicht eingefügt ist. Diese Schicht wird für die Übertragung großer Anwendungsdaten verwendet. Wie beim IEC 60870-5-Protokoll ergibt sich ein vierschichtiges Referenzmodell (Yadav & Paul, 2021).

Das Modbus-Protokoll ist ein Nachrichtenprotokoll auf Anwendungsebene für speicherprogrammierbare Steuerungen (SPS) der Modicon-Serie. Modbus wurde 1979 von der Firma Gould Modicon entwickelt (Yadav & Paul, 2021). Dieses Protokoll wurde offen veröffentlicht und ist sehr einfach zu verwenden. Daher ist es eines der am häufigsten verwendeten Protokolle für die Verbindung von elektronischen Geräten und die Interaktion zwischen MTU und RTU. Typische Modbus-Netzwerke verwenden in der Regel einen Master und unterstützen bis zu maximal 247 Slaves. Modbus wird in der Regel in SCADA-Systemen eingesetzt, in denen relativ wenige Informationen ausgetauscht werden, und das vorzugsweise zeitversetzt. Im Gegensatz zu den vorherigen Protokollen ist Modbus ein einschichtiges Protokoll, das nur vier verschiedene Arten von Kommunikationsnachrichten verwendet. Dies umfasst Anfragen und Antworten an die MTU bzw. von der MTU sowie Bestätigungen über die erfolgreiche Zustellung von Nachrichten sowohl in der MTU als auch in den RTUs. RTUs in Systemen, die dieses Protokoll verwenden, vermeiden es im Allgemeinen, auf Übertragungen zu antworten, und antworten nur, wenn die Nachrichten ausdrücklich an sie gerichtet sind. Es gibt inzwischen erweiterte Modbus-Varianten für SCADA-Systeme wie Modbus ASCII, Modbus RTU und Modbus/Ethernet (Gardner, 2020). Eine weitere Option ist Modbus/TCP, das einen konsistenten Informationsaustausch im Netzwerk (Intranet oder Internet) gewährleistet. Die Fehlererkennung erfolgt nach den Methoden des TCP/IP-Modells.

Das Open-Source-Protokoll Foundation Fieldbus (FF) wurde 2004 von der FieldComm Group in die SCADA-Anwendergemeinschaft eingeführt (Yadav & Paul, 2021). FF arbeitet mit vier Schichten, den drei Schichten des EPA-Referenzmodells, und fügt über der Anwendungsschicht eine Benutzerschicht hinzu, ähnlich dem IEC 60870-5-Protokoll. Die Benutzerschicht dient dabei als Gateway zwischen Feldgeräten und Softwareprogrammen. Außerdem ist die FF-Anwendungsschicht in zwei Teilschichten unterteilt: die FF-Zugangsschicht (FAS) und die FF-Nachrichtenspezifikation (FMS; Clarke & Reynders, 2004). Foundation Fieldbus zeichnet sich nicht nur dadurch aus, dass es ein offener Standard ist. Auch der Einsatz von multifunktionalen Geräten, die einfache Prozessintegration und die drastische Reduzierung des Verkabelungsaufwandes begründen seine Überlegenheit gegenüber anderen Protokollen.

Das 1989 vom Bundesministerium für Bildung und Forschung (BMBF) geförderte PROFIBUS-Protokoll (Process Field Bus) ist ein proprietäres Protokoll (Yadav & Paul, 2021). Profibus verwendet ebenfalls vier Schichten, ähnlich wie Foundation Fieldbus, drei Schichten des EPA-Referenzmodells und die Benutzerschicht oberhalb der OSI-Anwendungsschicht. In diesem Fall wird die Benutzerschicht verwendet, um die Profile der verwendeten Geräte und die Anwendungsbereiche in Abhängigkeit von der verwendeten Profibus-Version zu beschreiben. Profibus führt die Datenkommunikation zwischen der MTU und den RTUs zyklisch durch. Bei diesem Protokoll muss die MTU Daten von den RTU-Ausgängen lesen und Daten in die RTU-Eingänge schreiben. Es gibt drei Arten von Profibus-Protokollen: Profibus FMS, Profibus DP und Profibus PA (Clarke & Reynders, 2004). Die auf Datenerfassungssysteme ausgerichtete Version FMS (Fieldbus Message Specification) basiert auf dem objektorientierten Datenaustausch. Die Version DP (Decentralized Periphery) wird eingesetzt, wenn eine flexible Kommunikation erforderlich ist, und findet breite Anwendung in der diskreten Fertigungs- und Prozesssteuerung. Die Version PA (Process Automation) erfüllt die Anforderungen der Prozessindustrie für den Einsatz in eigensicheren und nicht eigensicheren Bereichen. Daher ist diese Version sehr empfehlenswert, wenn die Räume eigensichere Kommunikation und Geräte erfordern.

Das IEC 61850-Protokoll ist ein Open-Source-Standardprotokoll, das für Umspannwerke entwickelt wurde, die eine schnellere Kommunikation zwischen IEDs benötigen (Mackiewicz, 2006). Das IEC 61850-Protokoll besteht aus zehn Hauptteilen und wurde zwischen 1995 und 2005 vom Technischen Komitee 57 der Internationalen Elektrotechnischen Kommission (International Electrotechnical Commission, IEC) entwickelt. Die Norm IEC 61850 ist in die folgenden 10 Teile gegliedert:

1. Einführung und Übersicht
2. Wörterbuch, Begriffssammlung
3. Allgemeine Anforderungen
4. System- und Projektverwaltung
5. Kommunikationsanforderungen für Funktionen und Gerätemodelle
6. Konfigurationssprache
7. Grundlegende Kommunikationsstruktur und Objektmodell
   1. Grundsätze und Modelle
   2. Beschreibung der abstrakten Schnittstelle für Kommunikationsdienste
   3. Abstrakte gemeinsame Datenklassen
   4. Definition von logischen Knoten
8. Spezifische Abbildung von Kommunikationsdiensten
   1. Abbildung auf MMS (ISO/IEC 9506 – Teil 1 und Teil 2) und zu ISO/IEC 8802-3
9. Spezifische Abbildung von Kommunikationsdiensten
   1. Abbildung für die punkt-zu-punkt-artige unidirektionale Kommunikation von Abtastwerten
   2. Über ISO/IEC 8802-3 abgetastete Werte
10. Konformitätsprüfung (Mackiewicz, 2006)

Um die Interoperabilität zwischen den Geräten zu verbessern, haben mehrere Hersteller dieses Protokoll als Standard vorgeschlagen. Dazu gehören Alstom, ABB, SEL, Schneider, Toshiba und Siemens (Yadav & Paul, 2021). Im Gegensatz zu anderen Protokollen, die auf dem OSI-Referenzmodell basieren, beschreibt dieses Protokoll nicht nur, wie Daten gesendet und empfangen werden, sondern auch, wie sie ausgeführt und gespeichert werden. Die Struktur ermöglicht außerdem die Nutzung der abstrakten Datenmodelle der IEC 61850 durch weitere Protokolle wie Manufacturing Messaging Specification (MMS), Generic Object-Oriented Substation Events (GOOSE) und Sampled Measured Values (SMV).

Das HART-Protokoll (Highway Addressable Remote Transducer) ist ein Open-Source-Protokollstandard für die bidirektionale Anfrage-/Antwort-Kommunikation, der ursprünglich von Rosemount Inc. in den frühen 1980er Jahren entwickelt wurde und 1986 zu einem offenen Protokoll erklärt wurde (Zhang, 2020). Da es einen analogen und einen digitalen Kommunikationskanal bietet, die parallel arbeiten, gilt es als Hybridprotokoll. Es hat ein breites Anwendungsspektrum in der industriellen Prozessmessung und -regelung, das von kleinen Automatisierungssystemen bis hin zu hochkomplexen industriellen Anwendungen reicht. Die digitalen Informationen werden mit Hilfe eines Frequenzumtastungsverfahrens (Frequency Shift Keying, FSK) übertragen (Yadav & Paul, 2021). HART unterstützt Punkt-zu-Punkt-Netzwerktopologien, die sowohl digitale als auch analoge Signale über eine 4- bis 20-mA-Leitung verwenden. Es ermöglicht auch Mehrpunkt-Topologien, bei denen ein Zweileitersystem für den Anschluss von Feldgeräten verwendet wird. HART erlaubt die Übertragung von zusätzlichen Informationen zusammen mit der Prozessvariablen. Es erlaubt jedoch nicht die Übertragung von Nachrichten.

### Fragen zur Selbstkontrolle

1. Bitte vervollständigen Sie die folgenden Sätze.

* Bei der *Ring- oder Daisy-Chain*-Topologie sind alle Knoten in einer geschlossenen Schleife *verbunden*, beginnend mit *der MTU*.
* Die *dritte Schicht* des *OSI-Modells* ist die Netzwerkschicht und diese dient der Festlegung der *Kommunikationsrouten*.

1. Bitte geben Sie zu jeder der folgenden Aussagen an, ob sie richtig oder falsch ist.

* Modbus wurde 1969 von der Firma Gold Modicon entwickelt. *Falsch*
* Profibus verwendet vier Schichten, drei Schichten des EPA-Referenzmodells und die Benutzerschicht über der OSI-Anwendungsschicht. *Richtig*
* Das IEC 61850-Protokoll besteht aus sechs Hauptteilen und wurde zwischen 1993 und 2000 entwickelt. *Falsch*
* Das HART-Protokoll ist ein Open-Source-Protokollstandard für bidirektionale Anfrage-Antwort-Kommunikation, der ursprünglich von Rosemount Inc. in den frühen 1980er Jahren entwickelt wurde. *Richtig*

## 4.4 Schnittstellen

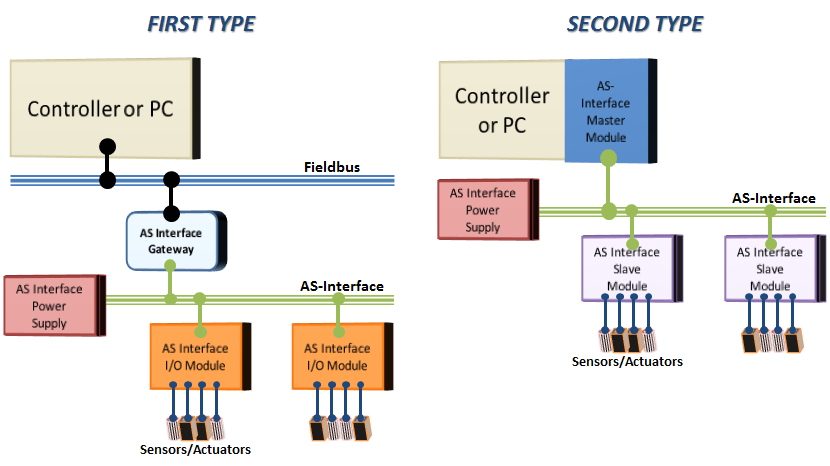
SCADA-Systeme benötigen, wie alle industriellen Steuerungssysteme, Schnittstellen, die als Bindeglied zwischen den Geräten, den Technologien und den Endnutzern dieser Systeme dienen. Diese Schnittstellen können in drei Typen unterteilt werden: Feldschnittstellen, Datenübertragungsschnittstellen und Benutzerschnittstellen.

### Feldschnittstellen

Feldschnittstellen sind Systeme zur Verbindung von Sensoren, Aktoren oder anderen Feldgeräten mit speicherprogrammierbaren Steuerungen (SPS) und/oder Fernwirkeinheiten (RTU). Die Kommunikation auf der Feldebene ist für die Automatisierung und Echtzeitsteuerung unerlässlich, da die Zustände von Geräten und Prozessen für mehrere Steuerungssysteme und Anzeigestationen lokal oder entfernt verfügbar sein müssen (Zhang, 2010). Wenn Prozesse ausgeführt werden, muss der Host-Controller (Netzwerkserver, SPS, PC, Laptop usw.) Informationen mit den Feldgeräten austauschen, um unter anderem den Gerätestatus und die Leistung zu überprüfen, sie zu konfigurieren oder zu rekonfigurieren, zusätzliche Messungen zu erfassen, Probleme zu beheben und Diagnosen durchzuführen. Eine zuverlässige und sichere Kommunikation vor Ort ist daher unerlässlich. Herkömmlicherweise werden Punkt-zu-Punkt-Netzwerke für die Ein-/Ausgangsverkabelung (E/A) verwendet, wodurch viele Kabelstrecken für jedes Feldgerät erforderlich sind, wenn eine zentrale Stelle mit jedem einzelnen E/A-Punkt verbunden ist. Diese Methode benötigt viel Platz und ist sehr teuer. Außerdem können sie für die Anforderungen des Datenaustauschs zwischen den gesteuerten Geräten und den Steuerungen sehr langsam und für einfache binäre Geräteverbindungen zu kompliziert sein. Zur Lösung dieses Problems werden die Aktor-Sensor-Schnittstelle (AS-Interface oder AS-i), HART (Highway Addressable Remote Transducer) und Feldbusse eingesetzt, die sich als wirtschaftlicher und zuverlässiger für die Produktionsautomatisierung und die Prozesssteuerung in Echtzeit erwiesen haben (Zhang, 2010).

Die Aktor-Sensor-Schnittstelle, AS-Interface oder AS-i, ist ein Bussystem, das in der Industrieautomatisierung für Anwendungen auf niedriger Ebene eingesetzt wird. Zur Entwicklung einer offenen Feldbusspezifikation gründeten die Sensorhersteller, die AS-i entwickelt und 1994 auf den Markt gebracht hatten, die AS-i Association (Park et al., 2003). Diese Schnittstelle ermöglicht die Kommunikation mit kleinen binären Sensoren und Aktoren über ein einziges Kabel für alle Geräte unter Verwendung des AS-Interface-Standards. Es hat sich weltweit zum Standard in der Prozessindustrie entwickelt, da es Automatisierungssysteme effektiv modernisiert, indem es Kabelbäume und Verteilerkästen überflüssig macht und die Größe der benötigten Schaltschränke erheblich reduziert.

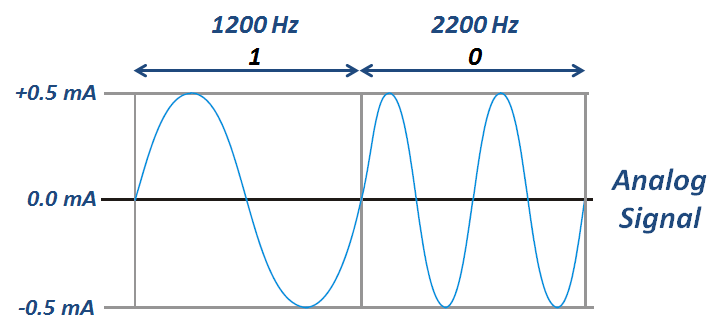
AS-Interface-Architekturen



Quelle: Rojas (2022)  
Die verwendete Plug-and-Play-Verkabelung ermöglicht alle Typologien und verwendet zwei Verbindungsarchitekturen (Zhang, 2010). Die erste Art der AS-Interface-Architektur verbindet über Feldbusse wie Profibus oder Foundation Fieldbus eine programmierbare Steuerung (SPS, SCADA oder PC) mit den zu steuernden Sensoren und Aktoren. AS-Interface benutzt Gateways, die direkt mit dem Feldbus verbunden sind, und E/A-Module, die mit Sensoren und Aktoren verbunden sind. Je nach Design und Systemanforderungen können mehrere AS-i Gateways an den Feldbus angeschlossen werden. Die zweite Art der AS-Interface-Architektur verwendet ein AS-i-Mastermodul, das sich in der programmierbaren Steuerung (SPS, SCADA oder PC) befindet. Mit dem AS-i-Master-Modul ist es möglich, sowohl analoge als auch digitale AS-i-Slaves direkt anzuschließen. In diesem Fall verwalten die AS-i-Slave-Module die Sensoren und Aktoren anstelle der Busse der Feldebene. Die Verbindung zwischen den einzelnen Modulen erfolgt über AS-i-Kabel, wobei Kabelverteiler eingesetzt werden können, wenn eine verzweigte Verbindung erforderlich ist. Zur Bildung von Teilabschnitten des industriellen Steuerungsnetzwerks können Cluster von Slave-Modulen gegebenenfalls einzelne Schnittstellenkabel verwenden. Abhängig von den Anforderungen des projektierten Systems kann ein AS-i Mastermodul die Verbindung mehrerer Segmente ermöglichen (Zhang, 2010). Die obige Abbildung zeigt die beiden AS-Interface-Architekturen.

HART wurde in den frühen 1980er Jahren entwickelt und gilt als erste Realisierung eines Feldbusses. Im Juli 1993 wurde die HART Communication Foundation gegründet, um die Weiterentwicklung und weltweite Anwendung dieser Technologie zu fördern. HART ist eine bidirektionale hybride analoge und digitale Kommunikationsschnittstelle und ein Protokoll, das mit Stromsignalen von 4 bis 20 mA arbeitet (Park et al., 2003). Der Hauptvorteil besteht darin, dass die vorhandene Instrumentenverkabelung von 4 bis 20 mA beibehalten werden kann, während diese Kabel gleichzeitig für die Übertragung des analogen Signals mit überlagerten digitalen Informationen verwendet werden. Aus diesem Grund wird HART auch in der Feldebene für konventionelle Messgeräte und Anlagen in industriellen Steuerungssystemen in großem Umfang eingesetzt, da es eine relativ einfache Punkt-zu-Punkt-Verbindung ohne zusätzliche Verkabelung ermöglicht.

HART Digitale Symboldarstellung

  
Quelle: Rojas (2022)

Für die digitale Darstellung verwendet HART eine auf dem Kommunikationsstandard Bell 202 basierende Technik, die Frequenzumtastung (Frequency Shift Keying, FSK). Darin werden die Symbole „0“ und „1“ durch die spezifischen Frequenzen 2200 bzw. 1200 Hz repräsentiert. Darüber hinaus wird das analoge 4-20-mA-Signal nicht gestört, da der Mittelwert der überlagerten Sinuswellen gleich Null ist und sein ursprünglicher Wert erhalten bleibt. (Mackay et al., 2004). Nach Zhang (2010) bietet die vollständige Nutzung der HART-Kommunikation viele Vorteile, da sie den Anlagenbetrieb verbessert, die Effizienz erhöht und die mit ungeplanten Abschaltungen und Prozessunterbrechungen verbundenen Kosten reduziert. Das HART-Kommunikationsprotokoll ist mit den Steuerungs-, Mess-, Regel- und Automatisierungssystemen der wichtigsten Hersteller auf der ganzen Welt kompatibel. HART ist zudem eine gute Alternative, wenn eine bestehende Anlage nachgerüstet werden soll, da viele Anbieter von Automatisierungssystemen direkte E/A anbieten, die für die Verwendung mit HART geeignet sind. Darüber hinaus bietet es Echtzeitdiagnose und multivariable Prozessinformationen durch Überwachung des Gerätestatus in intelligenten HART-Feldgeräten mit Hilfe spezieller PC-basierter Softwareprogramme. Die digitale Darstellung auf der HART-Schnittstelle ist in der folgenden Abbildung dargestellt.

Als Ersatz für die HART-Technologie wurden Feldbusse entwickelt, die vor allem durch die Reduzierung der für HART erforderlichen langen Spezialkabel und Abschlusswiderstände Kosten einsparen sollen (Zhang, 2010). Ein weiteres Ziel war die Bereitstellung einer schnellen und fortschrittlichen Diagnose zur Verkürzung der Entwicklungs- und Konfigurationszeiten und zur Beschleunigung der Verifizierungs- und Inbetriebnahmeverfahren mit dem Hauptziel, eine maximale Verfügbarkeit der Anlage zu erreichen. Ursprünglich wurden mehrere Feldbus-Standards entwickelt und von lokalen Industrieorganisationen verabschiedet. 1990 wurde das IEC/ISA SP50 Komitee gegründet, das sich aus verschiedenen nationalen Organisationen zusammensetzt, wie z. B. (PROFIBUS) dem deutschen nationalen Standard, (FIP) dem französischen nationalen Standard, der Instrument Society of America (ISA) und der International Electrotechnical Commission (IEC), um diese Standards zu vereinheitlichen.

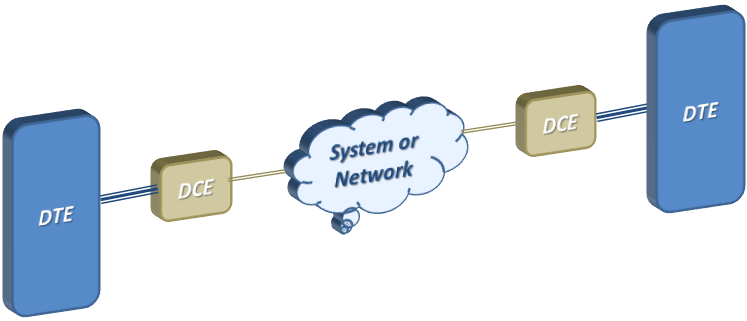
Feldbusse sind bidirektionale, serielle, digitale Multidrop-Kommunikationsnetzwerke für Feldgeräte, die von der Steuerungszentrale entfernt sind. Um dies zu erreichen, müssen die vernetzten Feldgeräte über eine installierte Rechenkapazität verfügen, die es ihnen ermöglicht, einfache Funktionen wie Wartung, Steuerung und Diagnose selbständig auszuführen, sowie bidirektionale Kommunikationsfähigkeiten anzubieten. Im Vergleich zu HART ist die Art der Verkabelung bei Feldbussen völlig anders (Park et al., 2003). Die Kommunikation erfolgt im Allgemeinen über die Struktur der Hierarchieebenen (Verwaltung, Steuerung und Feld). Bei Feldbussen verbindet eine einzige, vollständig parallele Zweidrahtleitung alle Geräte mit der Zentrale und ersetzt die herkömmliche analoge 4-20-mA-Versorgungsleitung. Darüber hinaus können auch völlig unterschiedliche Feldgeräte angeschlossen werden, unabhängig davon, ob sie kontinuierlich oder diskontinuierlich gesteuert werden. Kurzum, flexible Feldbusse bieten eine Vielzahl von Anwendungsmöglichkeiten, die normalerweise nicht immer notwendig sind (Zhang, 2010).

Auch wenn es den Anschein hat, dass ein einziges Feldbussystem für alle Anwender:innen geeignet ist, ist dies nicht immer der Fall (Park et al., 2003). Es gibt viele Systeme, deren Feldanwendungen nur eine binäre Kommunikation (Ein/Aus) zur Meldung des Zustands eines einfachen Geräts (Endschalter, Näherungsschalter usw.) oder zum Senden des Steuersignals an ein einfaches Stellglied (Relais, Ein/Aus-Ventil usw.) erfordern. Die Reaktionszeiten müssen jedoch kurz sein (Millisekunden), da diese Anwendungen in der Regel in Echtzeit ablaufen (Park et al., 2003). Ein Lösungsansatz besteht darin, die Komponenten über ein vereinfachtes Bussystem wie AS-Interface miteinander zu verbinden. Wenn es sich hingegen um komplexe Komponenten wie SPS, PLS oder Bedienstationen handelt, sind normalerweise Nachrichten von mehreren Bytes Länge und Aktualisierungszeiten zwischen 10 und 100 ms erforderlich. In diesem Fall sind aufgrund der hohen zu übertragenden Datenmengen größere Informationspakete erforderlich. Aus diesem Grund wurden verschiedene Feldbuskonzepte entwickelt, die alle unterschiedliche Zielanwendungen, Geschwindigkeiten und Technologien haben. Sie werden nach der Länge (Bit, Byte oder Nachricht) des Wortes klassifiziert, das von den jeweiligen Komponenten für eine korrekte Kommunikation benötigt wird. Nach Zhang (2010) gibt es mehr als 100 verschiedene Arten von Feldbussen, von denen nur einige wenige wie Profibus (Process Fieldbus), Foundation Fieldbus H1, P-net, ControlNet, Foundation Fieldbus High-Speed Ethernet (HSE), Interbus-S und World-FIP als Standard anerkannt sind. Alle diese Feldbusse verwenden den IEC-61158-Standard. Dieser Standard besteht aus einer Reihe von Protokollen, die für Netzwerke im Bereich der industriellen Datenverarbeitung für die verteilte Steuerung in Echtzeit entwickelt wurden.

### Datenübertragungsschnittstellen

Unter Datenübertragung versteht man die Übermittlung digitaler elektrischer oder elektromagnetischer Signale von einem beliebigen Ausgangspunkt zu einem räumlich entfernten Ziel mit Hilfe elektrischer Mittel (Zhang, 2010). Datensignale werden von Geräten oder Anlagen (SPS, Roboter, Drucker, PC usw.) gesendet und/oder empfangen, die als Datenendeinrichtungen (DEE) bezeichnet werden und in der Regel über industrielle Netzwerke oder Steuerungssysteme miteinander verbunden sind. Diese Datensignale sind zwar digital, müssen aber als analoge elektrische Signale über eine Leitung übertragen werden. Daher werden Multiplexer oder Modems, die allgemein als Datenübertragungseinrichtungen (DÜE) bezeichnet werden, als Digital-Analog-Wandler und umgekehrt benötigt. Bei Übertragungssteuerungsgeräten um spezielle Komponenten, die entweder die synchrone oder die asynchrone Datenübertragung zwischen den DEE verwalten. Um andererseits Inkompatibilitäten zwischen DEE und DÜE zu vermeiden, wurden spezielle Schnittstellen als DEE-DÜE-Schnittstellenstandards entwickelt. RS-232 und RS-485 sind die grundlegenden klassischen DEE-DÜE Schnittstellenstandards. Sie sind Teil der Recommended-Standard-Reihe (RS) der EIA (Electronic Industries Alliance). Es ist zu beachten, dass die EIA-Normen keine Protokolle beschreiben, sondern nur die mechanischen und elektrischen Eigenschaften der Schnittstelle festlegen. In SCADA-Systemen, in denen Modems für die Übertragung über große Entfernungen erforderlich sind, sind die RS-232- und RS-485-Schnittstellen die strategische Komponente für die Übertragung digitaler Informationen zwischen RTUs und Modems (Clarke & Reynders, 2004).

Schema der Datenübertragungsschnittstelle



Quelle: Rojas (2022)

Der RS-232C-Schnittstellenstandard (CCITT V.24-Schnittstellenstandard) ist der am weitesten verbreitete Standard. Er wurde für die Datenkommunikation zwischen DEE- und DÜE-Geräten unter Verwendung des binären seriellen Datenaustauschs entwickelt (Bailey & Wright, 2003). Dieser Kommunikationsstandard legt die genauen Anforderungen an die Schnittstellen fest, die für den Anschluss von Datenverarbeitungsgeräten an das Telefonsystem der Bell Company erforderlich sind. Er ist das Ergebnis einer 1969 in den USA begonnenen Zusammenarbeit zwischen einigen der größten Hersteller von Kommunikationsgeräten, den Bell Laboratories und dem EIA Engineering Department (Bailey & Wright, 2003). Dieser Standard wird immer noch allgemein als RS-232 bezeichnet, obwohl er ständig überarbeitet und aktualisiert wird, wie z. B. die Revision EIA-232E von 1991. Die drei Teile der Spezifikation dieses bekannten Standards (EAI-232 oder RS-232) sind folgende:

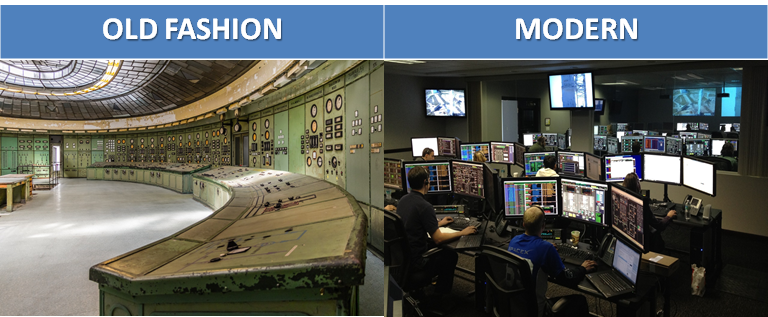
* + Erdungsmerkmale, verwendete Schaltkreise und Spannungspegel (elektrische Signalspezifikation).
  + DEE-DÜE-Schnittstelle (mechanische Spezifikation).
  + Steuer-, Zeit- und Datensignale zwischen DEE und DÜE (Funktionsbeschreibung der Datenkommunikation) (Bailey & Wright, 2003; Park et al., 2003; Clarke & Reynders, 2004; Mackay et al., 2004).

Bei der seriellen Datenkommunikation hingegen können mit der EAI-485- bzw. RS-485-Schnittstelle größere Entfernungen und Geschwindigkeiten (bis zu 1200 m bzw. 10 Mbit/s) zuverlässig erreicht werden, da sie neben der üblichen Punkt-zu-Punkt-Verbindung auch eine Mehrpunkt-Vernetzung über zwei Kabel ermöglicht (Bailey & Wright, 2003; Park et al., 2003; Clarke & Reynders, 2004; Mackay et al., 2004). Die maximale Anzahl von Sendern und Empfängern, die mit Hilfe dieser Schnittstelle auf derselben Leitung platziert werden können, beträgt jeweils 32 Stück. Die logische Eins und die logische Null werden durch Leitungsspannungen im Bereich von -6 V bis -1,5 V bzw. +1,5 V bis +6 V dargestellt. Der Leitungstreiber für die RS-485-Schnittstelle erzeugt pro Kanal eine Differenzspannung von 5 Volt zwischen zwei Leitungen. Daher ist ein zusätzliches Kabel erforderlich, um eine gemeinsame Referenzspannung für das System und alle seine Komponenten bereitzustellen, so dass für Halbduplex-Systeme drei Kabel und für Vollduplex-Systeme fünf Kabel erforderlich sind. Im Gegensatz zur RS-232-Schnittstelle erlaubt die RS-485-Schnittstelle einen Dreizustandsbetrieb für Leitungstreiber. Zusätzlich zu den typischen logischen Werten (0 und 1) gibt es einen neuen Zustand, der als Zustand hoher Impedanz oder deaktivierter Zustand bezeichnet wird, in dem das Steuergerät nicht online zu sein scheint, da es keinen Strom verbraucht. Die Leitungstreiber-IC verfügt über einen Pin, der es ermöglicht, ein Steuersignal einzugeben, um den hochohmigen Zustand auszulösen. Diese Schnittstellenfunktion ermöglicht die Verwendung einer einzigen Leitung für eine Mehrpunktanlage. Es kann jeweils nur ein Sender aktiv sein. Es ist jedoch möglich, bis zu 32 Sender an eine Leitung anzuschließen. Außerdem muss jedem Terminal eine eindeutige Adresse zugewiesen werden, um Konflikte zwischen den verschiedenen Komponenten des Mehrpunktsystems zu vermeiden. Schließlich wird bei Konflikten der Strom über die RS-485-Schnittstelle begrenzt, um Schäden am System zu vermeiden (Bailey & Wright, 2003).

### Benutzerschnittstellen

Benutzerschnittstelle ist ein technischer Begriff, der alle Vorrichtungen oder Mittel umfasst, die die Kommunikation des Menschen mit den von ihm benutzten Maschinen erleichtern (Zhang, 2010). Die Benutzerschnittstelle von SCADA-Systemen wird üblicherweise als Mensch-Maschine-Schnittstelle (MMS; auch Human-Machine Interface, HMI) bezeichnet, aber auch als Human-Computer Interface (HCI) (Dey & Sen, 2020). Grafische Benutzeroberflächen (GUI) und Web-Benutzeroberflächen (WUI) sind die heutzutage üblicherweise verwendeten Arten von Benutzerschnittstellen. GUIs liefern im Allgemeinen eine grafische Rückmeldung an ein Ausgabegerät, die mit einem von einem Eingabegerät erlaubten Zugriff verknüpft ist. Ein- und Ausgabe in die WUI erfolgen über Webseiten, die vom Benutzer in einem Webbrowser betrachtet und/oder über das Internet verbreitet werden können. Benutzerschnittstellen wie diese sind nicht nur zu einem wichtigen Bestandteil von SCADA-Systemen, sondern auch der meisten modernen automatisierten Systeme geworden (Displays für Fahrzeugführer, Schiffs- und Flugzeugsteuerungen, Mensch-Roboter-Kommunikationsschnittstellen, Monitore für medizinische Instrumente und Luft- und Raumfahrzeuge usw.; Zhang, 2010). Je nach Anwendung kommen unterschiedliche Techniken und Methoden zum Einsatz. Im Wesentlichen erfüllen Benutzerschnittstellen zwei Aufgaben: Sie übermitteln alles, was der Benutzer anfordert, an die Maschine und sie geben die Antworten, welche die Maschine dem Benutzer gibt, an den Benutzer zurück (Zhang, 2010).

Benutzerschnittstellen in Steuerungszentralen

  
Quelle: Pixabay (2012) & Pixabay (2016). CC

Im Allgemeinen verwenden SCADA-Systeme grafische Benutzeroberflächen (GUIs) zur dynamischen grafischen Anzeige, die es ermöglichen, Hinweise, Variablen und Betriebsparameter in Echtzeit über schematischen Anlagendiagrammen anzuzeigen (Gardner, 2020). Dort können sie eine unendliche Anzahl von Werten für Tankfüllstände, Temperaturen, Drücke, Viskositäten, Durchflussmengen, Kraftwerkseinspeisungen, Ventil- und Schieberstellungen, chemische Reaktionskonzentrationen, Reinheitsgrade, Ein- und Ausschaltzustände von Anlagen und vieles mehr beobachten. All dies ermöglicht es dem Bediener im Kontrollraum, in der Produktionsanlage oder aus der Ferne, die Überwachungsaufgaben (Überwachung, Aufzeichnung und Diagnose des Zustands des Produktionsprozesses) durchzuführen und das System über Geräte wie Steuerkonsolen, Tastaturen, Mäuse, Touchscreens und sogar Laptops, Tablets und Smartphones für den lokalen oder Fernzugriff zu steuern. SCADA-Systeme verwenden zur Navigation durch die verschiedenen Prozessphasen häufig Seitenstrukturen. Wenn sie sorgfältig programmiert sind, enthalten sie Links zwischen den Seiten, die dem Bediener einen schnellen und direkten Zugriff ermöglichen (Dey & Sen, 2020; Gardner, 2020). Unabhängig davon, wie hoch entwickelt und automatisiert der Produktionsprozess ist, wird der Bediener in SCADA-Systemen zu einem wesentlichen Bestandteil des Regelkreises.

Benutzerschnittstellen in SCADA-Systemen ermöglichen nicht nur die Überwachung und Steuerung in Echtzeit, sondern auch andere wichtige Aufgaben wie die Erstellung von Berichten, die Darstellung historischer Informationen und die Anzeige von Alarmsignalen (Gardner, 2020). Die Erstellung von Berichten beruht auf der Berechnung statistischer Daten über den Prozess in Echtzeit, die vom SCADA-System durchgeführt wird und dem Bediener zu einem bestimmten Zeitpunkt präsentiert oder ausgedruckt wird. In der Regel ist dieser so programmiert, dass er sich regelmäßig wiederholt und vom Bediener geändert werden kann. Diese Berichte können die Anlagenleistung anhand von Indikatoren wie Brennstoffverbrauchsraten, Produktionstrends oder Versorgungskosten aufzeigen. So können die Bediener:innen die Anlagensysteme anpassen, um die wirtschaftliche Rentabilität zu verbessern. Die Darstellung historischer Informationen erfolgt in der Regel auf Anforderung des Bedieners oder eines anderen Nutzers auf Managementebene, der Trendanalysen, wirtschaftliche Belastungsanalysen und Vorhersagen durchführen möchte, um die Erfüllung vertraglicher Verpflichtungen zu fördern, aktuelle Probleme zu lösen oder zukünftige Entscheidungen zu planen. Die Dauer der Aufbewahrung historischer Daten hängt von der Speicherkapazität der Datenbanken sowie von den Interessen und der Planung des Unternehmens ab. Die Anzeige von Alarmsignalen hat den Zweck, den Bediener auf eine Störung oder das Vorhandensein eines gefährlichen oder unzulässigen Zustands aufmerksam zu machen. Diese Signale können sowohl sichtbar als auch hörbar sein. Repräsentative Alarmtafeln werden häufig in Schnittstellenkonfigurationen angezeigt, die die Systemhardware imitieren, so dass der Bediener den gleichen visuellen Eindruck erhält, als stünde er vor dem Gerät (Dey & Sen, 2020).

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie die drei Arten von Schnittstellen, die in SCADA-Systemen verwendet werden.

* *Die Feldschnittstellen*
* *Die Datenübertragungsschnittstellen*
* *Die Benutzerschnittstellen*

1. Geben Sie an, wann die Aktor-Sensor-Schnittstelle, AS-Interface oder AS-i, entwickelt und auf den Markt gebracht wurde.

* 1992.
* 1991.
* *1994.*
* 1993.

Zusammenfassung

SCADA ist die Abkürzung für Supervisory Control and Data Acquisition Systems (Überwachungs-, Steuerungs- und Datenerfassungssysteme) und entstand ursprünglich aus dem Bedarf der chemischen, petrochemischen, Öl-, Gas- und Stahlindustrie sowie der Stromerzeugung und -übertragung, den Zustand ihrer Geräte, Maschinen und Anlagen zu überwachen und zu steuern. Daher ist es für das Verständnis dieses Bereichs unerlässlich, die Zusammensetzung dieser Systeme zu kennen und zu wissen, wie sie ihre Funktionen erfüllen, um Automatisierungsaufgaben in Produktions- und Fertigungsprozessen zu erfüllen. Aus diesem Grund werden im Abschnitt „Überblick“ die Bestandteile von SCADA-Systemen und die vier Hauptfunktionen Datenerfassung, Datenkommunikation, Datendarstellung und Systemsteuerung beschrieben. Der Abschnitt „Komponenten“ beschreibt den zentralen Host, die Master-Station oder das Master-Terminal-Gerät (MTU) als Kernkomponente des SCADA-Systems, die Felddatenschnittstellengeräte (RTUs und PLCs), die für die Verbindung der MTU mit der Feldinstrumentierung verantwortlich sind, die Kommunikationsinfrastruktur (kabelgebunden oder drahtlos) mit ihren zwei Kommunikationsmodellen für SCADA-Systeme und die Feldinstrumentierung, Sensoren und Aktoren, die dafür verantwortlich sind, Informationen zu sammeln und die lokale Leistung in den verschiedenen Phasen des Produktions- oder Herstellungsprozesses zu steuern. Der Abschnitt „Kommunikationstechnologien“ beschreibt die verschiedenen Topologien, die für SCADA-Kommunikationsnetzwerke verwendet werden. Außerdem werden die Kommunikationsprotokolle beschrieben, die für eine erfolgreiche Kommunikation zwischen den verschiedenen Geräten, die in einem Netzwerk miteinander verbunden sind, verantwortlich sind, sowie die wichtigsten kabelgebundenen Kommunikationsprotokolle, die in SCADA-Systemen verwendet werden. Schließlich werden im Abschnitt „Schnittstellen“ die verschiedenen Arten von Schnittstellen (Feld-, Datenübertragungs- und Mensch-Maschine-Schnittstellen) vorgestellt, die als Bindeglied zwischen den Geräten, Technologien und Endnutzern von SCADA-Systemen dienen.

Lektion 5 – Industrielle Kommunikationstechnologien

**Lernziele**

Nach der Bearbeitung dieser Lektion …

… können Sie zwischen industriellen und kommerziellen Netzwerken unterscheiden.

… kennen Sie die Komponenten der industriellen Kommunikationsnetze.

… verstehen Sie die wichtigsten industriellen Kommunikationsprotokolle.

… erkennen Sie die drahtlosen Kommunikationstechnologien.

… können Sie OPC als das Prozesssteuerungs-Kommunikationsprotokoll identifizieren.

… können Sie KNX und LonTalk als die wichtigsten Protokolle für die Gebäudeautomation unterscheiden.

5. Industrielle Kommunikationstechnologien

## Einführung

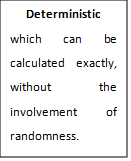
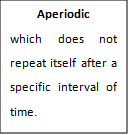
Das Gebiet der industriellen Kommunikationstechnik ist sehr breit gefächert und umfasst alles, was mit den verschiedenen Arten von industriellen Netzwerken zu tun hat, wie z. B. Steuerungsnetzwerke, Überwachungsnetzwerke und Kommunikationsnetzwerke. Die verschiedenen Netzwerktypologien oder -architekturen, die Netzwerkelemente (Ausrüstung, Komponenten und/oder Geräte), die Kommunikationsprotokolle und -schnittstellen der Netzwerke, die Software, die sie verwaltet, und andere Details werden ebenfalls betrachtet. Aufgrund dieses Umfangs bietet diese Lektion nur eine kurze Einführung in den Bereich der industriellen Kommunikationstechnologien, insbesondere in industrielle Netzwerke, HART, PROFIBUS, drahtlose Kommunikation, OPC, Konnex (EIB/KNX) und LonWorks.

## 5.1 Industrielle Netzwerke

Industrielle Netzwerke, industrielle Kommunikationsnetzwerke oder industrielle Steuerungsnetzwerke (Industrial Control Networks, ICN) sind integrierte Kommunikationssysteme, die miteinander verbundene Geräte zur Überwachung und Steuerung von Produktions- und Fertigungsprozessen verwenden. (Decotignie & Pleinevaux, 1993; Zhang, 2010; Galloway & Hanke, 2013). ICNs sind verantwortlich für die Implementierung von Kommunikationsprotokollen zwischen Feldgeräten, Steuergeräten, einer Reihe von computergestützten Systemen und mit externen Systemen. ICNs unterscheiden sich aufgrund der besonderen Anforderungen an ihren Betrieb deutlich von typischen Geschäfts- oder Unternehmensnetzwerken. Die Überwachung und Steuerung physischer Systeme unterliegt strengen Regeln und zeitlichen Beschränkungen, deren Nichteinhaltung zu Schäden und sogar zum Verlust von Menschenleben führen kann (Decotignie & Pleinevaux, 1993). Trotz der funktionalen Unterschiede zwischen diesen beiden Netzwerktypen hat die Notwendigkeit, das Management in die Entscheidungsfindung im Produktionsprozess einzubeziehen, zu einer zunehmenden Integration zwischen beiden geführt. Die Trennlinie zwischen den beiden Netzwerktypen wird dadurch unschärfer. In den höheren Ebenen der Netzwerkstruktur hat sich daher in letzter Zeit eine starke Abhängigkeit von Web- und Ethernet-Standards entwickelt, die typisch für kommerzielle oder geschäftliche Computernetzwerke sind. Aus diesem Grund müssen die an der Entwicklung und Wartung von ICNs beteiligten Spezialisten in der Lage sein, sowohl mit den üblichen geschäftlichen Anforderungen, einschließlich der Netzwerksicherheit, als auch mit den üblichen industriellen Anforderungen, wie z. B. dem angemessenen Umgang mit Antwortzeiten und dem damit verbundenen Determinismus, umzugehen (Galloway & Hancke, 2013).

### Unterschiede zwischen industriellen Netzwerken (ICNs) und kommerziellen Netzwerken (Commercial Networks, CCNs)

Im Folgenden werden einige Unterschiede zwischen herkömmlichen Kommunikationsnetzen und industriellen Netzwerken nach Galloway & Hancke (2013) kurz beschrieben:

1. Während der Anwendungsbereich von NICs sehr breit ist und sämtliche Produktionsprozesse, die Stromerzeugung, die Wasserversorgung und die Fertigung umfasst, ist der Anwendungsbereich von CCNs etwas eingeschränkter. Er bezieht sich im Allgemeinen auf Unternehmen und Haushalte (Decotignie & Pleinevaux, 1993; Galloway & Hancke, 2013).
2. Ungeachtet der leicht unterschiedlichen Anforderungen in den verschiedenen industriellen Bereichen, in denen sie eingesetzt werden, besteht die Hauptfunktion von ICNs darin, physische Geräte zu überwachen und zu steuern, während CCNs in erster Linie der Verarbeitung und Übertragung von Daten dienen (Decotignie & Pleinevaux, 1993).
3. Die Architektur der ICNs ist in der Regel breiter als die der CCNs und umfasst in kleinen Industrien drei oder vier Hierarchieebenen (Feld, Steuerung, Überwachung und Verwaltung). In Unternehmen oder Konzernen hingegen bestehen die CCNs in der Regel aus lokalen Netzwerken (LANs) der einzelnen Niederlassungen oder Zweigstellen, die über ein Wide Area Network (WAN) oder ein Backbone-Netz miteinander verbunden sind (Galloway & Hancke, 2013).
4. Die Geschwindigkeit, mit der die angeschlossenen Geräte und Prozesse auf den verschiedenen Ebenen des ICN arbeiten, erfordert eine adäquate Datenverarbeitung und -übertragung mit einer angemessenen Reaktionszeit. Technisch ist festgelegt, dass die Reaktionszeit kleiner sein muss als die Abtastzeit der erfassten Daten. Bei CCN gibt es diese Einschränkung nicht, da die Echtzeitreaktion für ihre Leistung nicht entscheidend ist (Decotignie & Pleinevaux, 1993).
5. In ICNs muss die Datenübertragung auf der Feldebene nicht nur in Echtzeit erfolgen, sondern auch **deterministisch** sein, d. h. es muss vorhersagbar sein, wann die Antwort auf diese Übertragung empfangen wird. Dies ist für CCNs im Allgemeinen nicht so wichtig, da sie nicht so anfällig für Schwankungen sind wie ICNs, mit Ausnahme von Voice-over-Internet-Protokollen, die eine gewisse Stabilität für die Sprachübertragung erfordern (Galloway & Hancke, 2013).
6. Die Größe der Datenfelder, die auf den verschiedenen Ebenen des ICN übertragen werden, ist in der Regel sehr gering (einige Bytes), insbesondere auf Feldebene, wo es wahrscheinlich nur erforderlich ist, regelmäßig oder periodisch einen numerischen Wert oder eine einfache Messung zusammen mit einigen allgemeinen Informationen zu übertragen. Im Gegensatz dazu beträgt die Mindestgröße eines Datenfeldes im CCN 64 Byte, und es werden regelmäßig Felder in der Größenordnung von Kilobyte und mehr übertragen. Daher sind ganz andere Kommunikationsprotokolle erforderlich (Galloway & Hancke, 2013).
7. Die Auswirkungen des Auftretens von Fehlern sind in den CCNs viel geringer als in den ICNs. Im letzteren Fall kann die Verbindung großer physischer Geräte und Anlagen nicht nur zu Schäden an diesen Anlagen, sondern auch zu Produktverlusten, Umweltzerstörung, Rufschädigung und sogar zur Gefährdung von Menschenleben führen (Decotignie & Pleinevaux, 1993; Galloway & Hancke, 2013).
8. Bei den **aperiodischen** Übertragungen, die in den ICNs durchgeführt werden, ist es regelmäßig erforderlich, den Zeitpunkt der Übertragungen und die Reihenfolge der Ereignisse im Netzwerk festzustellen. Hierfür sind synchronisierte Uhren und eine zeitliche Signalisierung von Ereignissen erforderlich. Diese Möglichkeit, die zeitliche Kohärenz und die Reihenfolge der Datenübermittlung zu gewährleisten, ist in den üblicherweise verwendeten Netzwerkprotokollen wie dem Transmission Control Protocol/Internet Protocol (TCP/IP), das in der Regel im CCN verwendet wird, praktisch nicht vorgesehen (Galloway & Hancke, 2013).
9. Die Arbeitsbedingungen in den Betriebsumgebungen der ICNs sind oft lebensfeindlich, mit einem hohen Maß an Hitze, Feuchtigkeit, Staub und Vibrationen, im Gegensatz zu den sauberen und oft speziell klimatisierten Umgebungen für hochempfindliche Geräte in den CCNs. ICN-Komponenten müssen robust sein und einen angemessenen Schutz gegen Schäden durch Feuchtigkeit und/oder Staub aufweisen, um den rauen Arbeitsbedingungen standzuhalten. (Decotignie & Pleinevaux, 1993).

### Von ICNs verarbeitete Informationen

Nach Moyne & Tilbury (2007) verarbeiten ICNs drei Arten von Informationen: Steuerungsinformationen, Überwachungsinformationen und Sicherheitsinformationen.

1. Die Steuerungsinformationen werden zwischen den Geräten (Sensoren und Aktoren) und den Steuerungen in Echtzeit ausgetauscht und umfassen die Eingangs- oder Ausgangssignale der Regel- oder Rückkopplungskreise.
2. Überwachungsinformationen sind andere Informationen, die von Sensorgeräten erfasst werden, auf die aber kein Regelsystem reagiert, sondern die dazu dienen, den Zustand der Anlagen zu beurteilen. Obwohl für Überwachungsinformationen zeitliche Konsistenz und minimale Datenverluste erforderlich sind, sind die Anforderungen an die Echtzeit wesentlich geringer als bei Steuerungsinformationen, da sie nur zur Erfassung und/oder Anzeige benötigt werden, aber keine Reaktion erfordern.
3. Sicherheitsinformationen sind für die Ausführung kritischer Funktionen, wie die Verwaltung von Schutzschaltungen oder das sichere Abschalten von Geräten, unerlässlich. Diese Informationen stellen nicht nur hohe Anforderungen an die Echtzeitfähigkeit. Sie erfordern auch ein hohes Maß an Zuverlässigkeit. Wegen der erforderlichen Zuverlässigkeit der Sicherheitsinformationen, ihrer begrenzten Anwendbarkeit und der hohen Kosten für ihre Implementierung werden Sicherheitsnetzwerke in der Regel getrennt aufgebaut.

Darüber hinaus enthalten die ICNs auch sogenannte historische Informationen. Diese Informationen umfassen alles, was aufgezeichnet, gespeichert und für den Offline-Abruf verfügbar ist. Dazu gehören daher alle in der Anlage verfügbaren Informationen zur Steuerung, Überwachung und/oder Sicherheit sowie berechnete Werte oder Referenzpunkte, die ebenfalls für die Analyse nützlich sein können (Galloway & Hancke, 2013).

### ICN-Komponenten

ICNs bestehen aus spezialisierten Geräten und Systemen wie speicherprogrammierbaren Steuerungen (SPS), übergeordneten Steuerungs- und Datenerfassungssystemen (SCADA) und Prozessleitsystemen (PLS) (Galloway & Hancke, 2013). Die Kommunikation zwischen und innerhalb dieser Komponenten ist die wesentliche Aufgabe der ICNs. SPS-Systeme sind der zentrale Bestandteil von ICNs, da sie in der Regel für die eigentliche Implementierung und Verwaltung der Steuerungs- und Sicherheitslogik verantwortlich sind, die für den Betrieb der Produktions- und Fertigungsprozesse, an die sie angeschlossen sind, verwendet wird. Die Protokolle, die die Übertragung von Informationen zwischen Feldgeräten und SPS-Systemen, zwischen SPS-Systemen untereinander und zwischen SPS-Systemen und Spezialsystemen regeln und ermöglichen, machen einen großen Teil der ICNs aus. Spezialisierte Systeme hingegen sind für Funktionen wie die Datenerfassung, die Überwachung von Anlagen und deren Betrieb sowie die Bereitstellung von Mensch-Maschine-Schnittstellen zuständig, die es ermöglichen, dem Bediener Informationen anzuzeigen und mit dem Prozess selbst über Schnittstellen wie Zeiger, Maus oder Tastatur zu interagieren, die die gewünschten Befehle übertragen können. Diese spezialisierten Systeme werden als SCADA- oder Prozessleitsysteme (PLS) bezeichnet, und obwohl sich die Anwendungen der beiden Systemtypen häufig überschneiden, gibt es einige Unterschiede, die im Folgenden aufgeführt sind (Galloway & Hancke, 2013):

1. Während Prozessleitsysteme prozessgesteuerte Systeme sind, sind SCADA-Systeme ereignisgesteuerte Systeme.
2. Im Gegensatz zu SCADA-Systemen, die in der Regel große geografische Gebiete mit verteilten Standorten umfassen, umfassen PLS-Systeme kleine Bereiche mit Standorten in lokalen, stark vernetzten Produktions- und Fertigungsprozessen.
3. PLS-Systeme eignen sich vor allem für große integrierte Systeme wie Stromerzeugungsanlagen oder chemische Prozesse, während SCADA-Systeme für den Einsatz in verschiedenen autonomen Systemen wie Versorgung und/oder diskrete Fertigung oder Montage geeignet sind.
4. PLS-Systeme sind relativ zuverlässig und erzeugen im Gegensatz zu SCADA-Systemen, die eine geringe Medienzuverlässigkeit und schlechte Datenqualität aufweisen, Daten von guter Qualität.
5. PLS-Systeme bestehen aus leistungsfähiger Hardware für die Rückkopplungssteuerung. Diese unterscheidet sich von der energiesparenden Hardware, die normalerweise für die Verarbeitung binärer Signale in SCADA-Systemen verwendet wird.

### ICNs und Industrie 4.0

Spricht man über die Kommunikation in der Industrie 4.0, ist es schwierig, von allem abzurücken, was mit digitaler Kommunikation über das Internet und/oder dem Internet der Dinge (IoT), genauer dem Industrial Internet of Things (IIoT), zusammenhängt. Nach Wollschlaeger et al. (2017) haben ICNs in den letzten Jahren mindestens drei Entwicklungsstufen durchlaufen:

1. Die Entwicklung begann in den 1980er und frühen 1990er Jahren, als Sensoren, Aktoren und Steuerungen über Feldbussysteme miteinander und mit übergeordneten Ebenen verbunden wurden;
2. Dies änderte sich um das Jahr 2000 mit der Einführung von Ethernet-basierten Netzwerken, die aufgrund ihrer weiten Verbreitung und ihres Ursprungs in der Informationstechnologie (IT) eine kostengünstigere Technologie und eine schnellere Verbreitung boten;
3. Später, um das Jahr 2010 herum, begann der Aufstieg der drahtlosen Netzwerke, die ihren Platz in der industriellen Automatisierung fanden, wenn auch mit gewissen Einschränkungen aufgrund der hohen Anforderungen an die Zuverlässigkeit in diesem Anwendungsbereich.

Für das spätere Aufkommen des Internet der Dinge (IoT) waren diese beiden letzten Phasen wegweisend. In ähnlicher Weise hat die Verbreitung der Mobilkommunikation und der WLAN-Technologien (Wireless Local Area Network) die Kosten und den Aufwand für die Verbindung mobiler Geräte mit dem Internet drastisch reduziert. Damit wurde das Fundament für das Internet der Dinge und die Industrie 4.0 weiter verstärkt. (Aceto et al., 2019).

Die Rolle des Internets in Industrie 4.0 ist an sich schon fundamental. Denn viele Elemente, die an der Umsetzung und Entwicklung der Industrie 4.0 beteiligt sind, nutzen das Internet als Basis. So ist nach Aceto et al. „das gesamte Paradigma der Industrie 4.0 durch und durch von der Infrastruktur des Internets abhängig, so dass es ohne das Internet, wie wir es kennen, so etwas wie die Industrie 4.0 gar nicht geben würde“ (2019, S. 3472). Das Internet fungiert in erster Linie als Bindeglied, das die Kommunikation zwischen verteilten Einheiten, seien es Menschen oder Maschinen, ermöglicht. Außerdem werden Produkte, Objekte und/oder Bediener:innen aufgrund der einfachen Integration durch das Internet „smart“, also intelligent. Diese Intelligenz ist das Ergebnis von Kontextwissen, das durch Echtzeitkommunikation über digitale Netze zur Verfügung gestellt wird, oder von Informationsspeicherung und Rechenleistung, die von kostengünstigen, entfernten Datensammelstellen, wie z. B. über das Internet zugängliche Clouds, bereitgestellt werden (Aceto et al., 2019).

Die International Telecommunication Union (ITU; 2005, S. 2) erklärt, dass nach dem Aufkommen des IoT „die Welt der Informations- und Kommunikationstechnologien (IKT) um eine neue Dimension erweitert wurde: Von der Konnektivität zu jeder Zeit und an jedem Ort für jeden werden wir nun Konnektivität für alles haben*“.* Die Einbeziehung dieser Technologie war jedoch dynamisch, so Aceto et al. (2019). Seit seinen Anfängen hat das Internet der Dinge drei Entwicklungsphasen durchlaufen:

1. Ausgehend von einer Ausrichtung auf den Aufbau einer digitalen Identität für interagierende Geräte und die M2M-Kommunikation (Machine-to-Machine). Insofern hat sich die Ausrichtung der Kommunikation als wesentlicher Schritt in der Entwicklung der Industrie 4.0 von der Interaktion zwischen Menschen bzw. Menschen, die mit Maschinen kommunizieren, hin zu einer ganzheitlichen Interaktion von Maschinen, die mit Maschinen kommunizieren, gewandelt.
2. Dann wurden Standards wie das IP-Protokoll und die Ausrichtung von Anwendungen auf Web-Entwicklung für die M2M-Kommunikation übernommen bzw. angepasst, um die generelle Adressierung und die Realisierung von Schnittstellenstandards zu lösen.
3. Basierend auf Typisierung und semantischer Standardisierung sowie informationsbasierten Kommunikationsnetzen wurde eine inhaltsorientierte Interoperabilität entwickelt. Es wurden auch Anwendungen für den allgegenwärtigen Zugriff auf Ressourcen entwickelt, die Cloud Computing als Ressource nutzen, um ein autonomes und kooperatives Verhalten von vernetzten Objekten zu erreichen.

Es wird allgemein empfohlen, offene, IP-basierte Netzwerke zu verwenden, um die Vorteile des IoT zu maximieren. Dadurch können alle Geräte, Maschinen und Anlagen über ein einziges Netzwerk miteinander verbunden werden, und das entweder kabelgebunden oder drahtlos (AdvanTech, 2017). Dies könnte dazu führen, dass ältere Geräte isoliert werden und/oder keine Verbindung mehr haben. Aus diesem Grund ist die Verwendung von Elementen, welche die Anbindung älterer Geräte an moderne Netzwerksysteme ermöglichen, zur Verlängerung der Lebensdauer vorhandener Geräte und zur Vermeidung unnötiger Anschaffungen von Erweiterungsgeräten oder größerer Aufrüstungen erforderlich. Als industrielles Internet der Dinge wird die spezifische Nutzung des IoT für die Entwicklung des Industrie 4.0-Paradigmas bezeichnet. Es wird im Wesentlichen definiert als eine Reihe von mit speziellen Sensoren ausgestatteten industriellen Maschinen und Anlagen, die es ermöglichen, sie über das Internet mit anderen Geräten zu verbinden, um z. B. Überwachungs- und Analyseaufgaben für die Betriebsführung zu erfüllen (Aceto et al., 2019).

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie vier Unterschiede zwischen industriellen Netzwerken (ICNs) und kommerziellen Netzwerken (CCNs).

* *Der Anwendungsbereich von ICNs ist vielfältig und umfasst sämtliche Produktionsprozesse, während der von CCNs etwas eingeschränkter ist.*
* *Die Hauptfunktion von ICNs ist die Überwachung und Steuerung von physischen Geräten, während CCNs hauptsächlich für die Datenverarbeitung und -übertragung zuständig sind.*
* *Die Architektur der ICNs ist im Allgemeinen breiter angelegt als die der CCNs und erreicht in kleinen Einsatzfeldern drei oder vier Hierarchieebenen.*
* *Die ICNs erfordern eine unterschiedliche Arbeitsgeschwindigkeit für die verschiedenen Hierarchieebenen, während diese Art von Einschränkung in CCNs nicht existiert.*
* *ICNs erfordern, dass die Datenübertragung auf der Feldebene in Echtzeit erfolgt und auch deterministisch ist, was bei CCNs nicht so wichtig ist.*
* *Die Größe der in ICNs verwendeten Datenfelder ist in der Regel sehr klein (einige Bytes), während in CCNs normalerweise Felder in der Größenordnung von Kilobytes oder mehr verwendet werden.*
* *Die Auswirkungen des Auftretens von Fehlern sind in CCNs wesentlich geringer als in ICNs.*
* *Im Gegensatz zu CCNs erfordern aperiodische Übertragungen in ICNs regelmäßig die Bestimmung des Zeitpunkts der Übertragungen und der Reihenfolge der Ereignisse im Netzwerk.*
* *Im Gegensatz zu der sauberen Umgebung in den CCNs sind die Arbeitsbedingungen in den Betriebsumgebungen der ICNs oft lebensfeindlich.*

1. Bitte vervollständigen Sie die folgenden Sätze.

*PLS-Systeme* sind relativ zuverlässig und erzeugen im Gegensatz zu *SCADA-Systemen*, die eine geringe Medienzuverlässigkeit und schlechte Datenqualität aufweisen, Daten von guter Qualität.

*Überwachungsinformationen* sind andere Informationen, die von Sensorgeräten erfasst werden, auf die aber kein *Regelsystem* reagiert. Sie dienen dazu, den *Zustand der Anlagen zu beurteilen*.

## 5.2 HART

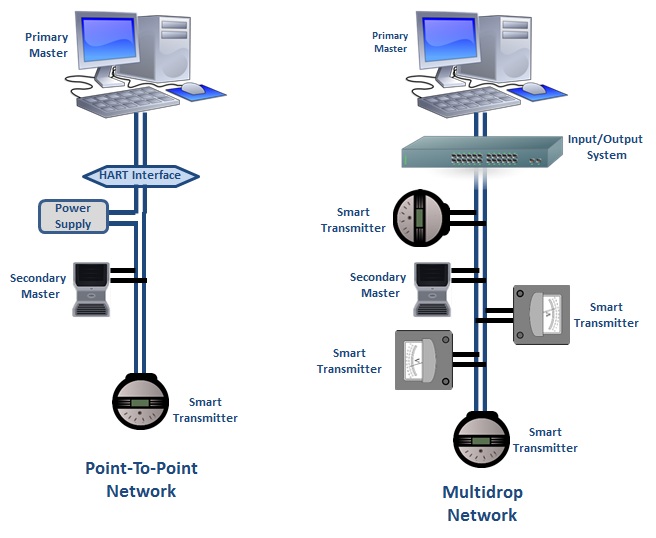
Zum Zeitpunkt der Entwicklung des Highway Addressable Remote Transducer (HART) im Jahr 1985 war es kaum vorstellbar, welche Verbreitung dieses digitale Kommunikationsprotokoll für intelligente Feldgeräte einmal erreichen würde (Howarth, 1994). Die Branchenführer sahen für die Zukunft vollständig digitale Lösungen in diesem Bereich voraus. Sie prognostizierten, dass Feldbusse sehr wichtig sein würden und dass HART nur eine Notlösung sein würde, um die Lebensdauer der vorhandenen 4-20-mA-Geräte zu verlängern. Es vergingen jedoch viele Jahre und der Feldbus war immer noch nicht vollständig entwickelt. HART hingegen verbreitete sich schnell und etablierte sich als hocheffiziente Lösung und nicht nur als Übergangslösung zum Feldbus. Die HART-Technologie hat sich von den ersten Geräten, die sich auf die Verbesserung der Genauigkeit und Zuverlässigkeit konzentrierten, zu universellen Softwareschnittstellen entwickelt, die die Interoperabilität zwischen neuen und vorhandenen Geräten unter Verwendung der Gerätebeschreibungssprache (Device Description Language, DDL) (Howarth, 1994; Zhang, 2010) und multivariablen intelligenten Geräten gewährleisten (Nixon et al., 2015).

### HART-Netzwerke

Die HART-Kommunikation besteht aus zwei Grundelementen: dem Verbindungssystem oder Netzwerk und dem Kommunikationsprotokoll. Zu Beginn waren die HART-Netzwerke, die in der Industrie zur Verfügung standen, vollständig kabelgebunden. Mit der Entwicklung der drahtlosen Kommunikation und der Möglichkeit, diese in der industriellen Automatisierung einzusetzen, entstanden drahtlose HART-Netzwerke (Zhang, 2010). Diese beiden Arten von Netzwerken unterscheiden sich erheblich in Design, Konfiguration, Verbindungsmöglichkeiten und Kommunikationsmechanismen und unterstützen daher unterschiedliche Architekturen und erfordern unterschiedliche Geräte. Dieser Abschnitt beschreibt nur kabelgebundene HART-Netzwerke.

Es gibt zwei Architekturen für kabelgebundene HART-Netzwerke, die Punkt-zu-Punkt- oder analog/digitale Konfiguration und die Multidrop- oder rein digitale Konfiguration (Howarth, 1994; Zhang, 2010; Nixon et al., 2015). Die Punkt-zu-Punkt-Konfiguration überlagert dem analogen 4-20-mA-Signal digitale Daten. Sie besteht aus einem primären Master oder Host, der die Aufgabe der Steuerung oder einer anderen relevanten Anwendung übernimmt, und einem Transmitter oder intelligenten Feldgerät, das über die HART-Schnittstelle angeschlossen ist. Der primäre Master ist in der Regel eine SPS oder ein zentrales computergestütztes Überwachungs- und/oder Steuerungssystem. Nach der Konfiguration kann ein:e Benutzer:in auch über einen sekundären Master, in der Regel ein Handheld-Gerät, kommunizieren. Dieses Gerät wird an Konverterterminals oder andere Zugangsgeräte im Netz angeschlossen, um eine vorübergehende Kommunikation herzustellen, das Gerät neu zu konfigurieren oder bestimmte Informationen vor Ort zu erhalten (Park et al., 2003; Zhang, 2010).

HART-Netzwerkarchitekturen



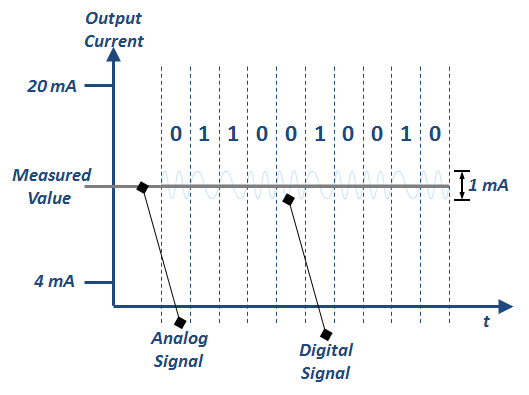
Quelle: Rojas (2022)

Die Multidrop-Konfiguration wiederum verbindet bis zu fünfzehn Transmitter oder intelligente Feldgeräte über zwei Kabel mit einem Eingabe/Ausgabe-Management-System, das ordnungsgemäß an den primären HART-Master angeschlossen ist. In dieser Konfiguration sind die Geräte elektrisch parallel geschaltet. Sie werden bei Bedarf von einer Hilfsquelle versorgt und die Kommunikation erfolgt digital. Dadurch verliert das Analogsignal an Bedeutung und der Stromwert durch jedes Gerät wird auf einen Mindestwert, typischerweise 4 mA, eingestellt (Nixon et al. 2015). Diese Konfiguration ermöglicht auch das Andocken eines sekundären Master-Kommunikators oder eines tragbaren Kommunikators. Theoretisch kann er an jeder beliebigen Stelle angedockt werden, was aber in der Praxis nicht unbedingt der Fall ist (Zhang, 2010). Für die Implementierung eines kabelgebundenen HART-Netzwerks gibt es praktisch keine Einschränkungen. Die Topologie wird im Allgemeinen als ein Bus betrachtet, der nach Belieben Subbusse bilden kann, aber dennoch ein einziges Netzwerk bleibt. Die Kommunikation in HART-Netzwerken erfolgt bidirektional, aber nicht gleichzeitig (Halbduplex) mit einer Übertragungsrate von etwa drei Nachrichten pro Sekunde unter normalen Bedingungen (Howarth, 1994). Die vorstehende Abbildung zeigt schematisch die beiden für HART-Netzwerke verfügbaren Architekturen.

**Funktionsweise des HART-Netzwerks**

Die Kommunikation in HART-Netzwerken findet zwischen zwei kommunikationsfähigen Geräten statt, typischerweise zwischen einem Transmitter oder einem Feldgerät und einem Überwachungs- oder Steuerungssystem. Alle HART-kompatiblen Feldgeräte unterstützen zwei Kommunikationskanäle: die typische Stromschleife und die digitale HART-Kommunikation (Zhang, 2010; Nixon et al., 2015). Diese beiden Kanäle teilen sich die Frequenzbänder, wobei die Stromschleife das Frequenzband von 0 bis 25 Hz belegt, wie dies bei allen 4- bis 20-mA-Geräten der Fall ist, um kontinuierlich einen einzigen Wert der betreffenden Variable zu übertragen. Ein oberes Band zwischen 500 Hz und 10 kHz wird für die digitale Kommunikation verwendet. Das ursprüngliche HART-Kommunikationsprotokoll basierte auf dem Standard Bell 202 (Telefonkommunikation), der das Frequenzumtastungsverfahren (FSK) verwendet. Das digitale FSK-Signal setzt sich aus den Frequenzen 1200 und 2200 Hz zusammen, die das Äquivalent der Bits 1 und 0 symbolisieren. Die Sinuswellen dieser beiden Frequenzen werden dem Analogsignal hinzugefügt, ohne es zu beeinflussen, da der Mittelwert des FSK-Signals gleich Null ist. Die Amplitude des FSK-Signals beträgt etwa 1 mA p-p bei dem eingestellten Ausgangsstrom. Außerdem muss das Analogsignal nicht gestört werden, da die Information durch das binäre Übertragungssignal in etwa drei Aktualisierungen übertragen wird (Nixon et al., 2015). Darüber hinaus ist dieses Signal phasenkontinuierlich, d. h. es gibt keine Unterbrechungen oder Sprünge, wenn sich die Frequenz ändert. Dies wird nur durch eine Änderung der Übertragungssteilheit der Wellenform erreicht (Zhang, 2010). Um eine höhere Geschwindigkeit (9600 Bd) zu erreichen, kann in späteren Versionen die digitale Darstellung durch eine geringfügige Änderung der Phasenumtastung (PSK) modifiziert werden. Diese Funktion wird jedoch kaum genutzt (Nixon et al., 2015). Die folgende Abbildung zeigt einen Analog-Digital-Ausgang eines HART-Geräts.

HART-Signal

  
Quelle: Rojas (2022)

### HART-Kommunikationsprotokoll

Das HART-Protokoll hat sich als Industriestandard für die 4-20-mA-Kommunikation auf der Feldebene durchgesetzt und wurde digital erweitert. Das HART-Kommunikationsprotokoll verwendet ein Master-Slave-Modell, so dass Feldgeräte als Slaves nur antworten, wenn sie von einem Master angesprochen werden (Zhang, 2010). Bei jeder Kommunikation sendet das Master-Gerät zunächst eine Befehlsnachricht, die das entsprechende Slave-Gerät empfängt, verarbeitet und erst dann eine Antwortnachricht senden kann. Sowohl die Befehls- als auch die Antwortnachrichten enthalten HART-Daten, die gemäß den entsprechenden HCF-Spezifikationen (HART Communication Foundation) aufbereitet sind. Das HART-Protokoll ist so konzipiert, dass es zur Übertragung von Informationen verwendet werden kann, die sowohl analoge und digitale Signale als auch nur digitale Signale enthalten. Am häufigsten wird die digitale Master-Slave-Kommunikation in Verbindung mit analogen 4-20-mA-Signalen verwendet. In diesem Modus ist es möglich, zweimal pro Sekunde die digitalen Informationen des Slave-Geräts im Master zu aktualisieren. Da die Analogsignale von vier bis zwanzig Milliampere kontinuierlich sind, ermöglichen sie auch die Übertragung der Steuergröße, ohne den Slave zu verwirren, da bei aktivierter Kommunikation zwischen Master und Slave keine Unterbrechung zulässig ist. Außerdem ermöglicht das HART-Netzwerk, dass ein gewünschtes Slave-Gerät sowohl vom primären als auch vom sekundären Master angesprochen werden kann. Die Kommunikation mit dem sekundären Master kann von nahezu jedem Ort im Netzwerk erfolgen, ohne den primären Master zu stören. In Multidrop-Netzwerken ist die Kommunikation auf den digitalen Master-Slave-Modus beschränkt.

|  |  |
| --- | --- |
| **Schichtaufbau des HART-Protokolls** | |
| **OSI-SCHICHT** | **HART-SCHICHT** |
| Anwendungsschicht | Orientiert an universellen Befehlen. Datentypen und Anwendungsoperationen vordefinieren |
| Darstellungsschicht | Nicht benutzt |
| Sitzungsschicht | Nicht benutzt |
| Transportschicht | Nicht benutzt |
| Vermittlungsschicht | Nicht benutzt |
| Sicherungsschicht | Binären Master-Slave-Modus byteorientiert einstellen. |
| Bitübertragungsschicht | Ermöglicht die gleichzeitige analog-digitale Signalisierung und die Verwendung der normalen 4-20mA-Kupferverkabelung. |

(Rojas, 2022)

Das HART-Protokoll basiert auf dem siebenschichtigen OSI-Referenzmodell. Wie bei den meisten Kommunikationsprotokollen der Feldebene wird auch hier die Enhanced Performance Architecture (EPA) vorgesehen, die auf den Schichten 1, 2 und 7 des Modells basiert (Park et al., 2003; Zhang, 2010). In der Praxis werden die dritte bis sechste Schicht nicht verwendet, da ihre Dienste in der Regel nicht benötigt werden. Bei Bedarf werden sie über die siebte Schicht oder die Anwendungsschicht bereitgestellt. Die Anwendungsschicht hat unter anderem die Aufgabe, die vom Protokoll akzeptierten Datentypen, Befehle, Antworten und Statusmeldungen zu definieren. Darüber hinaus gibt es im HART-Protokoll einige Vereinbarungen, die ebenfalls als Teil der Anwendungsschicht betrachtet werden, z.B. wie der Netzwerkdatenstrom abgeschnitten werden soll. Obwohl es im Allgemeinen unvermeidlich ist, dass die Anwendungsschicht des OSI-Modells eine Befehlszusammenfassung, die Definition von Antwortcodes und die Verwendung gemeinsamer Tabellen (mit Datentypen, deren gemeinsamen Definitionen und normalen Prozessen) umfasst, werden bei der Implementierung aller HART-konformen Geräte universelle Befehle verwendet, die den erforderlichen Mindestinhalt definieren (Zhang, 2010). Die obige Tabelle zeigt die Schichtenstruktur des HART-Protokolls in Bezug auf das OSI-Referenzmodell.

### Fragen zur Selbstkontrolle

1. Bitte geben Sie an, ob die folgenden Aussagen richtig oder falsch sind.

* HART verlängerte die Lebenserwartung von 4-20mA-Instrumenten. *Richtig*
* In der Industrie gibt es nur vollständig kabelgebundene HART-Netzwerke. *Falsch*
* HART verwendet das Band zwischen 500 Hz und 10 kHz für die digitale Kommunikation. *Richtig*
* Das HART-Protokoll sieht die Enhanced Performance Architecture (EPA) vor. *Richtig*

1. Geben Sie an, wann Highway Addressable Remote Transducer (HART) entwickelt wurde.

* *1985*.
* 1981.
* 1979.
* 1983.

## 5.3 PROFIBUS

In Deutschland wurde 1987 ein nationales strategisches Feldbusprojekt gestartet, als die Feldbustechnologien voll entwickelt waren. Das Projekt ist ein Zusammenschluss von 21 Unternehmen und Institutionen, unterstützt durch den Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI) und gefördert durch die öffentliche Hand, insbesondere durch das Bundesministerium für Bildung und Forschung (BMBF) (Zhang, 2010; PROFIBUS Nutzerorganisation (PNO), 2016). Das Hauptziel dieses Projekts war es, den PROFIBUS (PROcess FIeld BUS), einen seriellen Bit-Feldbus, nach einem vereinbarten technischen Konzept zu entwickeln und zu implementieren, um seine Standardisierung für den Einsatz in der Fabrik- und Prozessautomatisierung zu ermöglichen. Das Ergebnis dieses Projekts wurde 1989 zusammen mit der Gründung der PROFIBUS-Nutzerorganisation vorangetrieben (PNO, 2016), die mit dem Ziel der weiteren Standardisierung gegründet wurde. Die erste Spezifikation, das Kommunikationsprotokoll PROFIBUS-FMS (Fieldbus Message Specification), wurde entwickelt, um anspruchsvolle Kommunikationsaufgaben zu erfüllen, was zu einem recht komplexen Produkt führte.

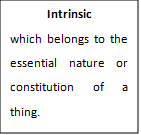
Mit der PROFIBUS-DP-Spezifikation (Dezentrale Peripherie), die insbesondere auf den Informationsaustausch auf der Feldebene zwischen Steuerungen und Feldgeräten ausgerichtet ist, wurde 1993 ein schnelleres und einfacheres Ergebnis erzielt. Mit dieser Neuentwicklung ist es gelungen, sich erfolgreich auf dem Markt der Fabrikautomation zu positionieren. Unterstützt wird dies durch die Effizienz des Kommunikationsprotokolls und eine Vielzahl von Anwendungsprofilen für zahlreiche Geräte (Zhang, 2010; Jecht et al., 2015). Die Entwicklung wurde 1995 erfolgreich fortgesetzt mit der Entwicklung von PROFIBUS-PA (Prozessautomatisierung), einer Low-Speed-Variante von PROFIBUS-DP mit eigensicheren Spezifikationen, um den Anforderungen in diesem Bereich gerecht zu werden. Im gleichen Jahr wurde die Organisation PROFIBUS & PROFINET International (PI) mit mehr als 1.000 Mitgliedern und 25 regionalen PROFIBUS-Vereinigungen (RPA) weltweit gegründet, um die Verbreitung und kontinuierliche Weiterentwicklung dieser Technologien voranzutreiben (Felser & Mitchel, 2011; PROFIBUS Nutzerorganisation (PNO), 2016).

### PROFIBUS-Netzwerke

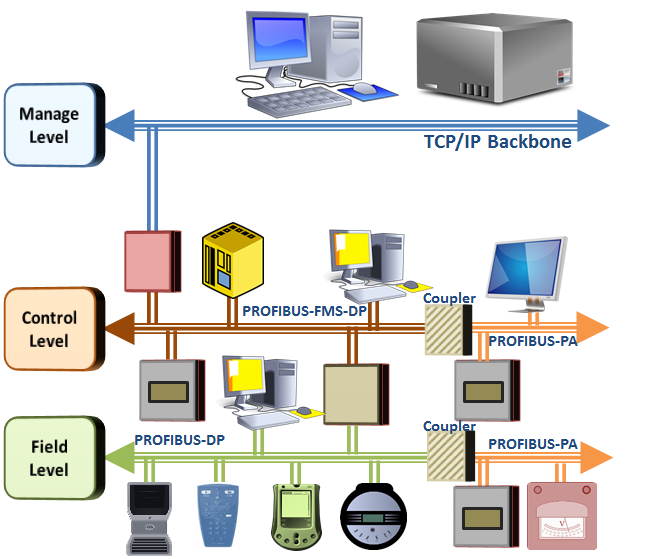
Die drei aktuellen Versionen von PROFIBUS bilden eine Familie von kompatiblen Netzwerken:

PROFIBUS-FMS wurde für die Kommunikation auf Steuerungsebene entwickelt, hauptsächlich zwischen Computern und SPS-Systemen, die in der Regel komplexe Informationen untereinander austauschen, und stellte ursprünglich eine unflexible Technologie und ein Protokoll dar, das für weniger komplexe Nachrichten und/oder für die Kommunikation in großen und komplexen Netzwerken völlig ungeeignet war (Zhang, 2010). Dies hatte zur Folge, dass diese Probleme in den neueren Versionen gelöst wurden, so dass sie auch heute noch verwendet werden können, auch wenn sich die meisten Benutzer:innen für die neueren Lösungen entscheiden, weil sie diese für besser geeignet halten.

PROFIBUS-DP, speziell entwickelt und optimiert für kostengünstige Hochgeschwindigkeitsverbindungen in der Feldebene, ermöglicht die Kommunikation zwischen SPS-Systemen oder Computern auf der Steuerungsebene und dezentralen Feldgeräten auf der Feldebene. PROFIBUS-DP kommuniziert ausschließlich über zyklischen Datentransport, d. h. jedes Feldgerät tauscht seine Ein- und Ausgangswerte mit der Steuerung aus, und zwar zu Zeitpunkten, die durch jeden Zyklus bestimmt werden. In automatisierten Prozess- und Fertigungssystemen werden Anzeigegeräte für Bedien- und Überwachungsaufgaben benötigt. Dabei muss die Anzeige von Gerätedaten zu Zeitpunkten gelesen oder geschrieben werden, die unabhängig vom Steuerungszyklus sind (Felser & Mitchell, 2011). Diese Aufgaben waren mit der ursprünglichen PROFIBUS-DP Spezifikation nicht kompatibel, so dass 1997 Erweiterungen definiert wurden, um die erforderlichen Funktionen bereitzustellen. Diese Erweiterungen sind optional und mit allen Versionen des PROFIBUS-DP-Protokolls kompatibel. Als erste Erweiterung in diesem Sinne gilt PROFIBUS-DPV0, das für die zyklischen Kommunikationsdienste zuständig ist. Darüber hinaus wurden zwei zusätzliche Erweiterungen entwickelt, PROFIBUS-DPV1 und PROFIBUS-DPV2. Diese bieten azyklische Dienste vor allem für Überwachungs- und Alarmmeldungen sowie weitere Aufgaben zur Parametrierung, Diagnose und Steuerung von Feldgeräten (Zhang, 2010).

PROFIBUS-PA wurde für die Prozessautomatisierung entwickelt. Es handelt sich im Wesentlichen um ein PROFIBUS-DP-Netzwerk, das den Prozess der Messdatenübertragung standardisiert und dabei **intrinsische** Sicherheitsspezifikationen verwendet, die es robust für den Einsatz in explosionsgefährdeten Umgebungen sowohl auf der Feld- als auch auf der Steuerungsebene machen (Zhang, 2010). Darüber hinaus umfasst es auch Funktionen wie die Versorgung von Feldgeräten über Buskabel, Interoperabilität und zuverlässige Datenübertragung – grundlegende Anforderungen in der Prozessautomatisierung. Eine PROFIBUS-Netzwerkkonfiguration, in der die Verbindung der drei Versionen in hierarchischer Weise dargestellt ist, ist in der folgenden Abbildung gezeigt.

PROFIBUS-Netzwerk

  
Quelle: Rojas (2022)

**Funktionsweise von PROFIBUS-Netzwerken**

Die Kommunikation über PROFIBUS-Netzwerke erfolgt im Wesentlichen über drei Technologien: RS-485, MBP und Lichtwellenleiter.

RS-485 oder EAI-485, empfohlener Standard der Electronic Industries Alliance (EIA), ist eine Technologie, die in der Fertigungsindustrie und teilweise in der Prozessindustrie eingesetzt wird. Sie ist kosteneffektiv und benutzerfreundlich für Aufgaben, die eine hohe Übertragungsgeschwindigkeit in einer ungefährlichen Umgebung (die keine Eigensicherheit voraussetzt) erfordern (Felser & Mitchel, 2011; PROFIBUS Nutzerorganisation (PNO), 2016). Als Basis dient hier ein abgeschirmtes Kabel mit zwei verdrillten Kupferleitern. Ihre Struktur (BUS) ermöglicht das nicht-reaktive An- und Abkoppeln von Stationen, so dass diese schrittweise in Betrieb genommen werden können, ohne andere Stationen im System zu beeinträchtigen. Wenn das System bereits in Betrieb ist, können spätere Erweiterungen (innerhalb bestimmter festgelegter Grenzen) ohne Beeinträchtigung der bestehenden Stationen vorgenommen werden. Pro Segment können bis zu 32 Stationen (Master oder Slave) angeschlossen werden. Obwohl der Übertragungsbereich groß ist (zwischen 9,6 kb/s und 12 Mb/s), muss vor der Inbetriebnahme des Systems eine einheitliche Geschwindigkeit für alle an den Bus angeschlossenen Geräte gewählt werden (Felser & Mitchel, 2011). Darüber hinaus ist der Einsatz der RS485-Schnittstelle mit ihren hohen Übertragungsraten auch im eigensicheren Bereich (RS485-IS) möglich (PROFIBUS Nutzerorganisation (PNO), 2016). Dabei müssen bestimmte Werte eingehalten werden, die Strom- und Spannungspegel definieren, die sowohl den individuellen Betrieb jedes Knotens als auch den globalen Betrieb des Systems gewährleisten.

MBP (Manchester Coded, Bus Powered) ist eine Datenübertragungstechnik, bei der gleichzeitig die Datenkommunikation mittels Manchester (M)-Codierung und die Stromversorgung (BP) der angeschlossenen Feldgeräte über ein einziges Kabel (BUS) realisiert wird (Felser & Mitchel, 2011; PROFIBUS Nutzerorganisation (PNO), 2016). Dies ermöglicht eine einfache und sichere Installation und reduziert den Verdrahtungsaufwand erheblich. Gleichzeitig werden die Vorteile der digitalen Übertragung zum und vom Feldgerät genutzt. Auch hier kommt die Zweidrahttechnik mit einer definierten asynchronen Übertragungsgeschwindigkeit von 31,25 kb/s zum Einsatz (Felser & Mitchel, 2011). MBP wurde speziell für die Anforderungen der Prozessautomatisierung in der chemischen und petrochemischen Industrie entwickelt. Die eigensichere Ausführung (MBP-IS) ist für den Einsatz in explosionsgefährdeten Bereichen einfach erweiterbar und begrenzt die Leistung der Busversorgung, um den Explosionsschutz zu gewährleisten (PROFIBUS Nutzerorganisation (PNO), 2016). Die MBP-IS-Technologie ist in der Regel auf bestimmte Anlagensegmente in explosionsgefährdeten Bereichen beschränkt. Diese werden dann über Segmentkoppler oder Links mit dem RS485-Segment in der Warte verbunden (Felser & Mitchel, 2011).

Die optische Übertragungstechnik wiederum wird eingesetzt, wenn es darum geht, Elemente über große Entfernungen oder in Umgebungen mit starken elektromagnetischen Störungen miteinander zu verbinden, also bei Aufgaben, die mit der Kabelübertragungstechnik nicht gelöst werden können. In diesen Fällen werden Lichtwellenleiter in verschiedenen Netzwerktopologien verwendet, die den PROFIBUS-Richtlinien für die Übertragung über dieses Medium folgen (Felser & Mitchel, 2011; PROFIBUS Nutzerorganisation (PNO), 2016). Bei der Festlegung der Spezifikationen ist darauf geachtet worden, dass die Integration vorhandener PROFIBUS-Geräte in ein LWL-Netz ohne nachteilige Auswirkungen möglich ist. Dies gewährleistet die Kompatibilität mit bestehenden PROFIBUS-Installationen. Die Verwendung des elektro-optischen Konverters ermöglicht eine einfache Implementierung von LWL-Netzwerken, indem er auf der einen Seite an ein LWL-Kabel angeschlossen wird und auf der anderen Seite jedes Feldgerät über eine RS-485-Schnittstelle angeschlossen wird (Jecht et al., 2015). Diese Konfiguration ermöglicht die Auswahl der Übertragungsart, RS-485 oder Lichtwellenleiter, je nach den Betriebsbedingungen der Anlage. Der interessierte Leser wird auf die Literatur zu weiteren Details dieser Technologien sowie anderer Übertragungstechnologien in explosionsgefährdeten Bereichen oder über drahtlose Medien verwiesen.

### PROFIBUS-Kommunikationsprotokoll

Wie die meisten spezialisierten Kommunikationsprotokolle der Feldebene bietet auch das PROFIBUS-Protokoll die Enhanced Performance Architecture (EPA). Diese basiert auf den Schichten 1, 2 und 7 des siebenschichtigen OSI-Referenzmodells (Mackay et al., 2004; PROFIBUS Nutzerorganisation (PNO), 2016). PROFIBUS-FMS und PROFIBUS-DP verwenden in der ersten Schicht bzw. Bitübertragungsschicht die gleichen Übertragungstechnologien, d.h. RS-485, MBP oder Lichtwellenleiter, während PROFIBUS-PA seine Variante gemäß der Norm IEC 61158-2 verwendet, um die Anforderungen an die Eigensicherheit zu erfüllen. In der zweiten Schicht bzw. Sicherungsschicht verwenden alle drei Versionen von PROFIBUS (FMS, DP und PA) das gleiche Master-Slave-Verfahren zusammen mit dem Token-Prinzip. In der Praxis werden die dritte bis sechste Schicht nicht verwendet, da ihre Dienste in der Regel nicht benötigt werden. Bei Bedarf werden sie über die siebte Schicht oder die Anwendungsschicht bereitgestellt. In der siebten Schicht bzw. Anwendungsschicht (Fieldbus Message Specification für PROFIBUS-FMS und Decentralized Periphery Specification für PROFIBUS-DP und PROFIBUS-PA) werden die Anwendungs- und Kommunikationsverbindungen implementiert. Darüber hinaus wird auf die Anwendungsschicht eine zusätzliche Schicht (eine vierte für das EPA-Modell oder eine achte für das OSI-Modell), die so genannte Benutzerschicht, aufgesetzt. In dieser Schicht werden die Profile der verwendeten Geräte und Anwendungsbereiche in Abhängigkeit von der verwendeten PROFIBUS-Version beschrieben. Die folgende Tabelle zeigt die Schichtenstruktur des PROFIBUS-Protokolls bezogen auf das OSI-Referenzmodell.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Schichtaufbau des PROFIBUS-Protokolls** | | | | |
| **Versionen** | | **FMS** | **DP** | **PA** |
| **8** | Benutzer | FMS-Profile | DP-Profile | PA-Profile |
| DP-Erweiterungen  (DP-V0, DP-V1, DP-V2) | |
| **7** | Anwendung | Fieldbus Message  Specification FMS | DP Grundfunktionen | |
| **6** | Darstellung | Nicht genutzt | | |
| **5** | Sitzung |
| **4** | Transport |
| **3** | Vermittlung |
| **2** | Sicherung | Fieldbus Data Link (FDL): Master-Slave-Verfahren, Token-Prinzip | | IEC-Schnittstelle |
| **1** | Bitübertragung | RS -485/MBP/LWL | | IEC 1158-2 |
| **OSI-Modell-Schicht** | | **Implementierung des OSI-Modells auf PROFIBUS** | | |

Quelle: Rojas (2022)

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie die drei Arten von PROFIBUS-Netzwerken.

* *Die auf Datenerfassungssysteme ausgerichtete Version FMS (Fieldbus Message Specification).*
* *Die Version PROFIBUS DP (Decentralized Periphery) wird eingesetzt, wenn eine flexible Kommunikation erforderlich ist.*
* *Die Version PROFIBUS PA (Process Automation) erfüllt die Anforderungen der Prozessindustrie für den Einsatz in eigensicheren und nicht eigensicheren Bereichen.*

1. Bitte markieren Sie die richtige(n) Aussage(n). Die Kommunikation über PROFIBUS-Netzwerke erfolgt im Wesentlichen über drei Technologien:

* RS-232.
* *MBP*.
* Funk.
* *RS-485*.
* FSK.
* Lichtwellenleiter.

## 5.4 Drahtlose Kommunikation

Heutzutage sind drahtlose Netzwerke in Mode und überall zu finden. Je nach Anwendungsbereich und Reichweite ihres Signals können diese Netzwerke in vier spezifische Gruppen eingeteilt werden (Albero-Albero & Sempere-Payá, 2011; Sharma & Dhir, 2014):

* Wireless Personal Area Networks (WPAN) mit einer Reichweite von bis zu 10 m;
* Wireless Local Area Networks (WLAN) mit einer Reichweite von bis zu 100 m;
* Wireless Metropolitan Area Networks (WMAN) mit einer Reichweite von bis zu 50 km und
* Wireless Wide Area Networks (WWAN), die mehr als 50 km abdecken.

Wie bei kabelgebundenen Netzwerken gibt es jedoch auch im industriellen Umfeld eine Reihe von Einschränkungen, die von herkömmlichen kommerziellen Netzwerken und ihren Kommunikationsprotokollen nicht erfüllt werden können. Daher entstehen industrielle drahtlose Sensornetzwerke (Industrial Wireless Sensor Networks, IWSN) als spezialisierte drahtlose Netzwerke, die nicht nur Überwachungs- und Steuerungsaufgaben im industriellen Bereich erleichtern, sondern auch besondere Eigenschaften wie Selbstorganisation, Flexibilität, rasche Bereitstellung und geringe Kosten bieten (Gungor & Hancke, 2011).

### IWS-Netzwerke

Viele Forscherinnen und Forscher haben sich mit dem Entwurf und der Implementierung von IWSNs beschäftigt, bei denen die Implementierungsumgebung und die technischen Herausforderungen oft sehr unterschiedlich sind, z. B. in rauen Industrieumgebungen. Daher ist es wichtig, den Anwendungsbereich zu definieren (Gungor & Hancke, 2011). Im Folgenden werden einige Bereiche beschrieben, in denen die Entwicklung von IWSNs von Bedeutung war:

1. Gebäudeautomation mit dem Ziel, den Energieverbrauch in Gebäuden durch automatisierte Mechanismen zu senken, die Kosten zu reduzieren und gleichzeitig die gesetzlichen Vorschriften einzuhalten und den Komfort zu erhöhen.
2. Automatisierung der öffentlichen Versorgung mit dem Ziel, eine zuverlässige, kosteneffiziente und zeitnahe Überwachung zu erhalten, die es ermöglicht, die notwendigen Maßnahmen zu ergreifen, um die Erzeugung, Verteilung und Versorgung mit Strom und/oder Trinkwasser optimal zu gewährleisten.
3. Automatisierte Zählerfernauslesung, bei der die Zählerstände von Versorgungszählern (Strom, Wasser, Gas) aus der Ferne abgelesen und drahtlos übertragen werden, um den Verbrauch zu ermitteln und die entsprechenden Rechnungen zu erstellen.
4. Fabrikautomation mit dem Ziel, die Flexibilität und Dynamik der Fertigungsprozesse zu erhalten und gleichzeitig die hohen Anforderungen an Zuverlässigkeit, Platzbedarf und Echtzeit zu erfüllen.
5. Automatisierung industrieller Prozesse mit dem Ziel, kritische Prozessvariablen und -parameter in Echtzeit zu überwachen, nicht nur um die Kontrolle zu gewährleisten, sondern auch um eine vorbeugende Wartung oder einen rechtzeitigen Austausch der Anlagen zu ermöglichen.
6. Bestandsmanagement mit dem Ziel, Informationen über Vermögenswerte und Bestände in Echtzeit zu erhalten und Einkaufsanforderungen sowie die Überwachung der Lieferkette zu rationalisieren.

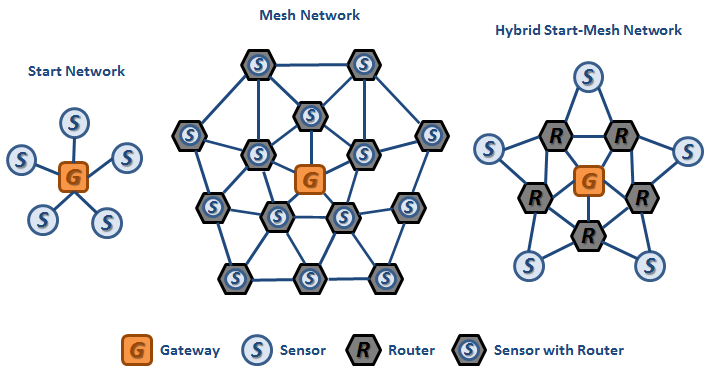
**Funktionsweise von IWSN-Netzwerken**

Im Hinblick auf die physische Infrastruktur ist zu bedenken, dass IWSN-Netzwerke Teil eines gemeinsamen Hybridszenarios sein sollten, in dem drahtlose Verbindungen zu bereits verkabelten Geräten hinzugefügt werden (Lennvall et al., 2015). Im Allgemeinen werden in IWSN-Netzwerken drei Arten von Topologien verwendet: Stern, Mesh und Stern-Mesh-Hybrid:

Die Sterntopologie ist in IWSNs weit verbreitet. Das Gateway ist der Knotenpunkt des Netzwerks, und jeder Endpunkt oder drahtlose Sensor tauscht Daten direkt mit ihm aus (Lennvall et al., 2015). Von diesem Gateway aus können Daten über andere Gateways oder Switches kabelgebunden oder drahtlos an andere Systeme gesendet werden. Diese Netzwerke bieten zwar die höchste Datenabtastrate und den geringsten Stromverbrauch, sind jedoch auf eine direkte Datenübertragungsreichweite von 30 bis 100 m beschränkt (PEPPERL+FUCHS, 2012).

In der Mesh-Netzwerktopologie verhält sich das Netzwerk seinerseits wie ein Multi-Hop-System, in dem alle drahtlosen Sensoren als Router fungieren und für die Weiterleitung von Informationen verantwortlich sind, die sie von anderen Sensoren oder vom Gateway erhalten und die nicht an sie selbst oder andere Sensoren in ihrer Reichweite adressiert sind. Netzwerke mit automatischer Konfiguration verwenden die Position des Sensors und des Gateways, um mittels Routinen die beste Route für die zwischen ihnen zu übertragenden Daten zu bestimmen (PEPPERL+FUCHS, 2012). Diese Topologie ermöglicht Selbstheilung und Redundanz. Sie sind daher in der Regel selbstkonfigurierend und fehlertolerant. Darüber hinaus ermitteln sie die optimale Route in Bezug auf Entfernung und Zeit vom jeweiligen Sensor zum Gateway. Die Mesh-Topologie mit Multi-Hop-Technik unterstützt eine wesentlich größere Reichweite als die Sterntopologie, verbraucht aber aufgrund des höheren Taktverhältnisses wesentlich mehr Energie. Dies schließt die Arbeit der Sensorknoten ein, die ständig auf Nachrichten oder Routenänderungen über die Verbindungen warten (PEPPERL+FUCHS, 2012). Die folgende Abbildung zeigt die drei typischen Topologien von IWSNs.

Typische IWSN-Topologien

  
Quelle: Rojas (2022)

Die hybride Stern-Mesh-Topologie schließlich kombiniert die beiden vorherigen Topologien, um die Vorteile beider zu vereinen: die Geschwindigkeit, den geringen Energieverbrauch und die Einfachheit der Sterntopologie und die Selbstheilungsfähigkeit, Redundanz und Reichweite der Mesh-Topologie (PEPPERL+FUCHS, 2012). Diese Topologie besteht aus Router-Geräten, die regelmäßig über das Stromnetz mit Strom versorgt werden. Sie sind direkt mit dem Gateway verbunden. Die Sensoren ihrerseits kommunizieren mit den Routern über eine Punkt-zu-Punkt-Verbindung (Lennvall et al., 2015).

### Kommunikationsprotokolle für IWSNs

Für die Kommunikationsprotokolle und -standards von drahtlosen Netzwerken wird der Stack verwendet, der auf einer vereinfachten Version des siebenschichtigen OSI-Referenzmodells (Open Systems Interconnection) basiert, das wie bei den flexiblen kabelgebundenen Netzwerken aus vier Schichten besteht, nämlich: der Bitübertragungsschicht (PHY), der MAC-Schicht (Medium Access Control), der Vermittlungsschicht und der Anwendungsschicht (Petersen & Carlsen, 2011). Die IEEE-Standards für WPAN (IEEE 802.15.4 und 802.15.4e) enthalten Einzelheiten zu den PHY- und MAC-Schichten, die als Grundlage für die Entwicklung der wichtigsten Kommunikationsprotokolle für IWSNs (ZigBee, WirelessHART, ISA100.11a, WIA -PA und 6LoWPAN) dienten (Petersen & Carlsen, 2015; Wang & Jiang, 2016; Raza et al., 2017). Hier werden nur die beiden am häufigsten verwendeten Protokolle für die Implementierung von IWSN-Netzwerken kurz beschrieben: WirelessHART, das erste Protokoll, das von der International Electrotechnical Commission (IEC) als Standard für die drahtlose Kommunikation in der Prozessautomatisierung genehmigt wurde, und ISA100.11a, weil es sein engster Konkurrent ist und weil beide speziell für die drahtlose Messwerterfassung entwickelt wurden.

Es ist zu beachten, dass sich WirelessHART und ISA100.11a generell in ihren Netzwerktopologien unterscheiden, da ein wesentlicher Unterschied auf Feldgeräteebene besteht. Aus diesem Grund muss es sich bei der Netzwerktopologie für WirelessHART um eine Mesh-Topologie handeln: Alle Feldgeräte müssen Router sein, da Datenpakete von anderen Geräten durch das gesamte Netzwerk geleitet werden müssen. ISA100.11a hingegen kann jede der drei Topologien verwenden, da in den Feldgeräten die Routerfunktion von der Sensor- und/oder Aktorfunktion getrennt ist und sie daher als Elemente mit oder ohne Routing-Fähigkeit konfiguriert werden können (Petersen & Carlsen, 2015).

Die Stack-Architektur der beiden Protokolle ist recht ähnlich. Auf der Bitübertragungsschicht implementieren beide das PHY der Spezifikation IEEE 802.15.4, wobei die Betriebsfrequenz auf das 2,4 GHz-Band beschränkt ist (Petersen & Carlsen, 2015). Es gibt jedoch einen Unterschied bei der Verwendung von Kanal 26: Während er nach ISA100.11a ein optionaler Kanal ist, ist er bei WirelessHART nicht enthalten, da seine Verwendung in einigen Ländern nicht legal ist. Auf der Sicherungsschicht (DLL) verwenden beide eine Kombination aus Zeitmultiplex-Vielfachzugriff (TDMA) und Frequenzsprungverfahren für den MAC. WirelessHART teilt jedoch die DLL in eine logische Verbindungssteuerungsschicht und eine MAC-Schicht auf, so dass nur die Kommunikation zwischen benachbarten Geräten (ein Hop entfernt) möglich ist. Die Verantwortung für die Kommunikation mit anderen Geräten liegt auf der Vermittlungsschicht. ISA100.11a hingegen unterteilt die DLL in eine Top-Level-DLL, eine MAC-Erweiterung und eine MAC-Subschicht, die das Mesh-Routing innerhalb eines Data-Link-(DL)-Subnetzes durchführt. Dies unterscheidet sich stark vom WirelessHART Ansatz und widerspricht völlig der Definition von DLLs im OSI-Modell (Wang & Jiang, 2016). In der Vermittlungsschicht findet der Informationsaustausch zwischen dem ursprünglichen kabelgebundenen HART-Netzwerk (Token-Passing) und dem WirelessHART-Netzwerk (TDMA) statt. Die Vermittlungsschicht in WirelessHART ist somit für das Routing der Pakete von der Quelle zum Ziel verantwortlich (Petersen & Carlsen, 2015). Darüber hinaus arbeiten alle Geräte in WirelessHART mit Routing-Tabellen, die vom Netzwerkadministrator zugewiesen werden, und unterstützen grafisches und Source-Routing. Andererseits unterstützt die Vermittlungsschicht in ISA100.11a IPv6-Datenverkehr und wird für das Routing auf der Backbone-Ebene verwendet. Sie ist auch zuständig für die Festlegung der entsprechenden Adressinformationen für Datennachrichten, entweder für Backbone-Netzwerke und Anwendungsendpunkte (128-Bit-Adressen) oder für DataLink-Subnetze (16-Bit-Adressen) ( Raza et al., 2017).

Was die Transportschicht betrifft, so unterstützen beide Protokolle unbestätigte Transaktionen zwischen Geräten, aber ISA100.11a unterstützt keine bestätigten Transaktionen. Dies erlaubt der Endanwendung in WirelessHART zu entscheiden, ob eine Quittierung erfolgen soll, wenn End-to-End-Pakete gesendet werden. Die ISA100.11a-Transportschicht ist ihrerseits eine Erweiterung des verbindungslosen Benutzerdatagramm-Protokolls, die die vom 6LoWPAN-Protokoll definierte Kompression als Option anbietet (Petersen & Carlsen, 2015). Schließlich ist die Kommunikation zwischen Geräten auf der Anwendungsschicht in WirelessHART befehlsorientiert. Sie übernimmt weitgehend die Befehle, Antworten, Datentypen und Statusmeldungen, die vom ursprünglichen HART-Standard unterstützt werden, und fügt einige für drahtlose Anwendungen typische Befehle hinzu. Die Anwendungsschicht in ISA100.11a ist objektorientiert. Sie unterstützt die Hardware-I/O-Verarbeitung, einfaches und intelligentes Protokoll-Tunneling und die Ausführung von Berechnungsfunktionen (Wang & Jiang, 2016). Die folgende Tabelle spezifiziert die Stack-Strukturen der WirelessHART- und ISA100.11a-Protokolle in Bezug auf das OSI-Referenzmodell.

|  |  |  |
| --- | --- | --- |
| **Stack-Strukturen von WirelessHART und ISA100.11a** | | |
| **OSI-Modell** | **WirelessHART** | **ISA100.11a** |
| Anwendungsschicht | Anwendungsschicht | Obere Anwendungsschicht |
| Anwendungssubschicht |
| Darstellungsschicht | Nicht definiert | Nicht definiert |
| Sitzungsschicht |
| Transportschicht | Transportschicht | Transportschicht |
| Vermittlungsschicht | Vermittlungsschichtdienst | Vermittlungsschicht |
| Vermittlungsschicht |
| Sicherungsschicht | Logische Verbindungssteuerung | Obere Sicherungsschicht |
| MAC-Erweiterung |
| MAC-Subschicht | MAC-Subschicht |
| Bitübertragungsschicht | Bitübertragungsschicht | Bitübertragungsschicht |

Quelle: Rojas (2022)

### Fragen zur Selbstkontrolle

1. Bitte geben Sie an, ob die folgenden Aussagen richtig oder falsch sind.

* Wireless Local Area Networks (WLAN) haben eine Reichweite von bis zu 500 m. *Falsch*
* Ziel der automatischen Zählerablesung ist die Vor-Ort-Ablesung von Zählern für öffentliche Versorgungsleistungen (Strom, Wasser oder Gas). *Falsch*
* Wireless Wide Area Networks (WWAN) haben eine Reichweite von mehr als 50 km abdecken. *Richtig*
* Ziel der Gebäudeautomation ist es, den Energieverbrauch in den Einrichtungen durch automatisierte Mechanismen zu senken. *Richtig*

1. Bitte vervollständigen Sie die folgenden Sätze.

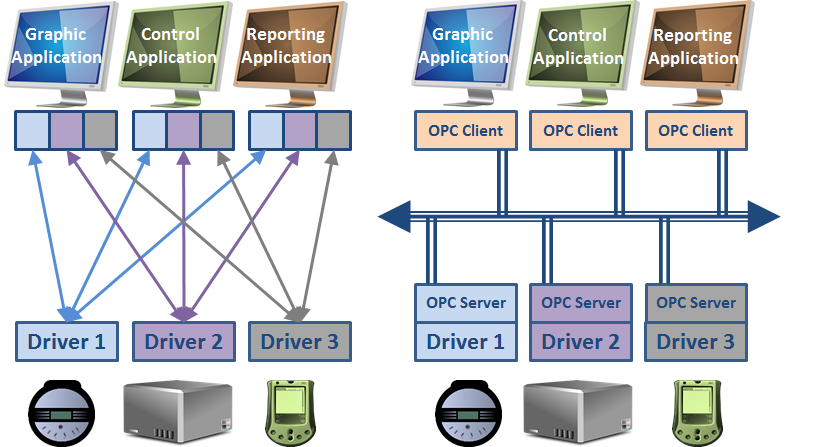
* *Die Sterntopologie* ist in IWSNs weit verbreitet, wobei *das Gateway* der Netzwerkknoten ist, mit dem jeder *Endpunkt oder drahtlose Sensor* direkt Daten austauscht.
* WirelessHART und ISA100.11a *unterscheiden sich generell* in ihren Netzwerktopologien, da ein *wesentlicher Unterschied* auf *Feldgeräteebene* besteht.

## 5.5 OPC

Fabriken und andere Produktionsprozesse sind seit langem in hierarchischen Strukturen organisiert, wie sie in der Automatisierungspyramide dargestellt sind (Hollender, 2010). Entsprechend dieser Struktur werden verschiedene Computeranwendungen oder -werkzeuge auf verschiedenen Ebenen und auf verschiedenen Computergeräten eingesetzt: Von SPS-Steuerungsanwendungen bis hin zu fortgeschrittenen Steuerungen in PLS- oder SCADA-Systemen und in konventionellen Computern; sowie ERP- und MES-Systeme auf höheren Ebenen für die administrative Verwaltung und die mittelfristige Steuerung der Produktion, um nur einige der Aufgaben zu nennen. Alle diese Anwendungen oder Tools mussten auf Daten von einem externen Gerät oder System zugreifen, was die Verwendung spezifischer Protokolle und Treiber für jede einzelne Anwendung erforderte. Dies bedeutete einen hohen Zeitaufwand für die individuelle Entwicklung, die sehr teuer und fehleranfällig war (Kastner et al., 2015). Die Notwendigkeit eines standardisierten Datenaustauschs zwischen diesen Anwendungen hat in den 1990er Jahren verschiedene Automatisierungsunternehmen (Spezialisten für HMI- und SCADA-Software) und Microsoft zur Entwicklung eines Standards zusammengebracht. Im Jahr 1996 legte diese Arbeitsgruppe die Spezifikation „Object-Linking and Embedding for Process Control“ oder OLE for Process Control (OPC-Spezifikation) vor, die auf der Windows OLE-Technologie von Microsoft als einheitliche Methode für den Netzwerkzugriff basiert. Später wurden sie in der OPC Foundation zusammengeführt, um die Unterstützung und Weiterentwicklung dieses Werkzeugs fortzusetzen (Hollender, 2010; Kastner et al., 2015).

Die OPC-Spezifikation stellt Dienste zur Verfügung, um Steuerungsdaten in Automatisierungssystemen zu überwachen, zu lesen und zu schreiben. Dieses Werkzeug nutzt die Client-Server-Architektur. Das bedeutet, dass jede Anwendung, die als OPC-Client konfiguriert ist, sofort und effektiv mit allen Geräten und Systemen kommunizieren kann, die einen OPC-Server zur Verfügung stellen (Hollender, 2010). OPC-Clients und -Server können auf jedem beliebigen Rechner laufen und sich sogar denselben Rechner teilen, so dass keine speziellen OPC-Anwendungsrechner erforderlich sind. Die folgende Abbildung zeigt, wie Anwendungen mit verschiedenen Geräten ohne OPC und mit OPC kommunizieren.

Anwendungen und Gerätekommunikation ohne und mit OPC

  
Quelle: Rojas (2022)

Im Anschluss an die erste Version des OPC-Standards wurden von der OPC Foundation weitere Spezifikationen definiert, so dass der ursprüngliche OPC-Standard heute als OPC Data Access (OPC DA) bezeichnet wird (Kastner et al., 2015). Nach dem gleichen Konzept wurden weitere Standards eingeführt: OPC A&E für die Behandlung von Alarmen und Ereignissen, OPC HDA für den Zugriff auf historische Zeitreihen, OPC Batch, das die Besonderheiten von Batch-Prozessen berücksichtigt, und OPC Security, das verschiedene Ebenen und Richtlinien für die Cybersicherheit bietet. Ergänzt wurde diese Liste durch OPC DX für den direkten Datenaustausch zwischen Servern und OPC DA-XML, um im Gegensatz zum ursprünglichen Binärformat auf Daten im XML-Textformat zuzugreifen. Nicht alle diese Spezifikationen hatten die gleiche Wirkung. Neben OPC DA sind OPC A&E und OPC HDA die herausragendsten. Da alle diese Spezifikationen auf der Basis von Microsofts OLE/COM und DICOM entwickelt wurden, sind diese Standards eigentlich keine, da sie nur auf dem Microsoft Windows-Betriebssystem laufen. Aus diesem Grund hat die OPC Foundation zwischen 2003 und 2008 eine Version von OPC entwickelt, die OPC Unified Architecture (OPC UA) genannt wird, und deren Hauptziel es ist, sich von der Microsoft COM/DCOM-Technologie unabhängig zu machen und auf die Technologie der modernen Webservices umzusteigen (Mahnke, 2010; Dang & Aubin, 2011). Um das Akronym OPC beizubehalten, wurde der Standard von „OLE for Process Control“ in „Open Platform Communications“ umbenannt und seine in der Automatisierungstechnik am weitesten verbreiteten Varianten (OPC DA, OPC A&E und PC HDA) als klassisches OPC klassifiziert. Die OPC-UA Spezifikation versucht die volle Funktionalität von klassischem OPC beizubehalten. Da OPC-UA unabhängig von der Windows-Plattform ist, wird es auch in Szenarien eingesetzt, in denen klassisches OPC nicht verwendet werden kann. Aufgrund der breiten Installationsbasis von klassischem OPC in der Industrie und dem wesentlich leistungsfähigeren, aber auch komplexeren OPC UA hat sich jedoch eine Koexistenz entwickelt. OPC UA hat sich aufgrund seiner Fähigkeit, Interoperabilität zu unterstützen, bis zu seiner Konsolidierung im Jahr 2010 durchgesetzt und unterstützt Industrie 4.0 und IoT (Yadav & Paul, 2021). Die Komponenten von OPC Classic und OPC UA werden im Folgenden kurz beschrieben.

### OPC Data Access – Spezifikation

Die OPC-DA-Spezifikation ist die erste und am weitesten verbreitete Entwicklung der OPC-Familie. Sie bietet über eine Reihe von Standardschnittstellen grundlegende Funktionen für das Lesen und Schreiben von Daten (in Echtzeit) von und zu verschiedenen High-Level-Geräten, die über ein Netzwerk verteilt sind. Ein OPC-DA-Server enthält die E/A-Punkte als Tags oder OPC-Elemente, die in flachen oder strukturierten Listen organisiert sind, um den Clients ihre Daten in einem Drei-Tupel-Format zur Verfügung zu stellen, das den tatsächlich empfangenen Wert, seinen Zeitstempel und ein Qualitäts-Flag enthält. Diese Daten werden aus physischen Geräten gewonnen oder aus bereits gewonnenen Daten generiert. Die OPC-Clients ihrerseits können den Server untersuchen und feststellen, welche Elemente verfügbar sind, um diese abzurufen oder gegebenenfalls neu zu schreiben. Da die Grundidee von OPC Data Access die Bereitstellung von Datenerfassungsschnittstellen zur Unterstützung der hierarchischen Struktur (Automatisierungspyramide) ist, kann ein Server einer Ebene ein untergeordneter Client oder umgekehrt ein Client einer Ebene der Server der obersten Ebene sein. Die gebräuchlichsten Methoden, um auf die verfügbaren OPC-Elemente zuzugreifen, sind im Allgemeinen asynchron oder zyklisch (Hollender, 2010; Kastner et al., 2015).

### OPC Alarms & Events – Spezifikation

Bei der OPC-A&E-Spezifikation wird die Kommunikation ereignisgesteuert aufgebaut, im Gegensatz zu OPC DA, wo die Prozessdaten periodisch aktualisiert werden. Daher liefert ein OPC-Server Ereignisbenachrichtigungen mit Informationen, die von einem dahinter liegenden System erzeugt werden. OPC-Clients müssen spezielle Alarme oder Ereignisse abonnieren, die für sie relevant sind. Wenn also ein Ereignis eintritt, benachrichtigt der Server nur die Clients, die Abonnenten sind. Zu beachten ist hierbei, dass die Ereignisse vom System hinter dem OPC-Server aktiviert werden und nicht vom Server selbst. Es gibt drei verschiedene Arten von Ereignissen in der OPC-A&E-Spezifikation: Das einfache Ereignis „OPCSimpleEvent“, das die grundlegenden Eigenschaften des Ereignisses selbst festlegt, und die beiden anderen, die sich als Folge des vorherigen Ereignisses ergeben. Das Bedingungsereignis, „OPCConditionEvent“, benachrichtigt den Abonnenten über das Eintreten einer bestimmten Bedingung in dem betreffenden Zustandswert. Das Tracking-Ereignis (OPCTrackingEvent), das für die Erweiterung des einfachen Ereignisses verantwortlich ist, so dass die Auslösung des eigentlichen Ereignisses verfolgt werden kann. Andererseits wird oft eine Bestätigung des Ereignisses durch den Kunden verlangt (Kastner et al., 2015).

### OPC Historical Data Access (OPC HDA) – Spezifikation

Die OPC-HDA Spezifikation hat die Aufgabe, die Fähigkeiten von OPC DA, das sich auf periodische Daten in Echtzeit konzentriert, auf Zeitreihen von Daten auszudehnen, die von einem Datenbanksystem über einen bestimmten Zeitraum gesammelt wurden (historische Daten). Historische Daten stellen an sich schon eine zusätzliche Informationsquelle dar. Sie können die Entscheidungsfindung auf verschiedenen Ebenen der Automatisierungshierarchie unterstützen. In diesem Sinne definiert OPC HDA, dass die historischen Prozessdaten für jeden OPC-Client, der sie benötigt, zugänglich sind und auf Anfrage verarbeitet werden können (Hollender, 2010).

### OPC Unified Architecture – Spezifikation

Die OPC-UA-Spezifikation basiert auf der Verwendung der Webservice-Technologie, die eine Plattformunabhängigkeit nicht nur von Windows, sondern auch von jeder anderen Plattform garantiert. Diese Spezifikation ermöglicht die Integration verschiedener spezialisierter Systeme wie Enterprise Resource Planning (ERP) und Manufacturing Execution Systems (MES), die in der Regel Java verwenden und auf UNIX- oder Linux-Plattformen laufen. Auch andere Werkzeuge wie Steuerungen und intelligente Geräte mit spezifischen Betriebssystemen und Echtzeitfähigkeit können integriert werden. OPC UA basiert auf objektorientierter Programmierung und ermöglicht die Kommunikation von Informationen entweder in binärem Code oder in Textform, wobei eine komplexe Semantik verwendet wird und eine wesentlich ausgefeiltere Cybersicherheit geboten wird. Damit erfüllt und erweitert OPC UA nicht nur die Anforderungen von klassischem OPC, sondern bietet auch eine leistungsfähige, zuverlässige und robuste Kommunikation, die für den Automatisierungsbereich geeignet ist. Kurz gesagt: OPC UA liefert als Datenqualität nicht nur einen Messwert und seine technische Einheit, sondern gibt auch an, warum ein bestimmter Sensortyp gemessen wurde (Mahnke, 2010; Dang & Aubin, 2011).

### Fragen zur Selbstkontrolle

1. Nennen Sie die drei klassischen OPC-Varianten, die in der Automatisierungstechnik am weitesten verbreitet und akzeptiert sind.

* *OPC Data Access (OPC DA).*
* *OPC Alarms & Events (OPC A&E).*
* *OPC Historical Data Access (OPC HDA).*

1. Bitte geben Sie an, ob die folgenden Aussagen richtig oder falsch sind.

* OLE for Process Control (OPC-Spezifikation) basiert auf der Windows-OLE-Technologie von Microsoft. *Richtig*
* Ein OPC-DA-Server enthält die E/A-Punkte als Tags, die in einer hierarchischen Struktur organisiert sind, um die Daten den Clients in einem Vier-Tupel-Format zur Verfügung zu stellen. *Falsch*
* OPC HDA stellt sicher, dass die historischen Prozessdaten von jedem OPC-Client, der sie benötigt, abgerufen und bedarfsgerecht verarbeitet werden können. *Richtig*
* OPC UA basiert auf objektorientierter Programmierung, ermöglicht die Kommunikation von Informationen in Binär- oder Textform, verwendet eine einfache Semantik und bietet eine vereinfachte Cyber-Sicherheitsmethode. *Falsch*

## 5.6 Konnex (EIB/KNX)

Mit dem Ziel, einen einheitlichen europäischen Standard für die Automation von Wohn- und Bürogebäuden zu schaffen, wurde 1999 der Verband Konnex gegründet. Er geht auf die Initiative dreier Organisationen zurück, die bereits seit vielen Jahren auf dem europäischen Markt für das technische Management von Haus- und Gebäudeinstallationen tätig sind (Ruta et al., 2015). Obwohl sie sehr unterschiedliche Technologien, komplementäre Ziele und Tätigkeitsbereiche haben, sind diese Verbände:

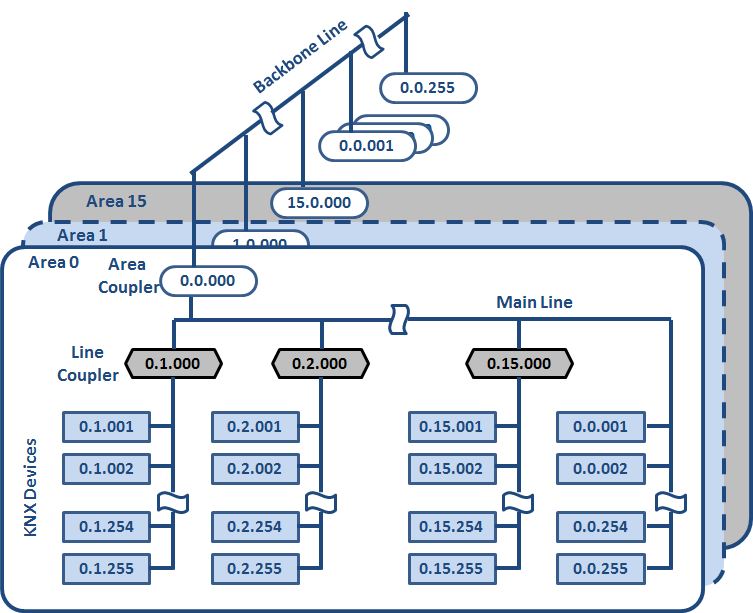
* + EIBA (European Installation Bus Association), belgische Genossenschaft, die das EIB-System vertritt.
  + BCI (BatiBUS Club International), französischer Verband, der das Batibus-System vertritt.
  + EHSA (European Home System Association), niederländischer Verband, Vertreter der EHS-Technologie.

Der Konnex Verband beginnt mit seinen Entwicklungen und bringt 2002 sein erstes Ergebnis, die KNX-Spezifikation, auf den Markt. Im Jahr 2003 wird KNX teilweise europäisch standardisiert (nur KNX-Medien und KNX-Stack). Grundlegende Eigenschaften von KNX sind die Kompatibilität mit den Produkten des damaligen EIB-Systems und ein Anwendungsbereich, der sich hauptsächlich auf Heizungs-, Lüftungs- und Klimaanlagen (HLK) sowie Beschattungs-, Jalousie- und Beleuchtungssysteme konzentriert. Auch Zählerfernauslesung und Zugangskontrolle gehören zu den möglichen Anwendungen. Eine der Stärken von KNX ist die Herstellerunabhängigkeit der Kommunikation und Steuerung. Diese wird dadurch erreicht, dass KNX eine gemeinsame Engineering Tool Software (ETS) verwendet, die eine einfache und effektive Konfiguration und Integration von Geräten verschiedener Hersteller ermöglicht. KNX wird zwar hauptsächlich für die Kommunikation und Steuerung auf der Feldebene eingesetzt, doch es ermöglicht auch die Integration mit höheren Ebenen über IP-basierte Trunks. Darüber hinaus bietet es ein flexibles Kommunikationssystem und Unterstützung für die verteilte Steuerung (Kastner et al., 2011; Kastner et al., 2015).

### KNX-Netzwerke

Das KNX-System bietet TP1 und PL110 als grundlegende Kommunikationsmedien an, die vom EIB-System für die Verkabelung bzw. die Kommunikation über das Stromnetz des Gebäudes übernommen werden (Ruta et al., 2015). Darüber hinaus wird durch den Einsatz von RF-Unterstützung für die Funkkommunikation von Geräten mit geringer Reichweite eine flexible und anpassungsfähige Kombination erreicht. Dadurch können herstellerunabhängige, verteilte, multimediale Netzwerkstrukturen geschaffen werden.

KNX-Netzwerkarchitektur

  
Quelle: Rojas (2022), basierend auf Ruta (2015)

Die Architektur der KNX-Netzwerke basiert auf einer allgemeinen Domäne, die aus bis zu 16 Bereichen besteht, welche über eine Backbone-Leitung miteinander verbunden sind. In jedem Bereich wird ein Subnetz aufgebaut, das durch eine Hauptleitung gebildet wird. Diese enthält den Bereichskoppler, der mit der Backbone-Leitung verbunden ist, an die wiederum bis zu 15 weitere Leitungen gekoppelt werden können. Schließlich unterstützt jede Linie bis zu 256 Geräte und es können bis zu 61.455 Endgeräte in das KNX-Netzwerk eingebunden werden, da die für Linien- und Bereichskoppler reservierten Adressen nicht verwendet werden können. Durch die Verwendung eines 16-Bit-Individualadressraums (IA) wird daher eine präzise Adressierung aller KNX-Netzwerkelemente erreicht (Kastner, 2015; Ruta et al., 2015). Die vorherige Abbildung zeigt die Architektur des KNX-Netzwerks.

### KNX-Kommunikationsprotokoll

Der KNX-Kommunikationsprotokollstapel ist in sieben Schichten unterteilt. Diese Schichten entsprechen dem OSI-Referenzmodell (Kastner, 2015; Ruta et al., 2015). Die Bitübertragungsschicht bietet zwei grundlegende Optionen: Twisted Pair One (TP1) und Powerline 110 (PL110), mit der Unterstützung offener und häufig verwendeter Medien wie Radiofrequenz (RF) und Ethernet (IP). Router können je nach den Bedürfnissen des Netzwerkdesigners all diese Medien kombinieren. Die Sicherungsschicht verwaltet die Adressierung von KNX-Geräten mit Hilfe von medienspezifischen Sicherungsschichten, die unter der allgemeinen Schicht aufgebaut sind und die den Medienzugriff und die logische Steuerung der Verbindungen auf hoher Ebene ermöglichen. Sie ist auch für die interne Übertragung einzelner KNX-Frames zwischen Geräten (zwei oder mehr) in einem Subnetz zuständig. Zusätzlich zur Verwaltung von Unicast-, Broadcast- und Multicast-Kommunikationsoptionen. Die Vermittlungsschicht ihrerseits ist für die Koordinierung der Kommunikation in den KNX-Subnetzen zuständig, d. h. ihre Funktion ist auf Knoten mit Routing-Funktionen ausgerichtet. Die Transportschicht unterstützt die Datenübertragung über fünf verschiedene Kommunikationsmodi:

1. Unicast-Übertragung (Punkt zu Punkt), keine Verbindung
2. Unicast-Übertragung (Punkt zu Punkt), verbindungsorientiert
3. Multicast-Übertragung (Punkt zu Mehrpunkt), verbindungslos
4. Broadcast-Übertragung (Punkt zu Domäne), verbindungslos
5. Übertragung durch das System (Punkt zu allen Punkten), ohne Verbindung

In diesem Protokoll werden die fünfte und sechste Schicht (Sitzung und Darstellung) nicht verwendet; außerdem bietet die Anwendungsschicht verschiedene Dienste für Anwendungsprozesse. Es ist zu beachten, dass der in der Transportschicht verwendete Kommunikationsmodus die Art des angebotenen Dienstes bestimmt. Die folgende Tabelle gibt die Schichtenstruktur des KNX-Protokolls in Bezug auf das OSI-Referenzmodell an.

|  |  |
| --- | --- |
| **Schichtenstruktur des KNX-Protokolls** | |
| **OSI-SCHICHT** | **KNX-SCHICHT** |
| Anwendungsschicht | Bietet Dienste für Anwendungsprozesse |
| Darstellungsschicht | Nicht genutzt |
| Sitzungsschicht | Nicht genutzt |
| Transportschicht | Unterstützt Unicast, Multicast, Broadcast und Systemübertragung |
| Vermittlungsschicht | Koordination der Kommunikation in KNX-Subnetzen |
| Sicherungsschicht | Verwaltet die Adressierung von KNX-Geräten |
| Bitübertragungsschicht | TP1, PL110, RF und Ethernet |

Quelle: Rojas (2022)

### Fragen zur Selbstkontrolle

1. Geben Sie an, wann die KNX-Spezifikation entwickelt wurde.

* 1999.
* *2002.*
* 2000.
* 2003.

1. Bitte vervollständigen Sie den folgenden Satz.

* Die Architektur der KNX-Netzwerke basiert auf einer *allgemeinen Domäne*, die aus bis zu *16 Bereichen* besteht, welche über eine *Backbone-Leitung* miteinander verbunden sind.
* Die Sicherungsschicht ist für die *interne Übertragung* einzelner *KNX-Frames* zwischen Geräten (*zwei oder mehr*) in einem Subnetz zuständig.

5.7 LonWorks®

Im Jahr 1990 entwickelte die Echelon Corporation das Local Operating Network (LON) oder LonWorks als proprietäres Steuerungsnetzwerksystem für die Haus- und Gebäudeautomation (Ryssel et al., 2011). LonWorks ist ein ereignisbasiertes System, das im Allgemeinen für die Überwachung und Steuerung von Beleuchtung, Heizung, Lüftung und Klimatisierung (HVAC), Aufzügen und Gebäudesicherheitssystemen verwendet wird. Später, im Jahr 1994, gründete Echelon LonMark als unabhängige Organisation für Hersteller, Installateure und Nutzer:innen von LonWorks, die sich für die Entwicklung kompatibler Geräte und die Gewährleistung der Interoperabilität von Produkten einsetzt (Echelon Corporation, 1999). Im Jahr 1999 erkannte das American National Standards Institute (ANSI) LonWorks als amerikanischen Standard ANSI/EAI-709.1 an, und 2005 wurde es als europäischer Standard EN-14908 anerkannt (Ryssel et al., 2011).

### LonWorks-Netzwerke

Das LonWorks-System basiert auf einem speziellen Controller, dem Neuron-Chip, der eine freie Topologie unter Verwendung von Twisted-Pair-Kanälen, Stromleitungen und Lichtwellenleitern ermöglicht (Loy et al., 2001). Darüber hinaus verwendet es Transceiver für den Buszugriff und Router, die mit dem Software-ToolLonMaker organisiert und programmiert werden können, um sie im System zu verwenden und über das LonTalk-Protokoll im Netzwerk zu kommunizieren. Aktuelle Neuron-Chips sind im Transceiver auf einem Chip integriert (Ryssel et al., 2011). Die Datenaustauschzeiten zwischen zwei Netzwerkknoten liegen im Millisekundenbereich (relativ langsam), so dass die Qualität der Übertragung von Video- und Audioströmen begrenzt ist, wie bei den meisten bekannten Steuerungsnetzwerkprotokollen (Loy & Soucek, 2015). Die logische Adresse eines jeden Knotens wird während der Konfiguration zugewiesen und basiert auf der Knoten-ID, dem Subnetz und der Domäne. Die Kommunikation zwischen verschiedenen Domänen erfolgt nur über Gateways. Die Domänen-ID ist die Kennung, die ein komplettes LonWorks-Netzwerk identifiziert und besteht aus einem Wort mit bis zu sechs Bytes. Netzwerke oder Domänen enthalten Repeater und Router, die ihre verschiedenen Kanäle korrekt koppeln. Jede Domäne ist logisch in bis zu 255 Subnetze unterteilt. Jedes Subnetz besteht wiederum aus bis zu 127 Knoten, so dass eine Domäne aus bis zu 32.385 Knoten besteht (Ryssel et al., 2011).

Die freie Topologie des Netzwerks ist zwar zulässig, schränkt jedoch die maximale Entfernung zwischen den Knoten ein. Diese beträgt bis zu 500 m, während bis zu 2.700 m zwischen den Knoten erreicht werden können, wenn das Netzwerk als linearer Bus mit kurzen Verzweigungen organisiert ist (Ryssel et al., 2011). Die Übertragungsgeschwindigkeiten hängen vom verwendeten Kanal ab und reichen von 4 bis 10 kbit/s für die Kommunikation über die Stromleitung (CEA-709.2), bis zu 19,5 kbit/s für die Radiofrequenz, von 78 kbit/s über Twisted Pair (CEA-709.3) bis zu 1,25 Mbit/s (RS-485) und 1,25 Mbit/s über eine LWL-Schnittstelle. Für die Kommunikation über Ethernet-Netze mit durchschnittlichen Geschwindigkeiten von 100 Mbit/s wurde später der EIA-852-IP-Kanal eingeführt (Loy & Soucek, 2015).

### LonTalk: Kommunikationsprotokoll für LonWorks

Im Gegensatz zu anderen Feldbusprotokollen definiert der LonTalk-Kommunikationsprotokollstapel nicht nur alle sieben Schichten gemäß dem OSI-Referenzmodell, sondern nutzt diese auch vollständig aus (Ryssel et al., 2011; Loy & Soucek, 2015). Die Bitübertragungsschicht bietet fünf Kommunikationsmedien: Twisted Pair, Stromleitung, Lichtwellenleiter, Radiofrequenz und Ethernet. Es wird jedoch kein globales Kodierungsverfahren für diese Medien verwendet, sondern jedes Medium verwendet sein eigenes Verfahren. So wird z. B. bei Twisted-Pair-Leitungen eine differentielle Manchester-Codierung verwendet, bei Stromleitungen eine Spread-Spectrum-Modulation, bei der Radiofrequenzkommunikation eine FSK-Codierung und im Falle von Ethernet wird kein eigenes Format verwendet, sondern das LonTalk-Paket wird direkt in ein IP-Paket verpackt (Ryssel et al., 2011). Die Sicherungsschicht enthält eine MAC-Schicht (Media Access Control), die einen Kontrollmechanismus zur Vermeidung von Kollisionen im Netz unter Verwendung des p-persistenten CSMA-Prädiktionsverfahrens (Carrier Sense Multiple Access) bereitstellt. Um sicherzustellen, dass die Frames fehlerfrei übertragen werden, verwendet die Sicherungsschicht zyklische Redundanzprüfungen (Cyclic Redundancy Checks, CRC) von 16 Bit und meldet entdeckte Fehler zur Korrektur an höhere Schichten. Darüber hinaus werden in der Frame-Codierung zusätzlich zur Präambel ein Prioritätsbit, ein Bit für einen alternativen Pfad und die Akkumulationsänderung verwendet. Die Vermittlungsschicht bietet ihrerseits die Möglichkeit zur Paketübertragung innerhalb einer Domäne ohne Verbindung und ohne Quittierung durch die Dienste: Unicast, Multicast und Broadcast.

|  |  |  |
| --- | --- | --- |
| **Schichtenstruktur des LonTalk®-Protokolls** | | |
| **OSI-Schicht** | **LonTalk-Schicht** | **Funktionen** |
| Anwendungsschicht | Anwendungs- und Darstellungsschicht | Anwendungsschnittstellen  Netzwerkverwaltung |
| Darstellungsschicht |
| Sitzungsschicht | Sitzungsschicht | Anfrage- und Antwortdienste |
| Transportschicht | Transportschicht | Erkannte Dienste  Nicht erkannte Dienste |
| Authentifizierungsdienst | Authentifizierung |
| Transaktionskontroll-Subschicht | Erkennung doppelter Pakete  Erneute Übertragung von verlorenen Paketen |
| Vermittlungsschicht | Netzwerkschicht | Topologie, Routing und verbindungslose Unterstützung Unicast, Multicast und Broadcast-Übertragung |
| Sicherungsschicht | Sicherungsschicht | CRC und Kodierung |
| MAC-Subschicht | CSMA und Kollisionsmanagement |
| Bitübertragungsschicht | Bitübertragungsschicht | Medienspezifische Protokolle |

Quelle: Rojas (2022)

Die Hauptverantwortung für Kommunikationsaufgaben tragen die Transportschicht und die Sitzungsschicht. Die Transportschicht ist in drei Schichten unterteilt:

1. Die Transportschicht, die für erkannte und nicht erkannte Dienste zuständig ist,
2. Der Authentifizierungsdienst und
3. Die Transaktionskontroll-Subschicht, die für die Erkennung doppelter Pakete und die erneute Übertragung verlorener Pakete zuständig ist.

In der Zwischenzeit wickelt die Sitzungsschicht den Client-Zugriff auf entfernte Server über eine einfache Anfrage- und Antwortmethode ab. Die Darstellungsschicht und die Anwendungsschicht arbeiten zusammen, um die Interoperabilität im Netz durch Netzmanagement und Schnittstellen für Anwendungsdienste zu gewährleisten, die das Senden und Empfangen von Nachrichten und die Datendarstellung unabhängig voneinander ermöglichen (Ryssel et al., 2011; Loy & Soucek, 2015). Die vorstehende Tabelle gibt die Schichtenstruktur des LonTalk-Protokolls in Bezug auf das OSI-Referenzmodell an.

### Fragen zur Selbstkontrolle

1. Geben Sie die drei Schichten an, in die die Transportschicht des LonTalk-Protokolls unterteilt ist.

* *Die Transportschicht, die für erkannte und nicht erkannte Dienste zuständig ist,*
* *Der Authentifizierungsdienst*
* *Die Transaktionskontroll-Subschicht, die für die Erkennung doppelter Pakete und die erneute Übertragung verlorener Pakete zuständig ist*

1. Bitte vervollständigen Sie den folgenden Satz.

* Die *Hauptverantwortung* für *Kommunikationsaufgaben* tragen die Transportschicht und die *Sitzungsschicht*.
* Das LonWorks-System basiert auf einem speziellen *Controller*, dem *Neuron-Chip*, der eine *freie* Topologie ermöglicht.

Zusammenfassung

Industrielle Kommunikationstechnik ist ein sehr weites Feld, das alles umfasst, was mit den verschiedenen Arten von industriellen Netzwerken zu tun hat, wie z. B. Steuerungsnetzwerke, Überwachungsnetzwerke und Kommunikationsnetzwerke, einschließlich der Technologien und Lösungen, die hauptsächlich in der Prozess- und Anlagenautomatisierung angeboten und installiert werden. Daher werden im Abschnitt Industrielle Netzwerke die Unterschiede zwischen industriellen Netzwerken (Industrial Networks, ICNs) und kommerziellen Netzwerken (Commercial Networks, CCNs) erläutert. Anschließend werden Steuerungsinformationen, Überwachungsinformationen und Sicherheitsinformationen als die drei Arten von Informationen beschrieben, die in industriellen Netzwerken verwendet werden. Dieser Abschnitt schließt mit einer Beschreibung der Komponenten der ICNs und wie die Kommunikation in der Industrie 4.0 aussieht. Anschließend wird im Abschnitt HART ein Überblick über alles gegeben, was mit HART-Netzwerken zu tun hat, beginnend mit der Netzwerkarchitektur, ihrer Funktionsweise und dem HART-Protokoll. In ähnlicher Weise gibt der Abschnitt über PROFIBUS einen Einblick in die PROFIBUS-Netzwerke, ihre Architektur und ihr Protokoll. Der Abschnitt über drahtlose Kommunikation führt in das Gebiet der drahtlosen Technologie ein. Dabei wird zunächst eine Einteilung nach Anwendungsgebiet und Signalreichweite vorgenommen. Anschließend werden industrielle drahtlose Sensornetzwerke (Industrial Wireless Sensor Networks, IWSN) als spezialisierte drahtlose Netzwerke vorgestellt, die Überwachungs- und Steuerungsaufgaben erleichtern. Die Beschreibung einiger Bereiche, in denen die Entwicklung von IWSNs von Bedeutung war, der in IWSNs verwendeten Topologien, ihrer Funktionsweise und der wichtigsten Kommunikationsprotokolle schließt diesen Abschnitt ab. Der nächste Abschnitt ist OPC gewidmet und beschreibt die Entwicklung des klassischen OPC (OPC DA, OPC A&E und OPC HDA) und der OPC Unified Architecture als spezialisierte Werkzeuge, die industrielle Prozesssteuerungsanwendungen auf allen Hierarchieebenen dabei unterstützen, Daten auf standardisierte Weise auszutauschen. Schließlich geben die Abschnitte über Konnex (EIB/KNX) und LonWorks einen Einblick in diese auf Gebäudeautomation spezialisierten Netzwerke, ihre Architektur und ihre Protokolle.

Lektion 6 – Verteilte Steuerungssysteme

**Lernziele**

Nach der Bearbeitung dieser Lektion …

… kennen Sie die Entwicklungsgeschichte der Steuerungssysteme.

… können Sie zwischen zentralisierten und verteilten Steuerungssystemen unterscheiden.

… erkennen Sie die verschiedenen Komponenten verteilter Steuerungssysteme.

6. Verteilte Steuerungssysteme

Einführung

Seit der offiziellen Anerkennung des vom Niederländer Cornelis Drebbel erfundenen Temperaturreglers (1620) als erstes rückgekoppeltes Regelsystem und des Watt-Reglers (1788) als Endpunkt der vorindustriellen Entwicklung der Automatisierung und Beginn der ersten industriellen Revolution (Lukas, 1986; Platero, 2009) haben sich die Steuerungssysteme in Europa stark weiterentwickelt. Die Entwicklung von Steuerungssystemen für industrielle Produktions-, Montage- und Fertigungsprozesse hat zu speicherprogrammierbaren Steuerungen (SPS), SCADA-Systemen und Prozessleitsystemen (PLS) geführt, die einen wesentlichen Bestandteil der heute in diesem Bereich eingesetzten Automatisierungstechnik darstellen (Zhang, 2010; Dey & Sen, 2020; Gardner, 2020). Diese Lektion bietet eine kurze Beschreibung der Entwicklung von Steuerungssystemen bis hin zu verteilten Steuerungssystemen und deren Komponenten.

6.1 Entwicklungsgeschichte der Steuerungssysteme

Anfangs gab es in industriellen Anlagen oder Prozessen keinerlei Integration, sondern jede Einheit, aus der die Anlage bestand, wurde lokal und isoliert verwaltet (Dey & Sen, 2020). Oder anders ausgedrückt: Wenn die einzelnen Einheiten über Steuerungssysteme verfügten, wurden diese lokal ausgeführt. Daher waren viele Arbeitskräfte erforderlich, um diese Einheiten zu koordinieren, damit die Produktion in akzeptabler Weise gekoppelt werden konnte. Mit dem Wachstum der Industrie wurde die Überwachung des Zustands von Geräten, Maschinen und Anlagen sowohl für die Entscheidungsfindung als auch für die Steuerung immer aufwändiger und monotoner (Zhang, 2010). Daraus resultierte die Notwendigkeit, Systeme zu schaffen, die es ermöglichen, den Zustand ihrer Feldanlagen zu steuern und zu überwachen.

Mit der Weiterentwicklung der Steuerungssysteme hat sich auch der Automatisierungsgrad erhöht (García Moreno, 2020). Viele ursprünglich manuelle Tätigkeiten wurden im Zuge der industriellen Automatisierung durch maschinelle Systeme ersetzt. Ausgehend von pneumatischen und hydraulischen Systemen hat sich die industrielle Automatisierung von Produktions- und Fertigungsprozessen im Laufe der Jahre weiterentwickelt und ist durch den Einsatz moderner Robotersteuerungssysteme, cyber-physischer Systeme und des industriellen Internets der Dinge (IIoT) u. a. zur Industrie 4.0 geworden (Dey & Sen, 2020). Nach García Moreno (2020) ist die erste Automatisierungsstufe die elementare Stufe und umfasst die lokale Automatisierung einer einfachen Maschine oder eines Maschinenteils, die Aufgaben der Totzeitüberwachung, Teilepositionierung und einfache Sicherheitsfunktionen übernimmt. Die zweite Stufe oder mittlere Stufe ist durch die Automatisierung einer Reihe von einfachen Maschinen oder einer komplexen Maschine gekennzeichnet und deckt den klassischen Bereich der industriellen Automatisierung ab. Die dritte Stufe besteht darin, einen kompletten Prozess zu automatisieren, der neben den grundlegenden Steuerungsaufgaben auch Überwachung, Optimierung, Wartungsmanagement, Qualitätskontrolle und Produktionsüberwachung umfasst.

Die Automatisierung der dritten Stufe, wie sie auch genannt wird, entsteht mit der Einführung von speicherprogrammierbaren Steuerungen (SPS) und den ersten Minicomputern in die Steuerung industrieller Prozesse. Die Architektur oder Struktur dieser Systeme hängt weitgehend davon ab, wie der Computer für die Steuerungsaufgaben eingesetzt wird. Denn ein Computersteuerungssystem ist nicht dasselbe wie ein computergestütztes Steuerungssystem (Zhang, 2010). Wenn die Überwachung durch einen Computer erfolgt, der von den überwachten Objekten entfernt ist, spricht man von einem Computersteuerungssystem. Betrachtet man dagegen ein einheitliches System, das neben der Hardware auch die Software in das zu steuernde System integriert, so spricht man von einem computergestützten Steuerungssystem. Die beiden bekanntesten industriellen Steuerungsarchitekturen oder -strukturen für die Automatisierung der dritten Stufe sind das zentralisierte Steuerungssystem und das verteilte Steuerungssystem, wobei anzumerken ist, dass dies nicht die einzigen sind und viele Automatisierungslösungen eine Mischung aus beiden darstellen, die an die spezifischen Anforderungen der jeweiligen Situation angepasst sind (García Moreno, 2020).

Zentralisiertes Steuerungssystem

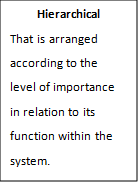
Das zentralisierte Steuerungssystem ist ein System, das aus einem zentralen Computer oder Controller besteht, der für die gesamte Informationsverarbeitung verantwortlich ist und dessen Ein- und Ausgänge mit jedem Sensor und Aktor der Anlage, einer Prozessschnittstelle und einer Bedienstation verbunden sind (García Moreno, 2020). Der Hauptvorteil besteht darin, dass seine Architektur den Informationsfluss erleichtert und globale Optimierungsziele ermöglicht. Der Nachteil besteht darin, dass die Zuverlässigkeit des Systems vom Zentralrechner abhängt. Bei den ersten Systemen dieser Art bestand die Bedienstation aus einer Konsole, einem Panel oder einer Tafel, die als zentrale Steuerungs- und Überwachungseinheit bezeichnet wurde und an die die Anzeigen und Zähler der wichtigsten Anlagensysteme angeschlossen waren (Gardner, 2020). Diese Konsolen ermöglichten das ferngesteuerte Starten und Stoppen der wichtigsten Maschinen und/oder Geräte, auch wenn diese mit der Bedienstation fest verkabelt waren. Sie ermöglichten außerdem den Zugriff auf die am häufigsten verwendeten Maschinen und Notfallsysteme, die immer aktiviert und einsatzbereit waren. Zu diesen Systemen gehörten u. a. Feuerlöschpumpen, Wasserpumpen und andere Reservesysteme zur Belüftung und Kühlung. Die Alarmverwaltung erfolgte über ein Panel, auf dem die Meldungen, die in der Regel von einem Überwachungstechniker erkannt wurden, durch Lichter angezeigt wurden. Der Bediener besuchte die Anlage in regelmäßigen Abständen, um sich über den Zustand des Prozesses auf dem Laufenden zu halten, insbesondere um zu bestätigen, was in der Station angezeigt wurde, und um zu beobachten, welche Parameter nicht erreicht wurden. Die wichtigsten Parameter der Anlage wurden kontinuierlich mit Hilfe von Grafikschreibern und manuell geführten Logbüchern aufgezeichnet. Diese Aufzeichnungen dienten der Analyse und Trendermittlung. Diese Steuerungssysteme sind praktisch veraltet. Für relativ kleine und einfache Anlagen können sie jedoch auch heute noch geeignet sein.

Später wurden die zentralisierten Steuerungssysteme mit elektronischen Instrumenten ausgestattet, und die festverdrahteten Schalter in der Bedienstation zur Steuerung von Fernausrüstungen und Notfallsystemen wurden durch einen mikroprozessorgesteuerten Controller ersetzt, der das Herzstück des elektronisch basierten Automatisierungssystems bildete. Dieser Controller empfing die Eingangssignale von der Anlage und führte die programmierte Steuerlogik aus, um Steuersignale als Ausgänge zu erzeugen, die an die Produktionsanlagen gesendet wurden (Gardner, 2020). Diese Ein- und Ausgangssignale ermöglichten nicht nur die Prozesssteuerung, sondern auch die Zustandsüberwachung und das Alarmmanagement. Auf diese Weise erhalten die anlagenweiten Aktoren (Motorstarter und Ventilsteuerungen) Befehle von der Leitwarte (oder Zentrale), von wo aus die steuerungstechnische Automatisierung erfolgt.

**Architekturen von zentralisierten Steuerungssystemen**

Diagram

Description automatically generated  
Quelle: Rojas (2022)

Eine Variante der zentralisierten Steuerung ist die so genannte mehrstufige oder **hierarchische** zentralisierte Steuerung, die aufgrund der erwiesenen Robustheit industrieller Steuerungen möglicherweise am besten geeignet ist (García Moreno, 2020). Dieses zunächst hierarchische zweistufige Steuerungssystem verwendet lokale Controller für bestimmte Regelkreise mit zeitlich begrenzten Steuerungsaufgaben. Bei dieser Architektur übernimmt der Zentralrechner die Überwachung, die Übermittlung von Anweisungen und Parametern an die lokalen Steuerungen und die Verarbeitung von Informationen für folgende Aufgaben Produktionsmanagement, Wartungsmanagement und Qualitätskontrolle. Durch diese Struktur kann der Prozess auch bei einem Ausfall des Host-Computers weiter funktionieren. Werden Planungs- und Steuerungsaufgaben erforderlich, kann diese Struktur durch Hinzufügen einer weiteren Hierarchieebene so verändert werden, dass sie diesen Aufgaben gerecht wird. Ein typisches Beispiel für solche zentralisierten Steuerungssysteme sind SCADA-Systeme (Zhang, 2010; García Moreno, 2020). Die vorherige Abbildung zeigt die Architekturen der zentralisierten Steuerungssysteme.

Verteilte Steuerungssysteme

Die Architektur verteilter Steuerungssysteme (Prozessleitsysteme, PLS) ähnelt im Wesentlichen hierarchischen, zentralisierten Steuerungssystemen wie SCADA-Systemen. SCADA-Systeme sind jedoch hauptsächlich auf die Datenverwaltung (Überwachung) ausgerichtet, während PLS eher auf die Prozesssteuerung ausgerichtet sind (Gardner, 2020). Beim PLS der ersten Generation nach García Moreno (2020) werden im Gegensatz zur hierarchischen Steuerungsstruktur, bei der verschiedene Aufgaben unterschiedlichen Ebenen zugeordnet werden, andere Überlegungen angestellt, wie z. B.

* das Vorhandensein mehrerer Steuerungs- und Produktionseinheiten, die dieselben Aufgaben ausführen.
* das Vorhandensein von Kommunikation zwischen den Controllern, die diese Einheiten steuern.
* die Möglichkeit, im Falle eines Ausfalls oder einer Arbeitsüberlastung einige oder alle Aufgaben auf andere Einheiten zu übertragen.

Diese Struktur bringt Vor- und Nachteile mit sich. Die Idee, problematische Einheiten zu umgehen, ermöglicht es einerseits, unnötige Blockaden des Systems zu vermeiden, andererseits erfordert sie aber auch, dass die einzelnen Produktionsinseln eine dynamische Aufgabenzuweisung haben können und somit hohe Kapazitäten für den Zugriff auf Kommunikation und Informationsverarbeitung benötigen. Darüber hinaus sind intelligente Algorithmen zur Fehlererkennung und -diagnose erforderlich.

Allerdings haben nicht alle PLS-Systeme die gleiche Architektur, da je nach Art des Prozesses und des erwarteten Ergebnisses des Produkts, zusätzlich zu den damit verbundenen Kosten, nicht alle Aufgaben repliziert werden können, so dass nicht alle Inseln identisch sind. In diesen Fällen werden die verschiedenen Verarbeitungsschritte dort durchgeführt, wo sie den größten Nutzen für die Gesamtziele des Systems bringen. Dies stellt höhere Anforderungen an die Kommunikation, da die Informationen durch das gesamte System fließen und dort zur Verfügung stehen müssen, wo und wann sie benötigt werden (Zhang, 2010). Dieses Problem wurde mit der Entwicklung der Prozessleitsysteme und der Kommunikationsnetze gelöst, indem die direkte Verbindung von der Leitwarte zu den einzelnen, über die Anlage verteilten Steuerungen in den Prozessleitsystemen der ersten Generation durch Netzwerksysteme oder Feldbusse ersetzt wurde, die in den modernsten Prozessleitsystemen von Computerarbeitsplätzen in der Leitwarte begleitet werden (Gardner, 2020). Die folgende Abbildung zeigt die Architekturen der verteilten Steuerungssysteme.

**Architekturen der verteilten Steuerungssysteme**

Diagram

Description automatically generated  
Quelle: Rojas (2022)

Beide Konzepte haben sehr interessante Eigenschaften. Deshalb gibt es in heutigen automatisierten Produktionssystemen eine Tendenz, verteilte Steuerungsmerkmale in hierarchischen Strukturen zu mischen, was zu Mischlösungen führt (García Moreno, 2020). Zusammenfassend lässt sich sagen, dass die verteilte Struktur dazu beiträgt, die Zuverlässigkeit des Systems und seine Wartungsfreundlichkeit zu erhöhen, da lokale Änderungen des Prozesses oder seiner Ausrüstung nur lokale Auswirkungen auf das Steuerungssystem haben. Darüber hinaus ermöglicht die zentralisierte Datenverarbeitung eine globale Optimierung und Überwachung. Heutzutage werden die Begriffe PLS und SCADA laut Gardner (2021) oft synonym verwendet, da sie viele Ähnlichkeiten aufweisen. Aber allgemein gilt:

* SCADA-Systeme sind datenorientiert, während PLS-Systeme eher prozessorientiert sind. Obwohl sowohl SCADA-Systeme als auch aktuelle PLS-Systeme über eine Überwachungsebene verfügen, werden bei SCADA-Systemen die gesammelten Daten verwendet, um dem Bediener mehr Informationen zu liefern, die häufig mit detaillierten Prozessdiagrammen überlagert sind, anstatt nur Messwerte zu kopieren, während bei aktuellen PLS-Systemen dem Bediener nur Echtzeitdaten zur Verfügung gestellt werden. Im Gegensatz dazu konzentrieren sich PLS-Systeme mehr auf die Steuerung von Anlagenprozessen.
* SCADA-Systeme verwenden weiträumige Kommunikationsnetze wie das Internet oder Wide Area Networks (WANs), da sie in der Regel über mehrere entfernte Gebiete verteilt sind, während PLS-Systeme lokale Kommunikationsnetze (LANs) verwenden können, da ihr Aktionsradius in der Regel begrenzter ist, z. B. auf bestimmte Bereiche der Anlage.
* SCADA-Systeme sind eher überwachungsorientiert, so dass in der Regel lokale Mikroprozessorsteuerungen die Einstellungen für die Rückkopplungsregelung vornehmen. Die PLS-Systeme ihrerseits verwenden in der Regel eine Rückkopplungsregelung über lokale RTUs und SPS-Systeme, aber die Rückkopplungsregelung kann auch von der zentralen Leitwarte über den zentralen Mikroprozessor erfolgen.
* SCADA-Systeme warten auf Signale, um Ergebnisse anzuzeigen, da sie im Allgemeinen ereignisgesteuert sind, während PLS-Systeme häufig aktuelle Informationen anzeigen, da sie den Prozess ständig überwachen. Während SCADA-Systeme Datenbanken mit aktuellen Anlageninformationen abfragen, die vom System abgerufen oder für eine spätere Analyse archiviert werden, betrachten PLS-Systeme nur die aktuellen Werte der Informationen (Gardner, 2020).

Fragen zur Selbstkontrolle

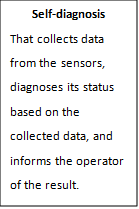
1. Bitte geben Sie an, ob die folgenden Aussagen richtig oder falsch sind.

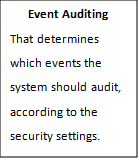
* SCADA-Systeme verwenden lokale Kommunikationsnetzwerke (LANs), da ihr Aktionsradius in der Regel begrenzt ist. *Falsch*
* PLS-Systeme sind prozessorientiert und bieten dem Bediener lediglich Echtzeitdaten. *Richtig*
* SCADA-Systeme sind überwachungsorientiert, so dass in der Regel lokale Mikroprozessorsteuerungen die Einstellungen für die Rückkopplungsregelung vornehmen. *Richtig*
* PLS-Systeme warten auf Signale, um Ergebnisse anzuzeigen, da sie im Allgemeinen ereignisgesteuert sind. *Falsch*

1. Wie nennt man die Automatisierungsstufe, die die lokale Automatisierung einer einfachen Maschine oder eines Maschinenteils umfasst?

* Industrielle Stufe
* Mittlere Stufe
* *Elementare Stufe*

6.2 Komponenten von verteilten Steuerungssystemen

Aufgrund der großen Ähnlichkeit zwischen PLS- und SCADA-Systemen sind auch ihre Komponenten ähnlich. Im Gegensatz zu SCADA-Systemen, die eine gewisse Tendenz zur Offenheit gezeigt haben, sind PLS-Systeme jedoch in Bezug auf die meisten Komponenten weiterhin geschlossen. Ausgehend von ihrer Architektur und der Flexibilität kostengünstiger Komponenten, wie z. B. speicherprogrammierbarer Steuerungen (SPS), scheint es einfach zu sein, auf ihrer Grundlage ein funktionsfähiges PLS-System zu entwickeln, aber die Fähigkeit zur **Selbstdiagnose**, die **Ereignisüberprüfung** und die intelligente Verwaltung von Messgeräten sowie andere Funktionen, die von PLS-Herstellern entwickelt wurden, und insbesondere die Software sind nicht einfach zu entwickeln (Kuphaldt, 2022). PLS-Systeme bestehen grundsätzlich aus Hardwareelementen, Softwaremodulen und Kommunikationsmodellen mit proprietären Protokollen und Verbindungen (Zhang, 2010; Dey & Sen, 2020), die im Folgenden beschrieben werden:

Hardwareelemente

Unabhängig von der Größe des jeweiligen verteilten Steuerungssystems gibt es fünf grundlegende Hardwareelemente, aus denen es sich zusammensetzt: die zentrale Bedienstation, die Feldüberwachungs- und Steuerungsstation, die Kommunikationsinfrastruktur, die direkten Steuerungselemente und die Feldinstrumentierung. Darüber hinaus ist die Verwendung einer selektiven Redundanz dieser Elemente auf allen Ebenen typisch für die fortschrittlichsten PLS-Systeme, um ihre Robustheit zu erhöhen und jede Möglichkeit eines Ausfalls zu berücksichtigen (Zhang, 2010).

**Zentrale Bedienstation**

Die Zentrale des Bedieners besteht im Allgemeinen aus den Datenbanken, in denen die historischen Dateien des Systems gespeichert sind, den Mensch-Maschine-Schnittstellen (HMI) und den Geräten wie Tastatur und Maus, mit denen der Bediener interagieren kann, wobei es sich heute auch um taktile Geräte handeln kann (Dey & Sen, 2020). HMIs ermöglichen den systematischen Zugriff auf alle Anlageninformationen entweder über hochauflösende Grafiken und grafische Benutzeroberflächen oder in Form numerischer Daten und bestehen in der Regel aus einem oder mehreren Monitoren, je nachdem, wie viele Informationen der Bediener benötigt (Zhang, 2010). Heutige HMIs sind u. a. darauf ausgelegt, die Anlagensicherheit zu erhöhen, eine angemessene Aufgabenpriorisierung und den Einsatz von Ausrüstungen zur Verbesserung der Produktqualität zu ermöglichen und einen kontinuierlichen Anlagenbetrieb über längere Zeiträume aufrechtzuerhalten. Darüber hinaus kann eine gut gestaltete Benutzerschnittstelle dazu beitragen, Ermüdung und Frustration des Bedienpersonals zu verringern und eine Arbeitsumgebung zu schaffen, die eine frühzeitige Prävention und eine angemessene Reaktion auf anormale Bedingungen ermöglicht (Dey & Sen, 2020). Die folgende Abbildung zeigt eine einfache Bedienstation.

**Einfache Bedienstation**

Ein Bild, das Text, drinnen, Computer enthält.

Automatisch generierte Beschreibung  
Quelle: Fonesca (2019), CC

Im Juli 2015 wurde die Industrienorm ISA-101.01 veröffentlicht, der sich mit der Konzeption, dem Design und der Implementierung von HMIs für PLS-Systeme sowie deren Betrieb und Wartung befasst (Dey & Sen, 2020). Die ersten drei der insgesamt neun Abschnitte dieser Norm enthalten den Anwendungsbereich, Verweise auf andere Normen und allgemeine Beschreibungen der in der Norm verwendeten Abkürzungen und Begriffe. Die anderen sechs Abschnitte konzentrieren sich auf verbindliche Anforderungen, Empfehlungen und Best Practices für die HMI-Implementierung und -Wartung über den gesamten Lebenszyklus. Die Norm ISA 101.01 empfiehlt eine Darstellungshierarchie, um einen strukturellen Überblick über den Prozess zu erhalten. Die Darstellung von Informationen auf einem Bildschirm oder einem Teil eines Bildschirms gehört zu den Anzeigestilen. Der HMI-Designprozess bestimmt die betrieblichen Anforderungen an eine Anzeige sowie deren Stil. Darüber hinaus können technologische oder physische Faktoren wie die Größe des Bildschirms, seine Position, die Menge der vom Benutzer tatsächlich verwalteten Informationen und die Art der Interaktion des Benutzers mit dem Bildschirm (Tastatur, Maus oder Touchscreen) die Art der Anzeige beeinflussen.

Die von ISA 101.01 vorgeschlagene Anzeigehierarchie ermöglicht es dem Designer, einen Überblick über einen großen Teil des Prozesses zu geben und, falls erforderlich, Ebenen der Steuerungsfunktionalität und mehr Details durch andere, tiefergehende Anzeigen bereitzustellen. Nach Dey & Sen (2020) beträgt die maximale Anzahl der empfohlenen Visualisierungsebenen für Menschen je nach kognitiven Begrenzungen vier. Dabei ist Ebene vier die Ebene mit der fokussiertesten Darstellung und Ebene eins die Ebene mit der umfassendsten Darstellung. Für die einzelnen Visualisierungsebenen werden folgende Inhalte empfohlen:

* Auf Ebene 1 sollten alle Informationen, die sich auf den gesamten Zuständigkeitsbereich des Bedieners beziehen, auf einem einzigen Bildschirm angezeigt werden. Dieser Bildschirm sollte eine Zusammenfassung oder einen Überblick über die Prozessbedingungen, die wichtigsten Parameter, anormale Bedingungen und Alarme enthalten.
* Die Bildschirme der Ebene 2 sind detaillierter als die der Ebene 1 und zeigen den Prozess auf einer höheren Ebene. Unter normalen Bedingungen kann der Bediener mit den Bildschirmen der Ebene 2 interagieren, so dass ihr Umfang in der Regel begrenzter ist als der eines Bildschirms der Ebene 1. Die Bildschirme dieser Stufe sind auf die Aufgabenbearbeitung ausgerichtet und nicht wie die Bildschirme der ersten Ebene auf eine kontinuierliche, allgemeine und beschreibende Darstellung.
* Auf Ebene 3 werden ebenfalls Aufgaben ausgeführt, die jedoch als nicht routinemäßig eingestuft werden. So werden auf den Bildschirmen Systemdetails angezeigt, die es dem Bediener ermöglichen, z. B. Gerätewechsel, Ausrichtungsänderungen oder einige routinemäßige, aber komplexere Aufgaben durchzuführen. Darüber hinaus müssen die Bildschirme auf dieser Ebene ausreichende Informationen liefern und gleichzeitig eine Interaktion mit dem Bediener ermöglichen, um als Grundlage für die Prozessdiagnose zu dienen.
* Auf Ebene 4 sind die Bildschirme mehr auf die Diagnose ausgerichtet und sollten z. B. Unterstützung bei der Steuerung und Diagnose oder beim Betrieb eines Geräts bieten. Für diese Darstellungsbildschirme wird die Verwendung von Popup- oder Dialogfenstern vorgeschlagen, da sie häufig verwendet werden und die angezeigten Informationen kurz sind.

Die HMI-Navigation ist in der Regel nicht notwendigerweise auf die Anzeigeebenen abgestimmt. Daher können die definierten Anzeigeebenen mehr oder weniger als die Ebenen der definierten Navigationshierarchie sein.

Andererseits ergänzt der heutige Einsatz von Touchscreens in Verbindung mit der Bedienermaus, meist in Form eines Trackballs, und der Tastatur die zentrale Bedienstation und ermöglicht eine benutzerfreundliche und transparente Interaktion, die einen robusten Betriebszustand des Prozesses oder der Anlage gewährleistet. Anzumerken ist, dass für die Tastaturen dieser Stationen eine besondere Konstruktion erforderlich ist, da sie einer ständigen und langen Betätigung der Tasten durch das Bedienpersonal unterliegen. Herkömmliche PC-Tastaturen sind nicht sehr robust und unter diesen Arbeitsbedingungen sehr störanfällig. Bedienertastaturen sind in der Regel robust, intuitiv und funktional gestaltet und mit flachen, staub- und spritzwassergeschützten Tasten ausgestattet (Dey & Sen, 2020).

**Feldsteuerstation**

Das Herzstück eines PLS-Steuerungssystems ist die Feldsteuerstation. Diese Feldsteuerstation (Field Control Station, FCS) besteht aus einem Gehäuse mit mehreren Einschüben, die als Feldsteuereinheiten (Field Control Units, FCU) bezeichnet werden, wenn sie einen Prozessor enthalten, oder einfach als Knoten, wenn sie keinen Prozessor enthalten (Dey & Sen, 2020; Kuphaldt, 2022). Die FCUs oder Knoten bestehen aus verschiedenen Kartentypen, die für die physischen Module von Prozessor, E/A, Kommunikation, Stromversorgung usw. verantwortlich sind. Die Stromversorgungs- und Prozessormodule in den FCUs sind in der Regel doppelt vorhanden. Dadurch entsteht ein redundantes System, das mit hoher Wahrscheinlichkeit einen ausfallsicheren Betrieb des PLS-Systems gewährleistet, da die Standby-Module sofort den Betrieb des PLS-Systems übernehmen, wenn die aktiven Module aus irgendeinem Grund ausfallen (Dey & Sen, 2020). Die folgende Abbildung zeigt zwei FCUs mit typischen kommerziellen Konfigurationen.

**Feldsteuereinheiten**

Ein Bild, das Text, drinnen enthält.

Automatisch generierte Beschreibung

Quelle: Kuphaldt (2022), CC 4.0

Die FCS sind aufgrund ihrer Konstruktionsmerkmale sehr kompakt und daher einfach zu installieren und zu warten. Sie bieten ein hohes Maß an Sicherheit und Zuverlässigkeit und sind aufgrund ihres geringen Verbrauchs und CO2-Ausstoßes umweltfreundlich (Dey & Sen, 2020). E/A-Module, Prozessormodule und Stromversorgungsmodule sind die wichtigsten Module oder Karten der FCS. Die Art und Anzahl der E/A-Module wird durch die Anzahl und Art der Feldgeräte (Sensoren und Aktoren) bestimmt. Die Hauptfunktion der E/A-Module besteht darin, die über die Eingänge erfassten Signale dem Prozessormodul zur Verarbeitung durch logische Operationen oder Steuerungsberechnungen zur Verfügung zu stellen und die aus dieser Verarbeitung resultierenden Signale über die Ausgänge auszugeben. E/A-Module werden in drei Typen unterteilt: analoge E/A, digitale E/A und E/A für spezielle Zwecke. Analoge E/A-Module verarbeiten normalerweise Spannungen von 1 bis 5 V oder Stromsignale von 4 bis 20 mA. Sie verarbeiten Eingangssignale von Feldsensoren und Transmittern sowie Ausgangssignale zur Steuerung von Aktionen. Digitale E/A-Module verarbeiten binäre Logiksignale, in der Regel ein Null- oder 24-V-Gleichspannungssignal, Eingangssignale von Logik-Eingangsschaltern und Ausgangssignale zur Ansteuerung von Ventilen, Relais und anderen Logikgeräten. Spezielle E/A-Module umfassen alle Module der Reihe intelligenter Feldgeräte, die für die Verwendung mit Feldbus, Profibus und/oder HART ausgelegt sind, sowie Module für verschiedene Arten von Thermoelementen, Impulssignalen und RTDs. Schließlich wird die Konfiguration der FCUs und Knoten sowie deren Anzahl durch die Anzahl und die Art der E/A-Module bestimmt. Die E/A-Module können auch redundant sein, wenn sie doppelt in der Konfiguration verwendet werden (Duplex-Format). Die E/A-Module müssen als Standard-E/A-Subsysteme von der Stange konfiguriert werden. Dadurch wird sichergestellt, dass für die verschiedenen E/A-Subsysteme dieselben Betriebsparameter für die Programmierung oder Systemkonfiguration verwendet werden können, da sie dieselbe Logik verwenden (Zhang, 2010). So wird vermieden, dass bei einem Wechsel von einem PLS-System zu einem anderen die E/A-Subsysteme ausgetauscht werden müssen. Da die PLS-Logik hardwareunabhängig ist, sind außerdem keine Änderungen erforderlich, wenn das E/A-Subsystem geändert werden muss.

Die Prozessormodule oder -karten hingegen sind mit zwei Mikroprozessoreinheiten und einem Komparator ausgestattet. Die Mikroprozessoreinheiten führen die gleichen Steuerungsberechnungen durch, und der Komparator überprüft die Ergebnisse jeder Berechnung (Dey & Sen, 2020). Wenn die Ergebnisse beider Mikroprozessoren gleich sind, ist das Modul in Ordnung. In diesem Fall werden die Ergebnisse über die Kommunikationsinfrastruktur an die Hauptspeichergeräte übertragen. Das aktive Prozessormodul ist durch das Backup-Modul zu ersetzen, wenn die Ergebnisse unterschiedlich sind. Dies wird als Störung angesehen. Das Backup-Modul ist immer auf dem neuesten Stand und gleicht seine Informationen mit denen des aktiven Prozessormoduls ab. Dadurch ist ein reibungsloser Austausch gewährleistet. In der Regel wird für ein FCS eine einzige FCU verwendet, die die Prozessormodule enthält. Daher müssen alle Knoten in dieser FCS mit der FCU kommunizieren, um auf die Prozessormodule zugreifen zu können.

Nach Dey & Sen (2020) ist das Stromversorgungsmodul der wichtigste Teil der FCS, da es für die notwendige Stromversorgung aller E/A-Module verantwortlich ist und daher redundant ausgelegt sein muss. Zusätzlich zu den E/A-Modulen müssen die Stromversorgungsmodule auch andere allgemeine Module, wie z. B. Kommunikations- und Prozessormodule, mit Strom versorgen, diese werden also beim Design berücksichtigt. Aus Redundanzgründen müssen immer beide Stromversorgungsmodule aktiv sein und liefern normalerweise eine Standard-Ausgangsspannung von +5 V DC ohne Restwelligkeit oder Rauschen. Um die Steuerung während eines vorübergehenden Stromausfalls aufrecht zu erhalten, muss die Stromhaltezeit des +5V DC-Ausgangs sowie das Eingangsspannungsüberwachungssignal (AC ready) und das Ausgangsspannungsüberwachungssignal (DC ready) gewährleistet sein. Die Art und Weise, wie die Software unmittelbar nach einem plötzlichen Stromausfall im CPU-Modul gespeichert wird, bestimmt, wie lange die Ausgangsspannung anhält, da beide eng zusammenhängen. Neben dem Anschluss an das Stromnetz sind Dieselgeneratoren und eine Online-USV vorzusehen, um eine kontinuierliche Stromversorgung des Stromversorgungsmoduls zu gewährleisten.

**Kommunikationsinfrastruktur**

An dieser Stelle ist die Kommunikationsinfrastruktur erforderlich, um die Verbindung zwischen der Zentrale des Betreibers, den Feldleitstellen, den direkten Steuerungen und der Feldinstrumentierung zu gewährleisten, wofür in den meisten industriellen Anwendungen Netzwerke verwendet werden (Zhang, 2010). In der Regel werden Bus- oder Sterntypologien verwendet. Ethernet ist dabei das am weitesten verbreitete LAN-Protokoll (Local Area Network) in verteilten Steuerungssystemen. Es verwendet Carrier Sense Multiple Access mit Kollisionserkennung (CSMA/CD), um den Datenverkehr des Ethernet-Netzwerks bei gleichzeitigen Anforderungen zu steuern, und unterstützt Datenübertragungsraten von 10 Mbit/s. Normalerweise sind die Bedienstation und die Feldsteuerungsstationen an denselben PLS-Datenbus angeschlossen (Dey & Sen, 2020). Die FCUs und Knoten sind untereinander und mit der Bedienstation sowie mit Gateways und anderen Stationen über den Kommunikationsbus verbunden. Diese Kommunikationsinfrastruktur ermöglicht das Herunterladen von Informationen über die verschiedenen Konfigurationen einer FCS und ihrer Datenbank von der Zentralstation des Bedieners. Dies erleichtert den Konfigurationsprozess und unterstützt gleichzeitig Alarmmeldungen in umgekehrter Richtung (von der FCS zu einer Bedienstation). Die verschiedenen E/A-Module in den Knoten und der FCU der FCS sind nicht nur mit analogen und digitalen E/A-Signalen ausgestattet, sondern auch mit universellen Kommunikationsschnittstellen wie RS-232C. Innerhalb einer FCS ermöglicht der Kommunikationsbus den Informationsaustausch zwischen den FCU- oder Knoten-Racks, die ihrerseits mit anderen FCS kommunizieren, da der Rückwandbus jedes Racks mit seinen E/A-Modulen verbunden ist.

Für die Kommunikation zwischen Feldinstrumenten und Steuerungssystemen verwenden PLS-Systeme im Allgemeinen die Feldbus- und PROFIBUS-Protokolle, unterstützen aber auch weniger verbreitete Protokolle, wie z. B.: Control Network (ControlNet), INTERBUS, Controller Area Network Bus (CANbus) und DeviceNet, neben anderen Protokollen (Zhang, 2010). In einigen Fällen ist eine Fernkommunikation zwischen räumlich weit voneinander entfernten Teilen des verteilten Steuerungssystems erforderlich. Dies wird durch den Einsatz drahtloser Subsysteme erreicht. In einem PLS wird ein drahtloses Subsystem durch Ersetzen einiger Ethernet- und Verbindungsbusse durch drahtlose und Wireless-Ethernet-Verbindungen erreicht.

**Direkte Steuerungselemente**

In bestimmten Fällen, in denen Feldelemente vorhanden sind, die nicht direkt mit der FCS verbunden werden können, ist der Einsatz von PCs, SPS oder RTUs, die unter einem beliebigen Betriebssystem laufen, für deren Überwachung und Steuerung erforderlich (Zhang, 2010). In diesen Fällen liefert die Bedienerzentrale die von den direkten Steuerungselementen benötigten Regel- und Ablaufschemata und ermöglicht die Echtzeitabfrage der Feldelemente. Für den Fall, dass diese Geräte nicht direkt von den SPS-Systemen oder RTUs abgefragt werden können, kann das PLS den Datenserver eines SCADA-Systems verwenden, um mit ihnen zu kommunizieren.

**Feldinstrumentierung**

Die Feldinstrumentierung ist ein wesentlicher Bestandteil dieser Systeme. Sie besteht aus den Elementen, die letztlich mit den Maschinen und Anlagen der Produktions- und Fertigungsprozesse interagieren, die vom PLS gesteuert und überwacht werden (Dey & Sen, 2020). Diese Instrumente wandeln im Allgemeinen physikalische Parameter in analoge und digitale elektrische Signale auf der Feldebene um und bestehen aus verschiedenen Arten von Sensoren, wie z. B. Temperatur-, Durchfluss-, Druck- und Energieverbrauchssensoren, Positionsgebern, Messumformern und Aktoren, wie z. B. Schaltern, Magnetventilen und Relaisspulen (Zhang, 2010; Dey & Sen, 2020). Bei pneumatischen Stellventilen ist es erforderlich, ein Ausgangssignal der E/A-Module (Strom 4 bis 20 mA) mit Hilfe von I/P-Wandlern in ein pneumatisches Signal (0,2 bis 1 kg/cm2 ) umzuwandeln. Die folgende Abbildung zeigt ein Beispiel für ein PLS und seine Hardware-Elemente.

**PLS und seine Hardware-Elemente**

Diagram

Description automatically generated

Quelle: Rojas (2022)

Softwaremodule

Nach Zhang (2010) gehören zu den Softwaremodulen in verteilten Steuerungssystemen das History-Modul, die Steuerungsmodule und die E/A-Module.

**History-Modul**

Die Hauptaufgabe des History-Moduls ist die Speicherung aller PLS-Einstellungen, einschließlich der Einstellungen aller Standorte des überwachten Systems. Die Grafikdateien, die verwendet werden, um die Bedienkonsole und andere Systembildschirme anzuzeigen, werden ebenfalls gespeichert, zusammen mit einigen Betriebsdaten der Steuerungssysteme und der gesteuerten Systeme, die sie darstellen. Für die Speicherung aller Daten, die vom History-Modul gespeichert und verwaltet werden, sind die Datenbanken der zentralen Bedienstation zuständig.

**Steuerungsmodule**

Die Steuerungsmodule sind das Herzstück eines PLS-Systems, da sie die Ausführung der Steuerungsfunktionen in den Zielsystemen überwachen. Steuerungsalgorithmen wie einfache Arithmetik, PID-Regelung, dynamische Kompensation, Verhältnisregelung und Fuzzy-Logik sowie andere fortgeschrittene Steuerungsfunktionen werden von benutzerdefinierten Funktionsblöcken ausgeführt, die speziell in diesen Modulen untergebracht sind.

**E/A-Module**

Die E/A-Module sind für die Verwaltung der Eingangs- und Ausgangs-Subsysteme im PLS verantwortlich. Da Eingangs- und Ausgangssignale im Allgemeinen analog oder digital sind, können E/A-Module auch analog oder digital sein. Analoge E/A-Module sind für die meisten Steuerausgangssignale und Messungen von Prozessvariablen verantwortlich. Digitale E/A-Module sind zum Beispiel Start- und Stoppsignale oder Ein- und Ausschaltsignale (Zhang, 2010). Die E/A-Punkte sind in der Regel mit den Sensoren und Feldaktoren verdrahtet. Wenn jedoch intelligente Feldgeräte oder intelligente elektronische Geräte (IEDs) verwendet werden, können diese direkt mit der Bedienerzentrale kommunizieren (Gardner, 2020).

Kommunikationsmodelle

Nach Zhang (2010) verwenden verteilte Steuerungssysteme in der Regel drei Kommunikationsmodelle: das Ethernet-LAN-Modell, das OSI-Netzwerkmodell und das TCP/IP-Netzwerkmodell.

**Das Ethernet-LAN-Modell**

Der Name dieses Modells leitet sich von der gemeinsamen Verwendung von lokalen Netzwerken und Ethernet als häufigste physikalische Schicht in PLS-Systemen ab. In verteilten Steuerungssystemen wird jedoch auch Ethernet als Transportmechanismus verwendet. Ethernet-Netzwerkprotokolle werden für verschiedene Anwendungen eingesetzt. Sie können unterschiedliche Arten von Daten übertragen und werden als TCP/IP bezeichnet.

**Das OSI-Netzwerkmodell**

Dieses Modell definiert sieben Netzwerkschichten und wurde von der International Standards Organization als OSI-Modell (Open System Interconnection) für Netzwerkprotokolle und verteilte Anwendungen eingeführt.

**Das TCP/IP-Netzwerkmodell**

Das TCP/IP-Netzwerkmodell sieht im Allgemeinen weniger Ebenen vor als das OSI-Modell. Es gibt verschiedene Beschreibungen dieses Modells, aber in den meisten Fällen werden drei bis fünf Schichten unterschieden. Die Informationen, die von den Anwendungen an die physikalische Netzwerkschicht übertragen werden, bilden die TCP/IP-Struktur dieses Modells (Zhang, 2010).

Fragen zur Selbstkontrolle

1. Listen Sie die empfohlenen Inhalte für die verschiedenen Visualisierungsstufen auf

*Stufe 1: alle Informationen, die sich auf den gesamten Bereich der Bedienersteuerung beziehen*

*Stufe 2: detailliertere Informationen als auf Stufe 1*

*Stufe 3: Details zu Aufgaben, die als nicht-routinemäßig eingestuft werden*

*Stufe 4: eher diagnostisch orientiert, bietet Hilfe bei der Kontrolle und Diagnose*

1. Welches Hardware-Element gilt als das Herzstück eines PLS-Steuerungssystems?

* die zentrale Bedienerstation
* *die Feldsteuerstation*
* die Kommunikationsinfrastruktur
* die direkten Steuerungselemente

**Zusammenfassung**

Verteilte Steuerungssysteme (Prozessleitsysteme, PLS) werden als wesentlicher Bestandteil der Automatisierungstechnik angesehen. Daher ist es für das Verständnis dieses Gebietes wichtig zu wissen, wie sich die Steuerungssysteme zu den heutigen verteilten Steuerungssystemen entwickelt haben und aus welchen Komponenten sie bestehen. In diesem Zusammenhang wird im Abschnitt „Entwicklungsgeschichte der Steuerungssysteme“ beschrieben, wie sich der Automatisierungsgrad der Produktions- und Fertigungsprozesse von der einfachen über die mittlere bis hin zur Anlagen-Vollautomatisierung entwickelt hat. Besonderes Augenmerk wurde auf die Beschreibung und Darstellung der Gemeinsamkeiten und Unterschiede zwischen zentralen und verteilten Steuerungssystemen gelegt, wobei SCADA- und PLS-Systeme als Referenz dienen. Im Abschnitt „Komponenten verteilter Steuerungssysteme“ werden Hardware-Elemente, Softwaremodule und Kommunikationsmodelle als Hauptkomponenten von PLS-Systemen vorgestellt. Die Hardware-Elemente umfassen die Beschreibung der zentralen Bedienerstationen und der Feldsteuerstationen sowie der Kommunikationsinfrastruktur, der direkten Steuerungselemente und der Feldinstrumentierung. Die Softwaremodule beschreiben die Historie, die Steuerung und die E/A-Module, welche die wichtigste und am häufigsten verwendete Software innerhalb der von den PLS-Herstellern entwickelten Spezialsoftware darstellen. Schließlich werden das Ethernet-LAN-Modell, das OSI-Netzwerkmodell und das TCP/IP-Netzwerkmodell als die Kommunikationsmodelle beschrieben, die üblicherweise von verteilten Steuerungssystemen verwendet werden.

Lektion 7 – Cybersicherheit in der industriellen Automatisierung

Lernziele

Nach der Bearbeitung dieser Lektion …

… können Sie die Cybersicherheit in der industriellen Automatisierung nachvollziehen.

… sind Sie mit Anlagensteuerungsnetzwerken und deren Komponenten vertraut.

… können Sie zwischen den Begriffen Cyber-Bedrohung und Cyber-Angriff unterscheiden.

… erkennen Sie die üblichen Schwachstellen industrieller Software.

7. Cyber-Sicherheit in der industriellen Automatisierung

Einführung

Computer und Kommunikationsnetzwerke sind ein wesentlicher Bestandteil der industriellen Automatisierung von Produktions- und Fertigungsprozessen. Sie steuern einen Großteil der industriellen Steuerungssysteme. Ein großer Teil dieser Computer und insbesondere die Netzwerke müssen ihrerseits mit ihrer Umgebung oder dem Cyberspace in Verbindung stehen, um Geschäftsaufgaben zu erfüllen und mit Kund:innen und Lieferanten in Kontakt zu bleiben. Daher sind diese Netzwerke nicht frei von Bedrohungen oder Cyber-Angriffen, was der Cyber-Sicherheit in der Automatisierungstechnik einen sehr hohen Stellenwert einräumt. Diese Lektion bietet eine kurze Einführung in das Thema Cybersicherheit in der industriellen Automatisierung. Sie beginnt mit dem Anlagensteuerungsnetzwerk und seiner Beziehung zur Cybersicherheit, erklärt dann kurz, worum es bei Cyber-Angriffen geht, und stellt schließlich einige häufige Schwachstellen in industrieller Software vor.

7.1 Anlagensteuerungsnetzwerk

Wenn wir an ein industrielles Automatisierungssystem und sein Anlagensteuerungsnetzwerk oder industrielles Steuerungssystem denken, finden wir Systeme, die große Fertigungs- und Produktionssysteme überwachen, steuern und verwalten. Dazu gehören das Supervisory Control and Data Acquisition System (SCADA), das Prozesssteuerungssystem und das Prozessleitsystem (PLS) (Macaulay & Singer, 2011; Kott et al., 2016; Gardner, 2020). Andere industrielle Steuerungssysteme wie Energiemanagementsysteme, Sicherheitssysteme und Gebäudeautomatisierungssysteme werden ebenfalls häufig dieser Liste hinzugefügt, da es sich um spezialisierte Systeme handelt, die unter anderem von den oben genannten Systemen abgeleitet sind (Sullivan et al., 2016). Anlagensteuerungsnetzwerke als Teil von cyber-physischen Systemen (CPS) und die meisten ihrer Komponenten sind zur Wartung, Verwaltung und Steuerung der Anlagensoftware über industrielle Kommunikationsnetze miteinander verbunden und stellen ihrerseits eine Verbindung zum Internet her, was sie anfällig für Cyber-Angriffe macht.

Funktionelle Komponenten von Anlagensteuerungsnetzwerken

Nach Sullivan et al. (2016) Nach Sullivan sind die wichtigsten funktionalen Komponenten von Anlagensteuerungsnetzwerken diejenigen, die direkt mit der Steuerung in Verbindung stehen, diejenigen, die mit dem Bediener als menschliche Komponente interagieren, diejenigen, die die Verbindung und Kommunikation zwischen ihnen ermöglichen und diejenigen, die physisch mit dem Prozess interagieren. Diese Komponenten sind unten aufgeführt:

**Speicherprogrammierbare Steuerungen (SPS)**

Seit ihren Anfängen sind speicherprogrammierbare Steuerungen mit ihren diskreten Logikkomponenten und ihren Verstärkern ein grundlegender Bestandteil der Automatisierung von Industriesystemen und Anlagensteuerungsnetzwerken gewesen. Speicherprogrammierbare Steuerungen sind heute in ihrer Gesamtheit als kompakte elektronische Geräte aufgebaut, die von Mikroprozessoren gesteuert werden. Sie nehmen die Messwerte der Sensoren als Eingangssignale entgegen, um sie an die Überwachungssysteme zu senden oder die programmierten Anweisungen zur Berechnung der Steuerungsaktion auszuführen und über die Ausgangssignale die Bewegung der Aktoren oder die Änderung der Schaltkonfiguration zu steuern (Sullivan et al., 2016).

**Fernwirkeinheiten (RTU)**

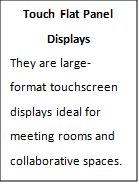
Diese mikroprozessorgesteuerten elektronischen Komponenten erfüllen ihre Funktion in rauen Umgebungen, in denen sie unter anderem elektromagnetischen Feldern, hohen Temperaturen oder Vibrationen ausgesetzt sind. Es gibt im Allgemeinen zwei Arten von RTUs: Feld-RTUs und Stations-RTUs. Feld-RTUs empfangen auch Eingangssignale von Feldgeräten und Sensoren, die dann von einer programmierten Logik verarbeitet werden. Heute ähneln diese Geräte speicherprogrammierbaren Steuerungen (Sullivan et al., 2016).

**Intelligente elektronische Geräte (IED)**

Diese Geräte bilden zusammen mit SPS-Systemen und RTUs die drei grundlegenden Arten von Steuerungen in Anlagensteuerungsnetzwerken. IEDs enthalten in der Regel einen oder mehrere Prozessoren und sind in der Lage, Daten von externen Quellen wie anderen Feldgeräten oder Sensoren zu empfangen und Steuersignale an digitale Schalter oder Relais mit Kommunikationsfunktionen zu senden (Sullivan et al., 2016).

**Bediener- oder Engineering-Workstations**

Diese Workstations können nicht nur Überwachungs- und Steuerungsaufgaben übernehmen, sondern sind auch für das Hosting der Programmiersoftware für Steuerungen und andere Anwendungen auf den Anlagensteuerungsnetzwerken zuständig. In ihnen können Techniker die notwendigen Änderungen in der Logik der Steuerungen sowie in den industriellen Anwendungen vornehmen. Es handelt sich dabei in der Regel um robuste Server oder Desktop-Computer mit Standard-Betriebssystemen, die mit industrieller Software von bewährter Qualität geladen sind (Sullivan et al., 2016).

**Mensch-Maschine-Schnittstelle**

Mensch-Maschine-Schnittstellen (HMI) sind Teil von Workstation-Softwareanwendungen, die aktuelles Wissen über automatisierte Produktions- und Fertigungsprozesse vermitteln sollen. Die Informationen, die sie verarbeiten, um sie dem Benutzer zu präsentieren, bestehen in der Regel aus Trends der interessierenden Variablen, Prozesswerten und Alarmen. Eine HMI kann auf einer Vielzahl von Plattformen laufen, von Smartphones über Tablet-PCs, Laptops und Desktops bis hin zu Workstations und speziellen **Touch-Flachbildschirmen** (Sullivan et al., 2016).

**Daten-Historian**

Ein Daten-Historian ist auch ein Teil von Workstation-Softwareanwendungen, deren Aufgabe es ist, Daten aus automatisierten Produktions- und Fertigungsprozessen in Echtzeit zu sammeln und sie in einer historischen Datenbank für die nachträgliche und/oder gleichzeitige Analyse zu speichern. Es ist zu beachten, dass die im Daten-Historian gespeicherten Daten in der Regel dieselben sind, die auch in der HMI angezeigt werden, mit dem Unterschied, dass jeder dieser Datenpunkte mit einer Angabe des Zeitpunkts, zu dem er auftrat, für seine jeweilige Speicherung verbunden ist (Sullivan et al., 2016).

**Kommunikationsgateways**

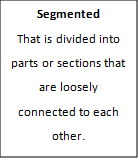
Die Funktion eines Kommunikationsgateways besteht darin, den Austausch von Informationen zwischen zwei Geräten mit unterschiedlichen Kommunikations- oder Transportprotokollen zu ermöglichen. Nachdem die Daten, die von einem sendenden System kommen, durch dieses Gerät konvertiert wurden, bleiben die resultierenden Daten vollständig kompatibel mit dem Übertragungsmedium und dem Protokoll des empfangenden Hosts. Ein typisches Beispiel ist die Konvertierung von OPC-Nachrichten über Ethernet in Modbus-Nachrichten für eine serielle Verbindung unter Verwendung der empfohlenen Standards RS-232 oder RS-485 (Sullivan et al., 2016).

**Front-End-Prozessor (FEP)**

Ein Front-End-Prozessor wird normalerweise verwendet, wenn Informationen über den Status verschiedener RTUs oder IEDs von einem Leitwarten-Host oder dessen Stations-HMI abgefragt werden müssen. Dieser Kommunikationsprozessor macht die Auswirkungen von Latenzen und Verarbeitungszeiten, die durch die Kommunikationsnetzwerkverbindungen entstehen, für den Benutzer transparent, so dass sie die Steuerungsfunktionen, die der Anlagenbediener an der Leitwarte ausführt, nicht beeinträchtigen. Wenn es darüber hinaus notwendig ist, Informationen von proprietären Protokollen des Anbieters in offene Standardprotokolle umzuwandeln, kann der FEP als Kommunikationsgateway fungieren (Sullivan et al., 2016).

**Prozesssteuerungsnetzwerk – Feldgeräte**

Geräte, die an digitale oder analoge E/A-Module zur direkten Interaktion mit einer der drei oben genannten Steuerungen angeschlossen sind, werden als Feldgeräte betrachtet; Sensoren, Aktoren, Messwandler und Maschinen sind Teil dieser Kategorie. Intelligente Geräte, die industrielle Kommunikationsprotokolle wie PROFIBUS oder Modbus für den Informationsaustausch mit der Steuerung verwenden, fallen ebenfalls in diese Kategorie (Sullivan et al., 2016).

Im Allgemeinen können Prozesssteuerungsnetzwerke von sehr einfachen Systemen bis hin zu sehr komplexen Systemen reichen. Große Prozesssteuerungsnetzwerke können komplexe Prozesse in Echtzeit steuern, die über verschiedene geografische Regionen verteilt sein und eine große Anzahl von Komponenten umfassen können (Kott et al., 2016). Aufgrund der Vielfalt der Anforderungen und Geräte müssen diese Systeme oft in mehrere Betriebszonen **segmentiert** werden. Die Anforderungen und Eigenschaften sind für jedes Einsatzgebiet einzigartig. Unter dem Gesichtspunkt der Cybersicherheit unterscheidet die Segmentierung von Prozesssteuerungsnetzwerken drei stark differenzierte Bereiche:

* + die Feldzone,
  + die Steuerungszone und
  + die Unternehmenszone.

Die Feldzone kann als Anlagen-, Prozess- oder Betriebszone betrachtet werden, da sie die cyber-physischen Systeme beherbergt und die Netzwerke und Geräte der Betriebstechnik (Operational Technology, OT) umfasst, die für die Automatisierung und Steuerung verantwortlich sind. Die Geräte in dieser Zone verfügen in der Regel über begrenzte Rechenressourcen, wie z. B. SPS und RTUs. Dabei handelt es sich um integrierte Geräte für einen bestimmten Zweck. Die Kommunikationsnetzwerke in diesem Bereich verwenden eine Vielzahl von physikalischen Schnittstellen und industriellen Protokollen, wodurch sie sehr vielfältig sind und über IP-Netzwerke hinausgehen. Die Anforderungen an die Synchronisierung, Zuverlässigkeit und Sicherheit von Netzwerken und Geräten in der Feldzone sind sehr hoch, so dass IT-basierte Cyber-Sicherheitslösungen nur selten zum Einsatz kommen (Kott et al., 2016).

Die Steuerungszone umfasst die Leitwartenstandorte und die verteilten Steuerungskomponenten des SCADA-Systems, also weitestgehend Betriebstechnik. In der Steuerungszone werden einige IP-basierte Netzwerke eingesetzt. Die Anforderungen an Sicherheit und Zuverlässigkeit sind jedoch strenger und anspruchsvoller als die, die normalerweise an die IT gestellt werden. Die Netzwerke in der Steuerungszone unterliegen in der Regel strengen zeitlichen Beschränkungen und die Geräte werden nicht sehr häufig aktualisiert, so dass nur wenige IT-basierte Cyber-Sicherheitslösungen direkt in dieser Zone eingesetzt werden können (Kott et al., 2016).

Die Unternehmenszone umfasst eine Vielzahl von ständig aktualisierten und sich schnell entwickelnden Endgeräten, die in IT-basierte Unternehmenssysteme und Unternehmensnetzwerke eingebettet sind. Diese Unternehmensnetzwerke sind in der Regel mit externen Netzwerken und dem Internet verbunden und basieren üblicherweise auf dem IP-Protokoll. Die operativen Netzwerke, die in den anderen Zonen eingesetzt werden, sind meist strategisch von diesen kommerziellen Netzwerken getrennt. Herkömmliche IT-Umgebungen außerhalb von Prozesssteuerungsnetzwerken und der Unternehmenszone sind sich sehr ähnlich, so dass viele IT-spezifische Cyber-Sicherheitslösungen direkt in diese Zone gelangen (Kott et al., 2016).

Der entscheidende Unterschied wird deutlich, wenn man sich auf die Überwachung und Steuerung der physischen Prozesse der Prozesssteuerungsnetzwerke konzentriert, die von der Betriebstechnik verwendet werden (Hahn, 2016). Es liegt auf der Hand, dass die Unterstützung bestimmter physischer Prozesse durch den OT-Ansatz erhebliche Unterschiede in der Art und Weise mit sich bringt, wie die Systeme betrieben und verwaltet werden. Dies steht im Gegensatz zum IT-Ansatz, ebenso wie die Technologien, die in jedem Fall zur Unterstützung eingesetzt werden. Um die Herausforderungen des Schutzes eines Prozesssteuerungsnetzwerkes zu verstehen, ist es wichtig, die Hauptunterschiede zwischen IT und OT zu kennen, insbesondere da Cyber-Sicherheitsansätze, die ursprünglich für IT entwickelt wurden, nun teilweise auch auf Prozesssteuerungsnetzwerke anwendbar sind. Im Gegensatz dazu gibt es im Bereich der OT häufig zusätzliche betriebliche, technologische und administrative Einschränkungen, die zu einem schwierigeren Umfeld für die Cyber-Sicherheit führen.

Fragen zur Selbstkontrolle

1. Bitte geben Sie an, ob die folgenden Aussagen richtig oder falsch sind.

* Es gibt in der Regel zwei Arten von Fernwirkeinheiten. *Richtig*
* Ein Daten-Historian verwendet einen anderen Datensatz als den, der vom HMI angezeigt wird. *Falsch*
* Engineering-Workstations sind für das Hosting der Programmiersoftware für Steuergeräte zuständig. *Richtig*
* Kommunikationsgateways sind zusammen mit SPS-Systemen und RTUs die drei grundlegenden Arten von Steuergeräten in Prozesssteuerungsnetzwerken. *Falsch*

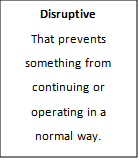
1. Bitte vervollständigen Sie die folgenden Sätze.

Speicherprogrammierbare Steuerungen sind heute in ihrer Gesamtheit als kompakte *elektronische* Geräte *aufgebaut*, die von *Mikroprozessoren* gesteuert werden.

Mensch-Maschine-Schnittstellen sind Teil von Workstation-*Softwareanwendungen*, die *aktuelles Wissen* über automatisierte Produktions- und Fertigungsprozesse vermitteln sollen.

7.2 Cyber-Angriffe

In unserer zunehmend von elektronischen Technologien abhängigen Welt stellt der Schutz von Computersystemen und ihren Daten vor Cyber-Angriffen eine große Herausforderung dar (Li & Liu, 2021). Wenn sich Cyber-Angriffe gegen Unternehmen richten, zielen sie in der Regel auf finanziellen Schaden ab, in anderen Fällen können aber auch politische oder militärische Motive hinter Cyber-Angriffen stecken. An dieser Stelle ist es wichtig, zwischen zwei Begriffen zu unterscheiden, die im Bereich der Cyber-Sicherheit verwendet werden: Cyber-Bedrohung und Cyber-Angriff. Während es sich bei der Cyber-Bedrohung um ein mögliches Sicherheitsrisiko handelt, bei dem eine Schwachstelle in einem Cyber-System oder -Gerät ausgenutzt werden kann, handelt es sich bei einem Cyber-Angriff um eine vorsätzliche, unbefugte Handlung, die an einem Cyber-System oder -Gerät vorgenommen wird. Weiter gefasste Definitionen finden sich an vielen Stellen, wie z. B. bei Li und Liu (2021, p. 8278):

Eine Cyber-Bedrohung ist „jedes Ereignis, das geeignet ist, Missionen, Aufgaben, Bilder, nationale Cyber-Assets oder Personal über ein Informationssystem durch unbefugten Zugang, Zerstörung, Offenlegung, Veränderung von Informationen und/oder Behinderung (**disruptive**) der Bereitstellung von Diensten zu beeinträchtigen“. Andererseits wird „jede unbefugte Cyber-Handlung, die darauf abzielt, die Sicherheitsrichtlinien eines Cyber-Assets zu verletzen und die Dienste oder den Zugang zu Informationen dieses nationalen Cyber-Assets zu beschädigen, zu stören oder zu unterbrechen, als Cyber-Angriff bezeichnet. Der vorsätzliche Einsatz einer Cyber-Waffe gegen ein Informationssystem in einer Weise, die einen Cyber-Vorfall verursacht, wird ebenfalls als Cyber-Angriff betrachtet“.

Nach Mahesh Parahar (2022) lassen sich die Hauptunterschiede zwischen Bedrohung und Angriff anhand der folgenden Stichworte festmachen:

* + Basierend auf der Absicht: Es gibt unbeabsichtigte Bedrohungen wie z. B. Naturkatastrophen. Menschliche Fahrlässigkeit wird jedoch als absichtliche Bedrohung angesehen. Die Angreifer:innen ihrerseits haben in der Regel ein Motiv und organisieren daher den Angriff, d. h. der Angriff ist eine absichtlich durchgeführte Operation.
  + In Abhängigkeit von der Böswilligkeit: Bedrohungen werden als böswillig oder nicht böswillig eingestuft, während Angriffe immer böswillig sind.
  + Basierend auf der Definition: Während Bedrohungen per Definition Umstände oder Bedingungen sind, die das System oder seine Produktion schädigen können, sind Angriffe als vorsätzliche Handlungen definiert, die das System oder seine Produktion schädigen.
  + In Abhängigkeit von der Wahrscheinlichkeit eines Schadens: Die Wahrscheinlichkeit, dass Informationen aufgrund einer Bedrohung beschädigt oder verändert werden, kann von gering bis sehr hoch sein, während die Wahrscheinlichkeit, dass Informationen aufgrund eines Angriffs beschädigt oder verändert werden, sehr hoch ist.
  + Bezüglich der Erkennung: Angriffe sind relativ leicht zu erkennen, verglichen mit Bedrohungen, die im Allgemeinen schwer zu erkennen sind.
  + In Bezug auf die Prävention: Es wird davon ausgegangen, dass die Kontrolle von Schwachstellen Bedrohungen verhindern kann, dass dies aber nicht ausreicht, um einen Angriff zu verhindern. Zur Bewältigung eines Cyber-Angriffs sind neben der Kontrolle der Schwachstellen weitere Maßnahmen erforderlich, wie z. B. Erkennung und Reaktion, Erstellung von Sicherungskopien und vieles mehr.
  + Bezüglich der Initiierung: Während Bedrohungen in der Regel vom System oder von einem Dritten ausgehen, werden Angriffe in ihrer Gesamtheit von einem Außenstehenden, sei es ein:e Benutzer:in oder ein System, initiiert (Parahar, 2022).

Akteure, die Prozesssteuerungsnetzwerke bedrohen

Obwohl klargestellt wurde, dass es Unterschiede zwischen Prozesssteuerungsnetzwerken und IT-Netzwerken gibt, da Prozesssteuerungsnetzwerke in der Regel Betriebstechnik enthalten, sind einige Autoren wie Macaulay & Singer (2011) der Ansicht, dass die Bedrohungsfaktoren für Prozesssteuerungsnetzwerke und IT-Netzwerke ähnlich sind. Sie gehen sogar so weit zu sagen, dass der Unterschied für sie darin besteht, dass die Wahrscheinlichkeit eines direkten Angriffs bei den Prozesssteuerungsnetzwerken geringer ist, auch wenn sie ihn nicht ausschließen, und dass sie ihrer Meinung nach nur Kollateralschäden oder einen Zufallstreffer erleiden könnten. Nach ihrer Analyse identifizieren und klassifizieren sie die Akteure, die das Prozesssteuerungsnetzwerk bedrohen, wie folgt:

**Professionelle Bot-Herder**

Professionelle Bot-Herder sind Malware-Großhändler, die sich der Entwicklung und dem Management von Bots widmen und diese zu kommerziellen Zwecken an andere Bedrohungsakteure vermieten. Ihr Hauptziel ist es, die Kontrolle über die kybernetischen Geräte zu erlangen, um sie bei Bedarf wiederzuverwenden und die Bot-Herden zu vermieten oder zu verkaufen, wenn möglich an jeden der anderen Akteure.

**Spammer**

So werden im Allgemeinen die Spezialisten genannt, die sich Zugang zu sozialen Netzwerken, Webmail-Anbietern, Blogs, Websites und allen anderen möglichen Quellen verschaffen, um legitime E-Mail-Adressen zu sammeln. Diese Täter verschicken unerwünschte E-Mails (Spam) an riesige Adresslisten, die sowohl mit echten als auch mit zufälligen oder erratenen Adressen erstellt werden. Ihr vorrangiges Ziel ist es, potenzielle Käufer von (halb)legitimen Produkten wie natürlichen oder biologischen Behandlungen zu erreichen und sie betrügerischen Transaktionen wie dem Verkauf gestohlener Waren, Schneeballsystemen oder Identitätsdiebstahl auszusetzen.

**Organisiertes Verbrechen**

Damit sind kriminelle Vereinigungen und Banden gemeint, die in der Regel in Kredit- und Scheckkartenbetrug verwickelt sind. Sie mussten auf der Suche nach höheren Gewinnen in andere Gebiete ausweichen, nachdem sie entdeckt hatten, dass die heutige chipbasierte Technologie sie dazu zwang, online zu gehen. Ihr primäres Ziel ist es, neben einer Vielzahl anderer Betrugsformen an persönliche Bank- oder Identitätsdaten zu gelangen, sei es zum Zwecke des Identitätsdiebstahls oder des Diebstahls von Bankkonten.

**Wirtschaftsspionage**

Wirtschaftsspionage wird von skrupellosen Unternehmen betrieben, die es auf bestimmte Unternehmenswerte und Branchen abgesehen haben. Dabei handelt es sich in erster Linie um Informationen über die Produktion und die Finanzen, das geistige Eigentum sowie die Geschäftsstrategien und -pläne der betreffenden Branche.

**Phisher**

Bei Phishern handelt es sich um Personen, die in Zusammenarbeit mit Spammern versuchen, einzelne Benutzer:innen auf Websites zu locken, die mit schädlicher Software infiziert sind. Sobald sie mit der Website verbunden sind, hacken sie sich in die Geräte der Benutzer:innen und verwandeln sie in Bots oder verschaffen sich Zugang zu deren Inhalten. Ihr oberstes Ziel ist Identitätsdiebstahl und individueller Betrug, entweder um sich Zugang zu öffentlichen Einrichtungen zu verschaffen, um an nationale Sicherheitsgüter zu gelangen, oder um Wirtschaftsspionage zu betreiben, wie oben beschrieben.

**Nachrichtendienste (fremder Staaten oder Nationen)**

Nachrichtendienste sind Einrichtungen oder möglicherweise Paramilitärs, die im Auftrag des Staates in der Regel von bestimmten geografischen Regionen oder Cyber-Netzwerken aus tätig sind. Ihr vorrangiges Ziel besteht in der Regel darin, die Pläne, Strategien und Geheimnisse einer Nation in Erfahrung zu bringen, in diesem Fall die Pläne, Strategien und Geheimnisse der Industrie.

**Aktivisten und Terroristen**

Ideologisch motivierte Akteure werden als Aktivisten und Terroristen angesehen, die in der Regel nicht über ausreichende Ressourcen verfügen, um selbst Exploits zu entwickeln, die aber mit den ihnen zur Verfügung stehenden Ressourcen die von den Herdern entwickelten Exploit-Kits (von der Stange) kaufen oder kompromittierte Geräte von ihnen mieten können. Ihr Ziel ist die Erlangung von Geheimnissen der nationalen Sicherheit, Strategie oder Planung durch industrielle Sabotage von physischen und logischen Anlagen sowie von öffentlichen, militärischen und Regierungseinrichtungen.

Hacker und Malware

Gardner (2021) argumentiert, dass externe Bedrohungen wie Hacker Malware entwickelt haben, die Computersysteme kompromittiert, wie z. B. Ransomware, die für katastrophale und schädliche Zwecke oder zur illegalen finanziellen Bereicherung eingesetzt wird. Die Havex-Malware und die Dragonfly-Hackergruppe sind bekannte Beispiele für Angriffe auf Infrastrukturen in Europa und den USA, die Automatisierungs- und Steuerungssysteme, Stromnetze und einige energiebezogene Branchen betrafen. Die Havex-Malware ermöglicht Hackern den Fernzugriff auf Computer oder Server über eine Hintertür, die als RAT bekannt ist. Die Sicherheit kann beeinträchtigt werden, lebenswichtige Infrastrukturen können lahmgelegt werden und Geräte können sogar durch Schadsoftware dieser Hackergruppen zerstört werden. Hacker laufen in der Regel kaum Gefahr, bestraft oder entdeckt zu werden. Dies gilt sowohl für Einzelpersonen als auch für staatlich unterstützte Hackergruppen. Zu den Bedrohungsquellen gehören neben den von Macaulay und Singer (2011) beschriebenen auch Malware, Spyware, Eindringlinge, aber auch ungeschulte Bediener:innen und Benutzer:innen. Eines der bekanntesten Beispiele für eine Sicherheitsverletzung in einem Prozesssteuerungsnetzwerk ist der Cyber-Angriff auf die Anreicherungsanlage für Kernbrennstoff in Natanz im Iran im Jahr 2010. Der Erfolg dieses Cyber-Angriffs beruhte auf der israelischen Malware Stuxnet, einem Wurmvirus, der offenbar über einen USB-Stick in das System gelangte und sich dann über vertrauenswürdige Netzwerke verbreitete. Stuxnet verursachte Über-, Unter- und Überdruckschwankungen, während im Kontrollraum normale Werte angezeigt wurden. Dadurch wurden etwa 1.000 Zentrifugen beschädigt und die Urananreicherung für mehrere Jahre unterbrochen.

Neben Havex und Stutnex sind Industroyer, BlackEnergy und TRITON/TRISS als Beispiele für Malware bekannt, die speziell auf Prozesssteuerungsnetzwerke abzielt (Gardner, 2020). Diese Bedrohungen sind nicht nur unangenehm, da sie nicht nur die individuelle oder nationale Sicherheit beeinträchtigen, sondern auch zu einer großflächigen, langfristigen militärischen Verwundbarkeit führen oder kritische Infrastrukturen stören können. So wurde beispielsweise vermutet, dass die Industroyer-Attacke, bei der 20 Prozent der Stadt Kiew in der Ukraine für eine Stunde ohne Strom waren, nur ein groß angelegter Test dieser Malware war. Mögliche Vorgehensweisen von Hackern sind z. B:

* + Kontrolle über die Steuerungs- und Regelungskomponenten des Prozesssteuerungsnetzwerks durch Eindringen in eine undokumentierte Hintertür oder ein undokumentiertes Portal, das häufig für die Inspektion oder Wartung der Software zur Verfügung steht,
  + Schaffung einer einfachen Möglichkeit, erneut Zugang zu erlangen, falls die ursprüngliche Hintertür für den Angreifer geschlossen wird, indem zusätzliche Hintertüren mit Hilfe eines Remote Access Trojaners (RAT) eingerichtet werden,
  + Gleichzeitig wird der Arbeitsprozess des Prozesssteuerungsnetzwerks gestört, indem ausführbare Dateien verarbeitet werden, die den Nutzlastteil der Malware starten, z. B. indem die Daten auf allen anfälligen Knoten des Prozesssteuerungsnetzwerks zu einem bestimmten Datum und einer bestimmten Uhrzeit gelöscht werden. Malware-Nutzlasten für Prozesssteuerungsnetzwerke führen in der Regel zu einer Unterbrechung der Kommunikationssysteme und der Datenübertragung in Verbindung mit HMI-Geräten und SCADA-Systemen.
  + Verhinderung des Systemstarts oder der Systemwiederherstellung durch Löschen kritischer Systemdaten wie z. B. Registrierungsschlüssel.

Unabhängig davon, ob es sich um eine Cyber-Bedrohung oder einen Cyber-Angriff handelt und ob der informationstechnische oder der betriebstechnische Teil betroffen ist – wichtig ist, dass die Cyber-Sicherheit des Prozesssteuerungsnetzwerks gefährdet ist.

Fragen zur Selbstkontrolle

1. Bitte nennen Sie vier Arten von Akteuren, die die Prozesssteuerungsnetzwerke bedrohen

*professionelle Bot-Herder*

*Spammer*

*organisiertes Verbrechen*

*Wirtschaftsspionage*

*Phisher*

*Nachrichtendienste*

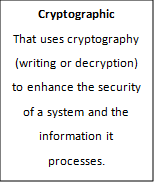
*Aktivisten und Terroristen*

1. Bitte geben Sie an, ob die folgenden Aussagen richtig oder falsch sind.

* Der Angriff ist eine Operation, die ohne Absicht durchgeführt wird. *Falsch*
* Bedrohungen sind definiert als vorsätzliche Handlungen, die dem System oder seiner Produktion Schaden zufügen. *Falsch*
* Die Wahrscheinlichkeit, dass Informationen durch eine Bedrohung beschädigt werden, kann von gering bis sehr hoch variieren. *Richtig*
* Angriffe sind im Vergleich zu Bedrohungen relativ leicht zu erkennen. *Richtig*

7.3 Häufige Schwachstellen industrieller Software

Bei der Untersuchung der Cyber-Sicherheitsschwachstellen von industriellen Steuerungssystemen (ICS) oder Prozesssteuerungsnetzwerken wurden drei häufige Bereiche für Schwachstellen identifiziert: Software, Konfiguration und Netzwerke (Nelson & Chaffin, 2011). In diesem Abschnitt werden nur häufige Schwachstellen industrieller Software vorgestellt. Im Gegensatz zu typischen Computersystemen verwenden ICS keine IT-Software von der Stange, sondern kundenspezifische Software, die nicht auf die gleiche Weise oder mit der gleichen Häufigkeit getestet wird wie herkömmliche IT-Produkte. Laut Nelson und Chaffin (2011) mangelt es bei der Entwicklung und Programmierung von ICS-Software an bewährten Sicherheitsverfahren. Ihre Studie basiert auf den Sicherheitsbewertungen des Control Systems Security Program (CSSP) der National Cyber Security Division des US Department of Homeland Security (DHS), den ICS-CERT-Operationen und den Bewertungen des Cyber Security Assessment Tool (CSET) für ICS. Sie identifizierten neun Kategorien von Schwachstellen in industrieller Software, nämlich:

* + unzureichende Eingabeüberprüfung
  + mangelhafte Codequalität
  + Berechtigungen, Privilegien und Zugriffskontrollen
  + unzureichende Authentifizierung
  + unzureichende Überprüfung der Authentizität von Daten
  + **kryptografische** Probleme
  + Anmeldeinformationsverwaltung
  + Konfiguration und Wartung (Entwicklung) der ICS-Software-Sicherheit

Unzureichende Eingabeüberprüfung

Die Eingabeüberprüfung ist eine Technik, die verhindern soll, dass Eindringlinge durch Eingaben in das System Zugang zu bestimmten Funktionen erhalten oder ihre Berechtigungen erweitern können. Wenn diese Überprüfung jedoch nicht korrekt durchgeführt wird, kann der Kontrollfluss des Programms verändert werden (Upadhyay, & Sampalli, 2020). Die häufigsten Schwachstellen in dieser Kategorie sind die folgenden:

**Pufferüberlauf**

Wenn ein laufendes Programm versucht, mehr Daten in einen Puffer zu schreiben, als im Speicher reserviert sind, kommt es zu einem sogenannten Pufferüberlauf (Nelson & Chaffin, 2011). Dies kann zu abnormalem Programmverhalten führen, da der an den Puffer angrenzende Speicher durch die zusätzlichen Eingabedaten überschrieben wird. Der Angreifer nutzt diese Schwachstelle in der Regel so aus, dass gültiger Code im kompromittierten Bereich überschrieben wird, was bei erfolgreicher Ausführung dazu führt, dass das Programm die vom Angreifer geplanten Aufgaben mit seinen versteckten Zielen ausführt.

**Fehlende Überprüfung von Array-Grenzen**

Die Größe eines Arrays, das von Computerprogrammen verwendet wird, ist begrenzt, ebenso wie der Speicherplatz, der für seine Speicherung reserviert ist. Die Array-Indexwerte müssen in einem bestimmten Bereich liegen, der vom Programm bestätigt werden muss. Wenn das Programm nicht bestätigt, dass diese Werte innerhalb des angegebenen Bereichs liegen, liegt eine fehlende Grenzwertprüfung vor, die in den meisten Fällen zu einer unerwarteten Reaktion führt (Nelson & Chaffin, 2011). Beispielsweise kann das System abstürzen, wenn Werte für einen Array-Index eingegeben werden, die ungültige, zu große oder negative Zahlen enthalten.

**Command Injection**

Gelingt es dem Angreifer, eigene Befehle einzufügen, die nichts mit dem auszuführenden Originalcode zu tun haben, indem er ein Begrenzungszeichen (Startzeichen für einen neuen Befehl und Ende des vorherigen Befehls) wie z.B. ein Komma, einen Punkt oder ein Semikolon einfügt, so liegt eine Command Injection (dt. Befehlsinjektion) vor (Nelson & Chaffin, 2011). Auf diese Weise gelingt es dem Angreifer, beliebige Befehle und Codes auszuführen. Diese Schwachstellen treten in der Regel in folgenden Fällen auf:

1. Unzuverlässige Quellen liefern die Daten an die Anwendung.
2. Die von der Anwendung ausgeführten Befehle werden in Form einer Zeichenkette übergeben, die auch die Daten enthält.
3. Der Angreifer erhält Kapazitäten oder Berechtigungen, die ihm nicht zustehen, wenn er den Befehl erfolgreich ausführt.

ICS-Anwendungen sind in der Regel für zwei Arten von Befehlsinjektionen anfällig: die Injektion von SQL-Befehlen (Structured Consultation Language) und die Injektion von Betriebssystembefehlen (OS), wobei die erste Art die häufigere ist.

Datenbankgesteuerte Websites lassen oft die SQL-Command-Injection zu. Generell kann jede Anwendung oder Website mit einer geringen Benutzerzahl zum Ziel solcher Angriffe werden, da sie eine Schwachstelle darstellen, die leicht zu entdecken und auszunutzen ist. SQL unterscheidet nicht effektiv zwischen der Daten- und der Steuerungsebene, was die Hauptfehlerquelle darstellt.

Wenn externe Einträge, die nicht ordnungsgemäß bereinigt wurden, zur Erstellung von Betriebssystembefehlen verwendet werden, sind ICS-Anwendungen, die diese Befehle ausführen, anfällig für die Injektion von Betriebssystembefehlen.

**Cross-Site Scripting**

Wenn anfällige Webanwendungen Webseiten erzeugen, über die Angreifer:innen Schadcode einschleusen können, liegt eine Cross-Site-Scripting-Schwachstelle (XSS-Schwachstelle) vor (Nelson & Chaffin, 2011). Diese Sicherheitslücke ermöglicht die Ausführung von Angriffscode auf dem Web-Client, aber mit Server-Rechten.

Wie bei der SQL-Injection sind mangelhaft bereinigte Daten die Hauptursache für die XSS-Schwachstelle. Der große Unterschied besteht jedoch darin, dass bei einem XSS-Angriff die betroffene Webanwendung das bösartige Skript an den Benutzer weiterleitet, ohne dass dieser es bemerkt.

In der Regel gibt die Website das bösartige Skript, das der Angreifer in einen Link eingeschleust hat, an das Opfer zurück, als wäre es legitim. Unter Ausnutzung einiger der zahlreichen Schwachstellen des Webbrowsers könnte der Computer des Opfers kompromittiert werden, da das bösartige Skript als gültig ausgeführt wird, weil es vom Server stammt. Im Allgemeinen basieren XSS-Angriffe auf der Interaktion mit dem Benutzer, indem dieser dazu verleitet wird, auf einen Link zu klicken. Dabei wird das Vertrauen des Benutzers in eine anerkannte Institution oder ein Unternehmen mit gutem Ruf ausgenutzt.

Der häufigste XSS-Angriff ist die Offenlegung von Informationen, die in Benutzer-Cookies gespeichert sind. Das bösartige Skript hat Zugang zu denselben Cookies wie das auszuführende Skript, das von der betreffenden Website angefordert wird.

**Unzulängliche Einschränkung eines Pfadnamens auf ein eingeschränktes Verzeichnis (Directory Traversal)**

Schwachstellen durch Directory Traversal entstehen, wenn Dateipfade nicht überprüft werden (Nelson & Chaffin, 2011). Diese Art von Schwachstelle kann in allen Arten von Anwendungen auftreten, obwohl sie in der Regel mit Webanwendungen verbunden ist. Wenn Software auf eine Datei oder ein Verzeichnis unterhalb eines eingeschränkten Elternverzeichnisses zugreifen muss, und zwar über einen Pfadnamen oder eine durch externe Eingabe erzeugte Kennung, treten häufig sogenannte Directory Traversals auf. Der Pfadname kann auf einen Ort außerhalb des eingeschränkten Verzeichnisses verweisen, wenn die Software bestimmte Elemente innerhalb des Namens nicht ordnungsgemäß deaktiviert.

Kritische Dateien wie wichtige Daten, Bibliotheken oder Programme könnten vom Angreifer erstellt, gelesen oder überschrieben werden, was es ihm ermöglicht:

* + nicht autorisierte Befehle oder Code auszuführen
  + Verzeichnisse oder Dateien zu ändern oder zu lesen
  + Denial-of-Service (DoS) kann durch das Neustarten, Beenden oder Abstürzen wichtiger Programme oder Dateien verursacht werden.

Upadhyay & Sampalli (2020) stellten anhand von Statistiken aus der Common Vulnerability Exposures Database (CWE, zugänglich über die CWE-Website) fest, dass von den gemeldeten Schwachstellen in der Kategorie fehlerhafte Eingabeüberprüfung etwa sechs Prozent auf fehlende Indexüberprüfung und Verzeichnispfadüberlauf, 15 Prozent auf Cross-Site Scripting, 30 Prozent auf Command Injection und 49 Prozent auf Pufferüberlauf zurückzuführen sind.

Mangelhafte Codequalität

Wenn bei der Softwareentwicklung nicht sorgfältig gearbeitet wird und Codeprobleme auftreten, auch wenn es sich nicht um Sicherheitslücken handelt, deutet dies auf eine mangelhafte Codequalität hin (Nelson & Chaffin, 2011). Software, die nach guten Programmierpraktiken, wie z. B. sicheren Entwicklungskonzepten, erstellt wurde, weist mit geringerer Wahrscheinlichkeit Sicherheitslücken auf als Software, die auf eine mangelhafte Codequalität schließen lässt. Wie die Überprüfung des ICS-Codes und die Reverse-Engineering-Maßnahmen gezeigt haben, ist die Software, die in der Regel in den ICS verwendet wird, nicht nach den Grundsätzen der sicheren Softwareentwicklung entworfen und implementiert worden. Die Tatsache, dass die Kernanwendungen von ICS bereits seit langer Zeit existieren, erhöht die Wahrscheinlichkeit, dass sie als autonome Systeme entwickelt wurden, die ausschließlich auf Effizienz und Zuverlässigkeit ausgerichtet sind. Für neue ICS-Anwendungen fehlen jedoch nach wie vor Grundsätze für eine sichere Programmierung. Die häufigsten Schwachstellen in dieser Kategorie sind die folgenden:

**Verwendung von potenziell gefährlichen Funktionen**

Besteht die Möglichkeit der Schaffung einer Schwachstelle durch den Aufruf einer potenziell gefährlichen Funktion oder durch die unsachgemäße Verwendung einer solchen Funktion durch die Anwendung, so handelt es sich um einen so genannten unsicheren Funktionsaufruf oder die Verwendung einer potenziell gefährlichen Funktion (Nelson & Chaffin, 2011). Die Verantwortung für die Eingabeüberprüfung liegt beim Programmierer, wenn die Verwendung unsicherer Funktionen zugelassen wird. Dies stellt ein offensichtlich hohes Risiko dar, wenn man die große Anzahl bekannter Schwachstellen durch fehlerhafte Eingaben und die öffentliche Wahrnehmung von Pufferüberläufen als häufigste und gefährlichste Software-Schwachstelle bedenkt. Es gibt kein Argument dafür, unsichere Funktionen zu verwenden oder sie in bestehendem Code nicht zu ersetzen, da alle bekannten ICS-Funktionen sichere Gegenstücke haben.

**NULL-Zeiger-Dereferenzierung**

Wenn ein NULL-Zeiger von der Anwendung als gültig erwartet wurde, führt dies normalerweise zu einem Abbruch oder Absturz, der als NULL-Zeiger-Dereferenzierung bekannt ist (Nelson & Chaffin, 2011). Zu den vielen Fehlern, die zu NULL-Zeiger-Dereferenzierungsproblemen führen können, gehören einfache Programmierfehler und Race Conditions.

Zusammenfassend kann gesagt werden, dass das Produkt aufgrund der mangelhaften Codequalität nicht über ausreichende Sicherheitsfunktionen verfügt. Die Einstufung eines Produkts als unsicher bezieht sich nicht nur auf seine Schwachstellen. Die Wahrscheinlichkeit, dass sich Schwachstellen leicht in den Code einschleichen, ist hoch. Dies gilt insbesondere dann, wenn die Programme komplex und schwer zu warten sind. Sie sind dann im Vergleich zu sicheren Produkten eher angreifbar (Upadhyay & Sampalli, 2020).

Berechtigungen, Privilegien und Zugangskontrollen

Zugangskontrollen in Computersystemen werden durch Sicherheitsmerkmale formalisiert, einschließlich Berechtigungen und Privilegien (Nelson & Chaffin, 2011). Unberechtigter Zugang zu ICS-Funktionen kann erlangt werden, wenn Zugangskontrollen fehlen oder schwach sind, was von Angreifern missbraucht werden kann. Die häufigsten Schwachstellen in dieser Kategorie sind die folgenden:

**Unzureichende Zugangskontrolle (Autorisierung)**

Wenn Benutzer:innen in der Lage sind, Aktionen auszuführen oder auf Daten zuzugreifen, die sie nicht ausführen sollten, liegt das daran, dass die ICS-Software entweder eine Zugangskontrollprüfung für alle verfügbaren Ausführungspfade fälschlicherweise durchführt oder eine Zugangskontrollprüfung überhaupt nicht durchführt.

**Ausführung mit unnötigen Privilegien**

Das Benutzerkonto gewährt Rechte, welche die angebotenen Dienste einschränken (Nelson & Chaffin, 2011). Angreifer:innen können durch Ausnutzen aller Dienste, die durch unberechtigte Privilegien erlangt wurden, im ICS-Netzwerk Fuß fassen. Der Angreifer kann seine Privilegien ausweiten, indem er einen verwundbaren Dienst manipuliert, der mit mehr Privilegien ausgeführt werden muss, als er derzeit hat. Wenn Dienste, die als privilegierte Benutzer arbeiten, effektiv ausgenutzt werden, ist ein vollständiger Hostzugriff möglich.

Unzureichende Authentifizierung

Wenn eine bestimmte Identität vorgegeben wird und die ICS-Software nicht in der Lage ist, diese korrekt zu verifizieren, entstehen mehrere Schwachstellen in ICS-Produkten. Diese Schwachstellen werden als fehlerhafte Authentifizierung klassifiziert (Nelson & Chaffin, 2011). ICS-Anbieter müssen, wenn die Kommunikation über ICS-Standardprotokolle erfolgt, in der Regel eigene Anwendungen für die Verarbeitung des Netzwerkverkehrs implementieren. Es ist Teil der Spezifikation des Netzwerkprotokolls, ob und wie Authentifizierung, Integritätsprüfung und Vertraulichkeit implementiert werden. Unerlaubte Privilegien können durch die Ausnutzung von Diensten erlangt werden, die schwache Authentisierungsmethoden verwenden. Die häufigsten Schwachstellen in dieser Kategorie sind die folgenden:

**Umgehung der Authentifizierung**

Wenn die Anwendung die Authentifizierung nicht korrekt durchführt, kann diese durch verschiedene Methoden umgangen werden. Unbefugte Zugriffe können häufig durch Angriffe auf den ICS-Webserver erreicht werden. Die für ICS erstellten Webdienste sind häufig angreifbar. Netzwerk-DMZs werden häufig in ICS-Architekturen eingesetzt, um die Gefährdung von Netzwerkkomponenten zu begrenzen und kritische Systeme zu schützen. Wenn der Zugriff in den angrenzenden äußeren ICS-Grenzen erlaubt ist, kann der erste Schritt auf dem Angriffspfad darin bestehen, Schwachstellen in den ICS-DMZ-Webservern auszunutzen.

**Fehlende Authentifizierung für kritische Funktion**

Die Anwendung authentifiziert normalerweise keine Funktionen, die viele Ressourcen verbrauchen oder eine überprüfbare Benutzeridentität erfordern. Für die meisten kritischen ICS-Funktionen ist in der Regel keine Authentifizierung erforderlich (Nelson & Chaffin, 2011). Wenn ein:e Angreifer:in in der Lage ist, eine kritische Funktionalität aufzudecken, erreicht er die Privilegienebene dieser Funktionalität. Abhängig von den damit verbundenen kritischen Funktionen kann der Angreifer unter seiner Kontrolle beliebigen Code ausführen, auf Verwaltungsfunktionen zugreifen, sensible Daten lesen oder ändern und andere privilegierte Funktionen nutzen.

Client-seitige Durchsetzung der Server-seitigen Sicherheit

Wenn die lokale Benutzerauthentifizierung auf einem Client durchgeführt wird, vertrauen die Anwendungen auf dem Client dem Client einfach, wenn er eine Verbindung zum Server herstellt. In diesen Fällen können mäßig versierte Angreifer:innen den Client manipulieren, um die Authentifizierung zu umgehen. Oder sie können einfach die für die Authentifizierung erforderlichen Informationen extrahieren, da sich diese Informationen auf dem Client befinden (Nelson & Chaffin, 2011). Mit den geänderten Informationen können sie dann auf den Server zugreifen.

**Man-in-the-Middle-Angriff**

Wenn ein Akteur, der kein Endpunkt ist, in der Lage ist, einen Kommunikationskanal zu beeinflussen oder auf ihn zuzugreifen, weil das ICS die Integrität des Kanals nicht ordnungsgemäß schützt oder die Identität der Akteure an beiden Enden des Kanals nicht ordnungsgemäß bestätigt, besteht die Möglichkeit eines Man-in-the-Middle-Angriffs (MitM-Angriff) (Nelson & Chaffin, 2011). Um eine sichere Kommunikation zwischen zwei Parteien zu gewährleisten, muss die Identifikation der Geräte an beiden Enden des Kommunikationskanals entsprechend überprüft werden. Eine falsche oder unzureichende Identifizierung einer der kommunizierenden Einheiten kann auf eine inkonsistente oder unzureichende Verifizierung dieser Einheiten zurückzuführen sein.

Unzureichende Überprüfung der Authentizität von Daten

Es besteht die Möglichkeit, dass ungültige Daten akzeptiert werden, wenn die ICS-Anwendung und die Protokolle die Authentizität oder Herkunft der Daten nicht ausreichend überprüfen. Systeme, die auf Datenintegrität angewiesen sind, stellen ein hohes Risiko dar (Nelson & Chaffin, 2011). Die häufigsten Schwachstellen in dieser Kategorie sind die folgenden:

**Cross-Site Request Forgery**

Es ist möglich, einen Client dazu zu bringen, unbeabsichtigte Anfragen an den Webserver zu senden und diese als authentisch zu behandeln, wenn der Webserver für den Empfang von Anfragen von Clients ohne Validierungsmechanismen zur Überprüfung der Absicht der Übertragung ausgelegt ist.

**Fehlende Unterstützung für die Integritätsprüfung**

Die Überprüfung der Datenintegrität während der Übertragung wird in den meisten ICS-Übertragungsprotokollen umgangen. Es gibt keine Möglichkeit festzustellen, ob Daten während der Übertragung beschädigt wurden, wenn Protokollprüfsummen oder Integritätsprüfwerte fehlen.

**Download von Code ohne Integritätsprüfung**

Angreifer:innen können Schadcode ausführen, wenn es ihnen gelingt, den Code während der Übertragung zu manipulieren, einen autorisierten Server zu imitieren oder den Master-Server zu kompromittieren, da es ICS-Komponenten gibt, die ausführbare Dateien oder Quellcode aus dem Netzwerk herunterladen und ausführen, ohne dass die Integrität des Codes und seine Herkunft ordnungsgemäß überprüft werden.

Kryptografische Probleme

Wenn Kryptografie als Sicherheitsinstrument zum Schutz von Daten eingesetzt wird, können einige technische Probleme auftreten. Zwei Arten von Schwachstellen in dieser Kategorie:

**Fehlende Verschlüsselung von sensiblen Daten**

Die unbefugte Nutzung der Identität eines legitimen Benutzers aufgrund der Übertragung unverschlüsselter Anmeldeinformationen über das Netzwerk gefährdet das System (Nelson & Chaffin, 2011). Ein:e Angreifer:in könnte sich mit den Rechten dieses Benutzers am System anmelden, wenn es ihm gelingt, dessen Passwort und Benutzernamen im Netzwerk abzufangen. Angreifer:innen können sich einen Vorteil verschaffen, wenn sie Zugang zu unverschlüsselten Informationen über die ICS-Topologie, die Geräte oder den Quellcode haben. Daher sollte dieser Zugang eingeschränkt werden.

**Verwendung eines defektenoder riskanten kryptografischen Algorithmus**

Durch das Knacken der ICS-Verschlüsselungsprotokolle kann der Angreifer Zugriff auf die Anmeldedaten des Benutzers für die Authentifizierung erhalten.

Anmeldeinformationsverwaltung

Als Teil der Sicherheitsprotokolle werden die Zugangsdaten von einer etablierten Form von spezialisierter Software ausgegeben und verwaltet. Diese Software kann manchmal Schwachstellen aufweisen. In dieser Kategorie gibt es zwei Arten von Schwachstellen:

**Unzureichend geschützte Anmeldeinformationen**

Mit Hilfe von Netzwerk-Sniffing-Tools, die sogar kostenlos heruntergeladen werden können, ist es möglich, den Netzwerkverkehr mit den als Text gesendeten Anmeldedaten einzusehen, wodurch das System durch die illegale Verwendung der Anmeldeinformationen eines authentischen Benutzers gefährdet wird.

**Verwendung von fest kodierten Anmeldeinformationen**

Die Verwendung von Konfigurationsskripten oder in ICS-Code kodierten Anmeldeinformationen, um ICS-Komponenten zu authentifizieren, schafft eine Schwachstelle, da das Lesen der Systemkonfigurationsdatei keine Authentifizierung erfordert.

Sicherheitskonfiguration und -wartung der ICS-Software

Die Sicherheit der ICS-Software hängt in hohem Maße von ihrer Konfiguration und Wartung ab. Dabei geht es darum, anfängliche Entwicklungsfehler zu korrigieren, nach der Entdeckung von Fehlern ein entsprechendes Update durchzuführen und bei der Inbetriebnahme die richtige Konfiguration festzulegen. In dieser Kategorie gibt es drei Arten von Schwachstellen:

**Mangelhaftes Patch-Management während der Entwicklung von ICS-Software**

Plattformen wie ICS-Anwendungen, Betriebssysteme und Hardware können aufgrund schlechter Wartung, falscher Konfiguration oder Fehlern angreifbar sein. Häufig eingesetzte Sicherheitskontrollen zur Beseitigung dieser Schwachstellen sind Sicherheitssoftware, Patches für Betriebssysteme und Anwendungen sowie physische Zugangskontrollen (Nelson & Chaffin, 2011). Das Patch-Management ist ein wesentlicher Bestandteil der Wartung von Computersystemen, insbesondere dann, wenn eine Sicherheitslücke entdeckt und öffentlich bekannt wird, da sie das System anfällig für Angriffe macht.

**Alte oder ungepatchte Versionen von Drittanbieteranwendungen, die in die ICS-Software integriert sind**

Wenn alte oder ungepatchte Versionen von Anwendungen in das ICS integriert werden, werden auch die Schwachstellen dieser Anwendungen integriert. Dies ermöglicht einen Angriff auf das System.

**Unzulängliche Sicherheitseinstellungen**

Auch wenn Anwendungen nicht ordnungsgemäß installiert und/oder konfiguriert werden, können Schwachstellen entstehen, selbst wenn sie über eine sichere Authentifizierung verfügen. Dies ist der Fall bei ICS-Anwendungen, die über Sicherheitsoptionen verfügen, die aber von dem für die Installation und Konfiguration verantwortlichen Programmierer nicht aktiviert oder verwendet werden.

Interessierte Leser:innen finden weitere Details zu diesen Schwachstellen in der zitierten Literatur. Eine aktualisierte Liste der gefährlichsten Schwachstellen findet sich in der *2022 CWE Top 25 Most Dangerous Software Weaknesses List* (CWE, 2022).

Fragen zur Selbstkontrolle

1. Bitte markieren Sie die richtige(n) Aussage(n).

* Die Größe eines Arrays, das von Computerprogrammen verwendet wird, ist unbegrenzt, ebenso wie der Speicherplatz, der für seine Speicherung reserviert ist.
* *Wenn Benutzer:innen in der Lage sind, Aktionen auszuführen oder auf Daten zuzugreifen, die sie nicht ausführen sollten, liegt das daran, dass die ICS-Software entweder eine Zugangskontrollprüfung für alle verfügbaren Ausführungspfade fälschlicherweise durchführt*.
* Schlechte Codequalität hat keinen Einfluss auf die Sicherheitseigenschaften des Produkts.
* *Durch das Knacken der ICS-Verschlüsselungsprotokolle kann der Angreifer Zugriff auf die Anmeldedaten des Benutzers für die Authentifizierung erhalten*.

1. Bitte vervollständigen Sie die folgenden Sätze.

Die Verwendung von in ICS-Code kodierten Anmeldeinformationen, um die *Authentifizierung* zwischen ICS-*Komponenten* durchzuführen, schafft eine *Schwachstelle*, da das Lesen der Systemkonfigurationsdatei keine Authentifizierung erfordert.

Wenn ungepatchte *Versionen* von Anwendungen in das ICS integriert werden, werden auch die *Schwachstellen* dieser Anwendungen *integriert*. Dies ermöglicht einen Angriff auf das System.

**Zusammenfassung**

Aufgrund der großen Vielfalt an Komponenten, die in industriellen Steuerungsnetzwerken zum Einsatz kommen, werden eine Vielzahl von Kommunikationsprotokollen mit unterschiedlichen Computercodes verarbeitet, was sie anfällig für Schäden durch versehentliche Fehler oder vorsätzliche Angriffe macht, die ihre Sicherheit beeinträchtigen. Darüber hinaus müssen diese Netzwerke mit ihrer Umgebung oder dem Cyberspace in Verbindung stehen, was sie nicht vor Bedrohungen oder Cyber-Angriffen schützt. Dies macht die Cyber-Sicherheit zu einem sehr wichtigen Thema in der Automatisierungstechnik. Aus diesem Grund werden im Abschnitt über Anlagensteuerungsnetzwerke die wichtigsten funktionalen Komponenten vorgestellt, um in das Gebiet einzuführen: angefangen bei denen, die direkt mit der Steuerung zu tun haben, über diejenigen, die mit den Bedienern als menschliche Komponente interagieren, bis hin zu denen, die die Verbindung und Kommunikation zwischen ihnen ermöglichen, und schließlich zu denen, die physisch mit dem Prozess interagieren. Der Abschnitt über Cyber-Angriffe beginnt mit einer Unterscheidung zwischen Cyber-Bedrohung und Cyber-Angriff. Beide Begriffe werden im Bereich der Cyber-Sicherheit häufig verwendet. Es folgt eine Beschreibung der Akteure, die Anlagensteuerungsnetzwerke bedrohen. Abschließend wird auf Hacker als externe Bedrohung eingegangen, die in der Regel Malware und andere mögliche Vorgehensweisen verwenden, welche ebenfalls beschrieben werden. Schließlich werden im Abschnitt über allgemeine Schwachstellen in industrieller Software die neun Kategorien vorgestellt, die in der Studie von Nelson & Chaffin (2011) auf der Grundlage der Sicherheitsbewertungen des Control Systems Security Program (CSSP) der National Cyber Security Division des US Department of Homeland Security (DHS), der ICS-CERT-Operationen und der Bewertungen des Cyber Security Assessment Tool (CSET) für ICS beschrieben werden.