



Mittelstand 4.0
Kompetenzzentrum
Magdeburg



STANDARDS IN DER INFORMATIONSTRANSFER IM LEITTECHNISCHEN UMFELD

Industrielle Datenübertragung als Baustein für die
Digitalisierung im Unternehmen



IMPRESSUM

Herausgeber:

Mittelstand 4.0-Kompetenzzentrum Magdeburg „vernetzt wachsen“

ifak e.V. Magdeburg

ifak ist Mitglied der Deutschen Industrieforschungsgemeinschaft Konrad Zuse (Zuse-Gemeinschaft)

Redaktion: Dr. Matthias Riedl, Dr. Thomas Bangemann

Gestaltung: dripstyle designstudio

Bildnachweise: Mittelstand 4.0-Kompetenzzentrum

Druck: FLYERALARM GmbH

Auflage: 150



Alle in diesem Leitfaden dargestellten Informationen entsprechen keiner Rechtsberatung oder Kaufberatung bzw. **ersetzen keine rechtliche und Kauf-Beratung**. Sie stellen lediglich die persönliche Wahrnehmung der Autoren wieder. Die Autoren übernehmen keine Haftung für eventuelle Folgeschäden, insbesondere rechtlicher Natur, die aus fehlerhaften Handlungen, die aus diesem Leitfaden herrühren, entstehen.

VORWORT

Im Privatleben sind wir heute rund um die Uhr online. Das heißt, wir nutzen das Internet, kommunizieren in sozialen Netzwerken und senden eher Kurznachrichten, als dass wir Briefe schreiben. Die Digitalisierung ist allgegenwärtig. Auch in den Produktionsstätten finden digitale Dienste schon seit Jahren Einzug. Nur, dass die Entwicklung in diesem Bereich viel langsamer und divergenter voranschreitet als im täglichen Leben. Die Gründe hierfür sind anwendungsspezifisch sehr vielfältig und resultieren in Anforderungen an die langfristige Verfügbarkeit der Dienste, die Echtzeitfähigkeit (Antwortzeiten, Zykluszeiten, Synchronität) sowie die Dateninhalte und Datenlängen. Aufgabenspezifisch oder auch herstellerspezifisch haben sich am Markt eine Vielzahl von Kommunikationstechnologien entwickelt, die in der Regel inkompatibel sind und nur mit erheblichem Aufwand harmonisiert werden können.

An den Kommunikationsendpunkten besteht dann das Problem der Datenintegration in die verschiedenen Anwendungen.

Für die Industrie 4.0 ist Vernetzung im Sinne von Diensten und Daten eine grundlegende Voraussetzung. Daten müssen vom Entstehungsort im Prozess bis in die Geschäftsprozesse hinein durchgängig verfügbar sein. Während Großunternehmen seit Jahren auf eine durchgängige konsistente Datenhaltung hinarbeiten, sehen sich kleine und mittlere Unternehmen angesichts der aktuellen Tendenzen auf dem Weg zur Industrie 4.0 mit neuen Herausforderungen konfrontiert. Sie fragen sich, welche Standards zukunftssicher sind und suchen nach den für ihr Unternehmen geeignetsten Kommunikationstechnologien.

INHALT

- 1 Vorwort
- 2 Einleitung
- 4 Warum sollten KMU Übertragungstechniken einsetzen?
- 8 Grundlagen und Standards der industriellen Kommunikation
- 12 Kommunikationssysteme und Integrationstechnologien
- 26 Handlungsempfehlung
- 31 Wer hilft mir weiter?



EINLEITUNG

Dieser Leitfaden konzentriert sich auf Kommunikations- und Integrationstechnologien in der Leittechnik für industrielle Prozesse. Er orientiert sich an heute verfügbaren Technologien als Ausgangsbasis für die Entwicklung hin zur Industrie 4.0 und soll Grundlagen für den Einsatz standardisierter und innovativer Kommunikations- und Netzwerktechnik für die Leittechnik in verschiedenen Branchen vermitteln. Es sollen Grundlagen der digitalen Kommunikationssysteme und der dazugehörigen Terminologien vorgestellt werden. Zudem zeigt der Leitfaden die Vielfalt, Einsatzmöglichkeiten und einige Vor- und Nachteile industrieller Kommunikationssysteme auf. Darüber hinaus geht es um Informationen zum effizienten und sichereren Einsatz von Ethernet-basierten Kommunikationssystemen und um Standards im Umfeld industrieller Kommunikationssysteme. Letztendlich soll dem Gerätehersteller als auch dem Anlagenbetreiber oder dem Ingenieurbüro ein prinzipielles Vorgehen für die Auswahl geeigneter Technologien aufgezeigt werden.

In den folgenden Kapiteln werden wesentliche Eigenschaften am Markt verbreiteter Kommunikationsprotokolle und Integrationstechnologien vorgestellt. Dieser Überblick soll Ihnen helfen, Technologie Kandidaten an den Bedürfnissen relevanter Anwendungsaufgaben zu spiegeln und somit die Auswahl einer geeigneten Technologie erleichtern. Allerdings kann dieser Leitfaden nicht alle Eigenschaften der vorgestellten Technologie Kandidaten aufzeigen. Zu jedem Kapitel gibt es daher Hinweise auf weiterführende Informationsquellen. Die Mitarbeiter des Kompetenzzentrums stehen gern für die Diskussion alternativer Varianten zur Verfügung und unterstützen bei der bedarfsgerechten Auswahl. Nehmen Sie sich nun etwas Zeit für den Leitfaden.

Wenn Sie weitere Fragen haben, dann helfen wir Ihnen gern weiter.

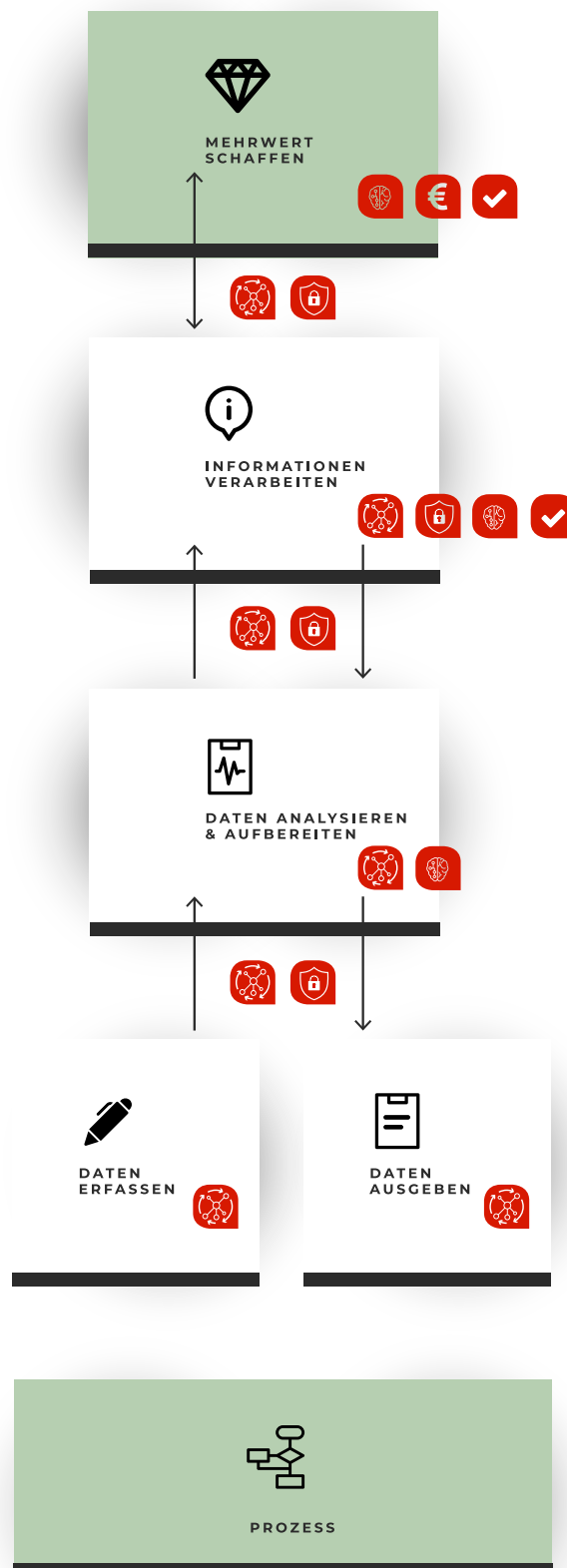
Ihr Mittelstand 4.0-Kompetenzzentrum Magdeburg

Was ist industrielle Kommunikation?

Der Begriff industrielle Kommunikation beschreibt das Einsatzgebiet eines Kommunikationssystems im industriellen Umfeld, das in der Regel die digitale Informationsübertragung nutzt. Das Einsatzgebiet umfasst beispielsweise die Fertigungsindustrie, den Maschinenbau, Automobil- oder Konsumgüterproduktion oder auch die Prozessindustrie. Auf Grund der vielfältigen Anforderungen der unterschiedlichen Einsatzgebiete hat sich am Markt eine Vielzahl von industriellen Kommunikationsprotokollen etabliert. Es kommen verschiedene Übertragungsmedien wie Kupferkabel, Lichtwellenleiter oder Funk zum Einsatz.

Nachhaltige Automation

Die Pfeile kennzeichnen die Informationsübertragung in der Automation.



INHALT UND STRUKTUR DER KAPITEL

KAPITEL 1



WARUM SOLLTEN
KMU ÜBERTRAGUNGS-
TECHNIKEN
EINSETZEN?

Im ersten Kapitel werden der Bedarf und der Nutzen für den Einsatz industrieller Kommunikationssysteme in der Produktion dargestellt. Weiterhin wird auf typische informationstechnische Strukturen in Produktionssystemen eingegangen. Es werden grundlegende Anforderungen an den Datenaustausch abgeleitet. Das Kapitel schließt mit einem Ausblick auf aktuelle Trends in der industriellen Kommunikationstechnologie.

KAPITEL 2



GRUNDLAGEN UND
STANDARDS DER
INDUSTRIELLEN
KOMMUNIKATION

Das zweite Kapitel stellt dar, wie vielfältig das Angebot an technischen Kommunikationslösungen ist und dass der Einsatz standardisierter Technologien aktiv zum Investitionsschutz beitragen kann.

KAPITEL 3



KOMMUNIKATIONS-
SYSTEME UND
INTEGRATIONS-
TECHNOLOGIEN

Das dritte Kapitel vermittelt einen ersten Überblick über typische Kommunikationsstandards für die Fertigungstechnik und die Prozesstechnik. Es gibt einen Überblick zu Technologien für die Integration von Sensoren, Aktoren oder auch komplexen Maschinen in die Leittechnik sowie in übergeordnete Ebenen im Unternehmen.

KAPITEL 4



HANDLUNGS-
EMPFEHLUNG

Im vierten Kapitel werden grundlegende Vorgehensweisen bei der Auswahl und Umsetzung von Kommunikationslösungen vorgeschlagen. Die Empfehlungen richten sich an Gerätehersteller, Anlagenbetreiber und Ingenieurbüros.

KAPITEL 5



PRAXISBEISPIEL

Im fünften Kapitel werden die Handlungsempfehlungen durch ein Beispiel aus der Praxis ergänzt.



KAPITEL 1: WARUM SOLLTEN KMU ÜBERTRAGUNGSTECHNIKEN EINSETZEN?

Märkte und Anforderungen an Produkte verändern sich

Deutsche Unternehmen befinden sich sowohl national als auch international in einem Spannungsfeld, in dem sie auf der einen Seite intelligente Produkte und Dienstleistungen anbieten wollen und andererseits unter einem enormen Preisdruck leiden. Verstärkt wird diese Situation durch einen zunehmenden Mangel an qualifizierten Arbeitskräften. Hohe Flexibilität und Produktivitätssteigerung der Komponenten, aber auch Faktoren wie Zuverlässigkeit, Verfügbarkeit, Konnektivität, Erfüllung von Anforderungen der IT- und funktionalen Sicherheit, Benutzerfreundlichkeit oder zum Produkt angebotene Dienstleistungen werden zu entscheidenden Kriterien für eine Abgrenzung vom Wettbewerb. Nicht zuletzt entscheidet auch der Preis.

Um Kosten zu sparen, werden künftig insbesondere für Industriegüter eine Reduzierung der Hardwarevarianz innerhalb und zwischen Produktfamilien als auch der Ersatz von Hard-

warevarianz durch Softwaremodularität notwendig sein. Der verstärkte Einsatz von Software erfordert beziehungsweise ermöglicht wiederum funktionale Upgrades oder auch einfach das Einspielen von Updates. Hierfür bieten sich Verfahren an, die über das Netzwerk realisiert werden können. Online-Dienste werden künftig eine wachsende Rolle spielen und entschieden zur Kundenbindung beitragen. Voraussetzung für die geforderte Konnektivität sind geeignete, möglichst standardisierte Kommunikationsschnittstellen für den Informationsaustausch im Wertschöpfungsnetzwerk. Je nach Anforderung existieren verschiedene geeignete Protokollstandards. Der Einsatz von Standards ermöglicht die Öffnung von Systemen in Richtung diverser Hersteller und erlaubt es Spezialisten, zugeschnittene Applikationen in diese Systeme zu integrieren. Hierbei sind Aspekte wie funktionale Sicherheit, Datensicherheit, Datenschutz, Privatsphäre von Kunden oder Abrechenbarkeit zu gewährleisten.

Anwendungsfälle für Kommunikation in der Leittechnik

Produzierende Unternehmen und ihr Bedarf an Daten- und Informationsaustausch:

- 01.** Entlang der Wertschöpfungskette eines Produktes sind Informationen mit Zulieferern, Kunden sowie externen Dienstleistern auszutauschen.
- 02.** Vom Entwurf bis zur Verschrottung eines Produktes fallen produktspezifische Daten an. Diese sind entweder statisch oder ändern sich während des Produktlebenszyklus. Diese Daten können für die Erbringung produktspezifischer Dienstleistungen genutzt werden.
- 03.** Während der Produktion sind Daten zwischen den an der Herstellung beteiligten technischen Einrichtungen sowie mit dem Produktionsmanagement auszutauschen.

Die Art des Datenaustausches oder auch der Grad der Datenintegration haben unmittelbaren Einfluss auf die Produktqualität, mögliche Dienstleistungsangebote, Zeiten für die Produkteinführung, die Herstellungsdauer oder Reaktionszeiten für den Service. All das beeinflusst die mit einem Produkt verbundenen Kosten und letztendlich die Kundenzufriedenheit.

Da die Anforderungen an den Datenaustausch unter den drei erwähnten Aspekten sehr unterschiedlich sind und weiterhin zwischen Branchen differenziert werden muss, entstand eine ganze Reihe inkompatibler Kommunikationslösungen. Der Wettbewerb zwischen Anbietern von Automatisierungslösungen hat diese Situation nicht unbedingt verbessert. In vielen Bereichen sind mittlerweile Standards entstanden, die dieser Diversität entgegenwirken, sie aber nicht komplett aufheben. Aktuell gibt es keinen einzelnen Standard, der allen Anforderungen gerecht wird. Eine mehrfache Schnitt-

stellenanpassung und Datentransformationen sind daher heute notwendig, um durchgängige Gesamtlösungen zu schaffen. Neben den spezifischen Kommunikationsprotokollen und Schnittstellenanpassungen wurden Integrationstechnologien entwickelt, die zum Beispiel eine Integration separat entwickelter Automatisierungskomponenten in die Leittechnik oder das Produktionsmanagement auf Datenebene unterstützen. Ziel muss es sein, die für die jeweilige Aufgabenstellung geeigneten Standards auszuwählen und somit ein gesundes Maß an Investitionssicherheit zu erzielen.

Automatisierungssysteme der Prozess- oder Fertigungsindustrie sind heute in klassischer Weise hierarchisch aufgebaut. IEC 62264 (oder auch ISA 95) ist ein internationaler Standard für die Integration zwischen strategischen Geschäftsprozessen, dem operativen Produktionsmanagement und der Leitebene.



ISA 95 / IEC 62264 definiert 5 Ebenen für die Produktionsinfrastruktur:

Ebene 0 bezeichnet den zu steuernden Prozess selbst.

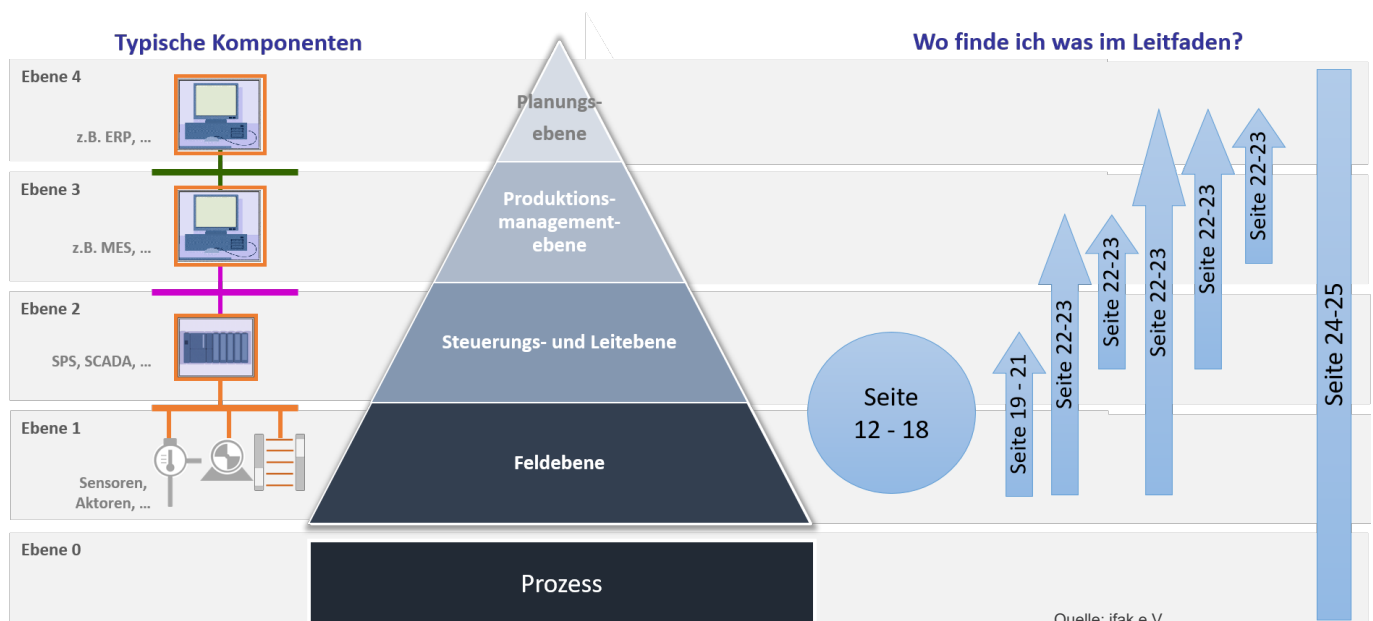
Ebene 1 verbindet den Prozess mit den Leiteinrichtungen (Steuerungstechnik). Hier werden Sensoren und Aktoren mit verschiedensten Vorverarbeitungsfähigkeiten eingesetzt. Sie wandeln physikalische Merkmale in analoge oder binäre Signale und schließlich in digital verarbeitbare Daten um.

Auf **Ebene 2** sind Leiteinrichtungen wie Speicherprogrammierbare Steuerungen (SPS), Supervisory Control and Data Acquisition (SCADA) oder Leitsysteme etabliert. Hier erfolgt die Steuerung oder Regelung des Prozesses in Echtzeit.

Ebene 3 dient dem operativen Management des Produktionsprozesses. Manufacturing Execution Systems (MES) stellen vielfältige Informationen für die Beobachtung, Bewertung (Key Performance Indicators – KPI) und Beeinflussung des Produktionsprozesses bereit. Ihre Hauptaufgabe ist jedoch das anlagenweite „Planning and Scheduling“.

Auf **Ebene 4** sind Enterprise Resource Planning (ERP) Systeme zur strategischen Planung der Unternehmensprozesse nach vorgegebenen Geschäftszielen installiert.

Einordnung der Kommunikations- und Integrationstechnologien



Nachfolgend soll die Diversität der Anforderungen an die Kommunikation am Beispiel der Produktionsphase verdeutlicht werden. In dieser Phase sind folgende Arten der Kommunikation relevant:

Verknüpfung von Sensoren, Aktoren und Steuereinrichtungen (Ebene 1 und 2):

Die Abarbeitung eines Steuerungsprogrammes erfolgt in Programmzyklen. Sensor- und Aktordaten werden entweder über viele Eingangs- und Ausgangsbaugruppen (Punkt-zu-Punkt) erfasst/ausgegeben oder aber seriell über Feldbusse übertragen. Hierbei sind kleine Datenmengen bis hin zu einzelnen Bits je nach Prozessparametern mit zum Teil extrem kurzen Abtastzeiten typisch. Die Leistungsfähigkeit der in Feldgeräten eingesetzten Prozessoren ist in der Regel stark eingeschränkt.

Schließen von Regelkreisen, Synchronisation (Ebene 1 und 2):

Für das Schließen eines Regelkreises kommt es auf eine möglichst äquidistante Abtastung der Eingangsinformationen (Ist-Werte/ Regelgröße), die Verarbeitung dieses Schnappschusses und Ausgabe des berechneten Stellwertes in Echtzeit an. Die Echtzeit hängt dabei von den Zeitkonstanten des Prozesses ab. Bei der Integration von Sensoren und Aktoren über Eingabe- und Ausgabebaugruppen einer Speicherprogrammierbaren Steuerung ist auch hier der Programmzyklus des Steuerungsprogramms maßgeblich für die Einhaltung der Echtzeitanforderungen. Bei der Integration von Sensoren und Aktoren über industrielle Kommunikationssysteme - als Integrationskomponenten in die Steuerung kommen Kommunikationsprozessoren zum Einsatz - sind zusätzlich die Zykluszeiten für die Buskommunikation zu berücksichtigen. Je nach eingesetzter Technologie können diese sehr unterschiedlich sein. Für spezielle Anwendungen, wie etwa die Synchronisation von Antrieben, gilt es zusätzlich, den Schlupf zwischen den einzelnen Abtastzyklen zu begrenzen. Auch für diese Anwendungsfälle wurden spezielle Varianten von Bussystemen realisiert.

Konfiguration von verteilten Automatisierungskomponenten (Ebene 1, 2 und 3):

Während Prozesswerte in der Regel zyklisch zu übertragen sind, besteht für die Konfiguration eines Automatisierungsgerätes lediglich zu „besonderen Anlässen“ Bedarf, wie etwa der Anlagen- und Geräteinbetriebnahme, einer Neuparametrierung im laufenden Betrieb oder nach einer Wartungsmaßnahme für den Zugriff auf die Geräteparameter. Eine solche Parameteränderung erfolgt entweder direkt über das Bedienfeld des Gerätes, eine an das Automatisierungsgerät „vor Ort“ angeschlossene Bediensoftware oder für den Fall, dass die Parametrierung aus der Ferne erfolgen soll, über das Kommunikationssystem. Hierfür sind für die Konfiguration geeignete Dienste notwendig, die die Auslastung des Kommunikationsmediums möglichst wenig belasten.

Datenaustausch zwischen Steuerungen und übergeordneten Produktionsmanagementanwendungen (Ebene 2 und 3):

Speicherprogrammierbare Steuerungen (SPSen) steuern räumlich und funktional abgegrenzte Prozesse. In komplexen Produktionssystemen sind diese SPSen in den produktionsbezogenen informationstechnischen Unternehmensverbund integriert. Informationen, die hier typischerweise ausgetauscht werden, sind beispielsweise: Auf der SPS ausführbare Programme, Konfigurationsdaten und/oder Status- und Zustandsinformationen aus dem Prozess und aus Maschinen. An den Datenaustausch werden hier in der Regel geringere Echtzeitanforderungen gestellt. Dafür sind die zu übertragenden Datenpakete meist größer.

Informationsaustausch mit und zwischen Managementanwendungen (Ebene 3 und 4):

Zwischen Produktionsmanagementsystemen werden Informationen etwa für die Produktionsprozesssteuerung, das Scheduling von Arbeitsaufträgen, die Verwaltung von Maschinen, Materialien, Personal oder ganzen Produktionsaufträgen mit zugehörigem Einkauf, der Planung, Produktion, Logistik bis hin zum Service ausgetauscht. Dieser Informationsaustausch unterliegt weniger kritischen Anforderungen bzgl. der Antwortzeiten.

Fernzugriff auf Maschinen und Anlagen (Ebene 1, 2 und 3):

Insbesondere für Dienstleistungen wie die Instandhaltung von Maschinen oder die Überwachung weit verteilter Automatisierungsaufgaben (z.B. Kanalnetze, Energieverteilnetze) tritt die Forderung nach überregionalem Informationsaustausch in den Vordergrund.

Aktuelle Entwicklungen in Richtung Internet der Dienste und Dinge / Industrie 4.0

Die beschriebenen Ebenen spiegeln sich typischerweise in der informationstechnischen Infrastruktur einer Produktionsanlage wider. Die Komponenten der einzelnen Ebenen sind über gewachsene, standardisierte oder auch proprietäre Kommunikationssysteme gekoppelt. Es haben sich diverse Netzwerkübergänge ausgeprägt, welche die Anpassung physikalischer, protokolltechnischer oder auch anwendungsbezogener Unterschiede vornehmen. Die Netzwerkübergänge reichen von einzelnen Gateways bis zu SPS mit mehreren verschiedenen Kommunikationsprozessoren.

Aktuelle Konzepte wie das Internet der Dienste und Dinge oder Industrie 4.0 sehen vor, dass auf Geräte und Anwendungen der verschiedenen Ebenen direkt, das heißt ohne viele Netzwerkbrüche, zugegriffen werden kann. Bereits heute gibt es zahlreiche Beispiele des Einsatzes von Internet-Technologien für den Zugriff auf produktionsrelevante Informationen. Dieser Trend zeigt den Weg vom datenzentrierten Informationsaustausch zu dienstorientierten Konzepten auf und hat unmittelbaren Einfluss auf die einzusetzenden Kommunikationstechnologien und den Einsatz von Sicherheitsmechanismen.

Moderne Produktionsanlagen müssen heute in kürzester Zeit an veränderte Marktanforderungen anpassbar sein. Hierfür sind Entscheidungsprozesse auf allen Management- und leittechnischen Ebenen zu treffen. Das heißt, kritische Infor-

mationen müssen zur richtigen Zeit, auf der richtigen Ebene und im entsprechenden Kontext verfügbar sein. Sowohl die organisatorischen als auch die topologischen Strukturen sind über die Jahre hinweg gewachsen. Einhergehend mit dieser strukturellen Entwicklung sind diverse, auf die unterschiedlichen Belange zugeschnittene und zum Teil inkompatible Kommunikations- und IT-Systeme entstanden. Auch wenn es momentan wieder Bemühungen zum übergreifenden Einsatz gemeinsamer Kommunikationstechnologien gibt, stehen insbesondere KMU vor der Frage, welche Technologien und Standards sie zur Sicherung aktueller Marktpositionen sowie des mittel- und langfristigen Bestehens am Markt einsetzen sollen.

In den folgenden Kapiteln sollen wesentliche Eigenschaften am Markt verbreiteter Kommunikationsprotokolle und Integrationstechnologien vorgestellt werden. Dieser Überblick soll helfen, Technologiekandidaten an den Bedürfnissen relevanter Anwendungsaufgaben zu spiegeln und somit die Auswahl einer geeigneten Technologie erleichtern. Doch kann dieser Leitfaden nicht alle Eigenschaften der vorgestellten Technologiekandidaten aufzeigen. Zu jedem Kapitel gibt es daher Hinweise auf weiterführende Informationsquellen. Die Mitarbeiter des Kompetenzzentrums stehen gern für die Diskussion alternativer Varianten zur Verfügung und unterstützen bei der bedarfsgerechten Auswahl.





KAPITEL 2: GRUNDLAGEN UND STANDARDS DER INDUSTRIELLEN KOMMUNIKATION

In Kapitel 1 haben wir erfahren, warum KMU Informationsübertragungstechniken einsetzen. In dem nun folgenden Kapitel erfahren Sie, warum bei der Planung der einzusetzenden Kommunikationslösungen in einer Maschine oder Produktionsanlage neben den rein technischen Anforderungen wie Bandbreite, Latenz, Netztopologie oder der Anzahl anschließbarer Teilnehmer vor allem die breite Verfügbarkeit von Geräten und Softwarekomponenten eine große Rolle spielt.

Eine Lösung für diese Anforderungen ist die Nutzung von Standards. Standards wurden eingeführt, um eine Aufgabe einheitlich und damit in der Regel einfacher, wiederholbar und letztlich auch kostengünstiger zu erledigen. Dabei werden bestimmte Festlegungen und Spezifikationen als bindend erachtet.

Vorteile von Standards

- Wiederholbarkeit der Vorgehensweise bei der Planung und Nutzung ermöglicht die Aneignung von Wissen und Fähigkeiten aus der Gewohnheit heraus
- Effizienz und Sicherheit bei der Ausführung der Arbeiten, weil sich erneutes Hineindenken erübrigt
- Sicherung gleichbleibend hoher Qualität der Arbeitsabläufe und damit der Produkte
- Leichtere Einbindung von Mitarbeitern in ähnliche Arbeitsprozesse
- Verringerung des Betreuungsaufwands beim Kunden sowie Verringerung der Abhängigkeit von Lieferanten, da in der Regel mehrere Marktteilnehmer ähnliche Produkte anbieten



Neben den genannten Vorteilen aus Sicht des Bezugs von Komponenten und der Schulung der Belegschaft ist auch die Attraktivität eigener Produkte gesteigert, wenn diese standardkonforme Schnittstellen und vor allem auch ein standardkonformes Verhalten aufweisen. Weiterhin lassen sich eigene Produkte besser in die Systeme der Kunden integrieren. Standards sind damit dem eigenen Absatz förderlich und ermöglichen Kosteneinsparung beim Engineering und beim Einsatz im Produktivbetrieb, in dem der Zugriff auf Daten vereinheitlicht wird und damit erste Schritte für eine Überführung der

Systeme hin zu den Konzepten von Industrie 4.0 angegangen werden.

In der Regel haben Produktionssysteme und die darin verbauten Komponenten bzw. Zusatzbaugruppen eine lange Lebensdauer. Schon unter diesem Gesichtspunkt empfiehlt es sich, standardisierte Kommunikationslösungen einzusetzen, weil nur dadurch ein Ökosystem entstehen kann und eine breite Community am Einsatz und Dienstleistungen wie Wartung und Pflege solcher Systeme interessiert ist.



Welche Standards bei der industriellen Kommunikation gibt es?

Die industrielle Kommunikation bietet dem jeweiligen Einsatzzweck entsprechend eine Vielzahl von standardisierten Kommunikationslösungen, wobei unterschiedliche Technologien entlang der Informationsverarbeitung zu betrachten sind. Aufbauend auf der physischen Datenerfassung durch Sensoren beziehungsweise der Beeinflussung des zu steuernden Produktionsprozesses durch Aktoren werden die Daten den Steuerungssystemen zur Verfügung gestellt. Die folgende Grafik gibt einen Überblick über verschiedene Technologien, die im Unternehmen für die Datenerhebung im Produktionsumfeld, deren Weiterleitung bis hin zur Verarbeitung und Auswertung häufig eingesetzt werden. Im Rahmen dieses Leitfadens liegt der Fokus auf der Datenübertragung. Dies bedeutet, die nachfolgend vorgestellten Kommunikationstechnologien sind in dieser Schicht angesiedelt. Den einfachsten Kommunikationsstandard stellt dabei die 4-20mA Technik dar, bei der ein analoges Signal mit begrenzter Stromstärke übertragen wird. HART nutzt diese Technik ebenfalls, modelliert aber ein digitales Signal auf die analoge Signalübertragung auf und ist neben rein digitalen Feldbussystemen wie PROFIBUS-PA in der Prozesstechnik weit verbreitet.

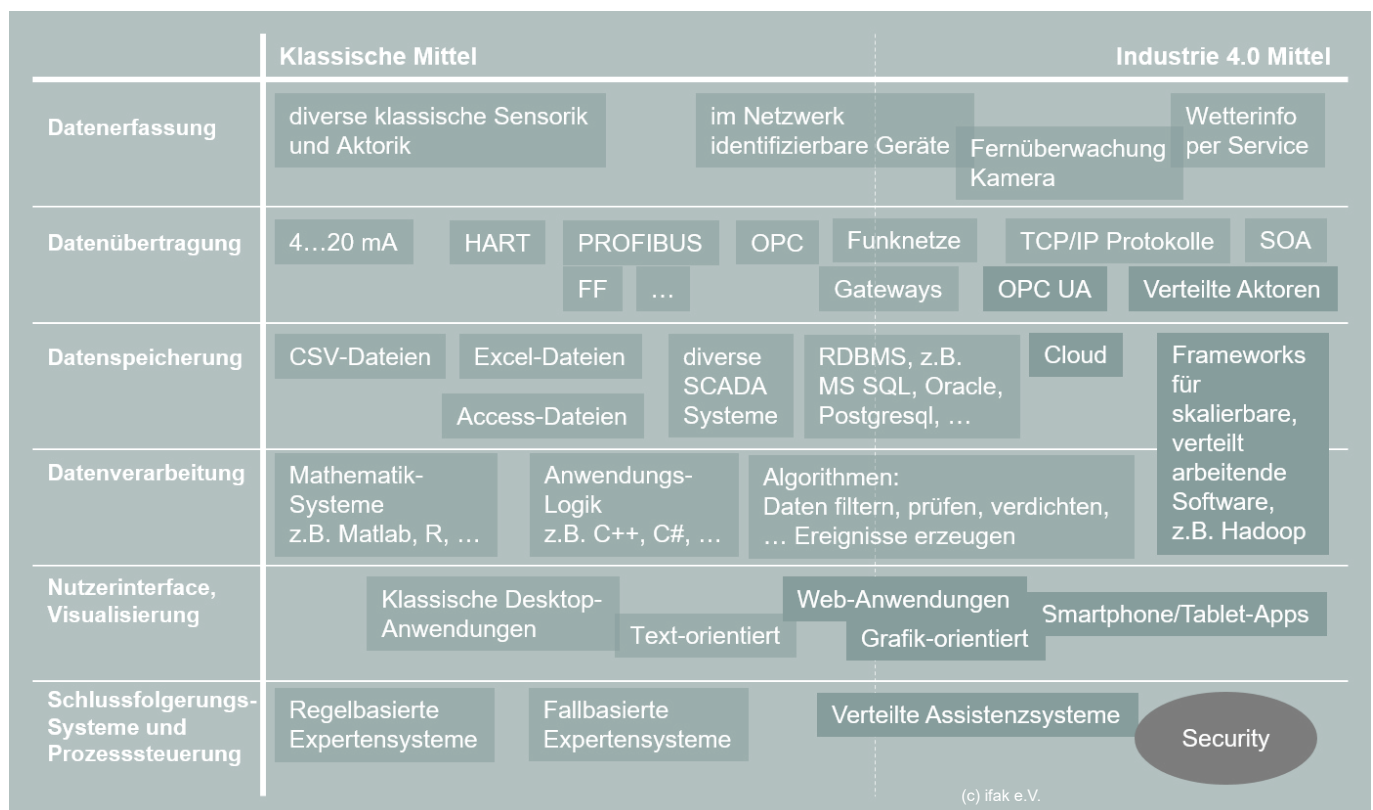
Durchgesetzt hat sich in der Fertigungstechnik auch der Process Field Bus – kurz PROFIBUS. Für PROFIBUS gibt es zwei Varianten: DP für die Verfahrenstechnik und PA für die Prozessautomation. Neben der Kommunikation auf Feldebene bietet zum Beispiel PROFIBUS auch die Integration in die Leitebene zum Bedienen und Beobachten des Produktionsprozesses. Etabliert haben sich für die vertikale Kommunikation zwischen Steuerungs- und Leitebene auch TCP/IP

basierte Protokolle wie OPC UA, das eine standardisierte Beschreibung des Informationsmodells eines Gerätes bis hin zur Produktionsanlage ermöglicht oder auch drahtlose Verbindungen zum Beispiel auf Basis von WLAN.

Die Handhabung der Daten für die Speicherung bis hin zur Archivierung erfolgt zunehmend in Datenbanken, die beispielsweise die in IEC und ISA standardisierte Datenbanksprache „Structured Query Language“, kurz SQL, benutzen und damit eher proprietäre Lösungen wie CSV-Dateien oder Tool-spezifische Formate ablösen. Diese Aufgaben sind den Schichten „Datenspeicherung“ und „Datenverarbeitung“ zuzuordnen und werden in diesem Leitfaden nicht weiter behandelt.

Gerade der Einsatz Ethernet-basierter Kommunikationsprotokolle und die damit prinzipiell mögliche Durchgängigkeit der Kommunikation von der Feldebene bis hin zur Ebene des Enterprise Resource Planning (ERP) erfordern die Betrachtung von Sicherheitsanforderungen. Diese kann man jedoch nicht pauschal bewerten, sondern muss dies fallspezifisch untersuchen. Ein bewährtes Vorgehensmodell stellt hierfür die STRIDE-Analyse dar.

Ein weiterer wichtiger Punkt für den Einsatz eines industriellen Kommunikationssystems ist die damit verbundene Skalierbarkeit des Netzwerks. Ändern sich Anforderungen, sollen neue Kommunikationsteilnehmer mit wenig Aufwand in das Netzwerk integrierbar sein. Eine entscheidende Voraussetzung dafür ist allerdings, dass standardisierte Lösungen eingesetzt werden.



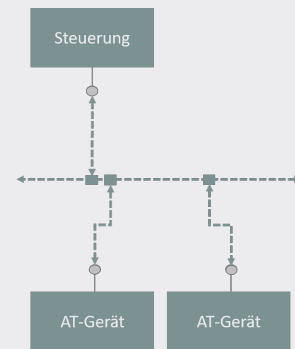
Aufbau von Kommunikationsnetzen

Wir möchten Ihnen nun die wichtigsten fünf Netzwerktopologien vorstellen, die unterschiedlich aufgebaut und im Falle von kabelgebundenen Netzen auch entsprechend verlegt werden. Dieser reale Aufbau wird auch als physische Topologie bezeichnet. Folgende Arten der Leitungen und Kabel zwischen den Geräten sind verbreitet. Die folgenden Abbil-

dungen nutzen die aus Sicht der Automatisierungstechnik typischen Gerätetypen wie Steuerung und AT-Gerät, das können Sensoren oder Aktoren sein, zur Veranschaulichung. Aus klassischer Sicht erfolgt der Informationsfluss vom Sensor zur Steuerung und diese sendet Sollwerte an die Aktoren, die dann wieder auf den zu steuernden Prozess einwirken.

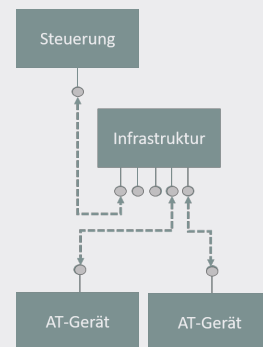
Bustopologie

Bei der Bustopologie werden alle Kommunikationsteilnehmer über ein Kabel miteinander verbunden. Die physischen Anschlüsse an den Bus können entweder über spezielle Anschlussklemmen oder auch direkt von Gerät zu Gerät erfolgen, in dem zum Beispiel zwei Kabel in einem Busstecker miteinander verbunden sind und der Stecker gleichzeitig die Verbindung zum Gerät darstellt. Durch diese Art der Kabelverlegung können sehr kurze Wege der Datenübertragung ermöglicht werden.



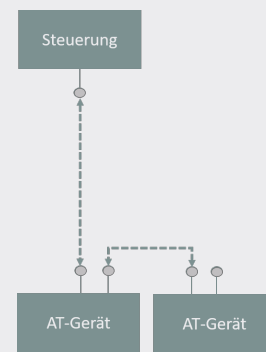
Sterntopologie

Die Sterntopologie benötigt in der Regel eine zusätzliche Komponente zur Verteilung des Informationsflusses auf dedizierte physische Verbindungen, die jeweils zwischen dem Gerät und der Infrastrukturkomponente vorhanden sind. Der Vorteil bei dieser Topologie liegt in der einfacheren und in der Regel schnelleren Datenübertragung zwischen der Infrastrukturkomponente und dem Gerät. Wie auch beim konventionellen direkten Anschluss von Sensoren und Aktoren an die I/O-Baugruppen der Steuerung wird zusätzliche Hardware benötigt und die Kabellängen sind enorm.



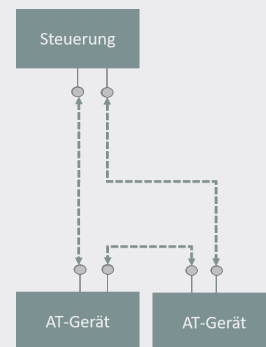
Linientopologie

Bei der Linientopologie erfolgt die Verbindung gerichtet von einem Gerät zum nächsten. Dabei kommt den Geräten die Aufgabe zu, eintreffende Daten, die nicht für sie bestimmt sind, am jeweils anderen Anschluss wieder auszugeben und damit weiterzuleiten. Analog zur Bustopologie können hier auch Kabellängen optimiert werden.



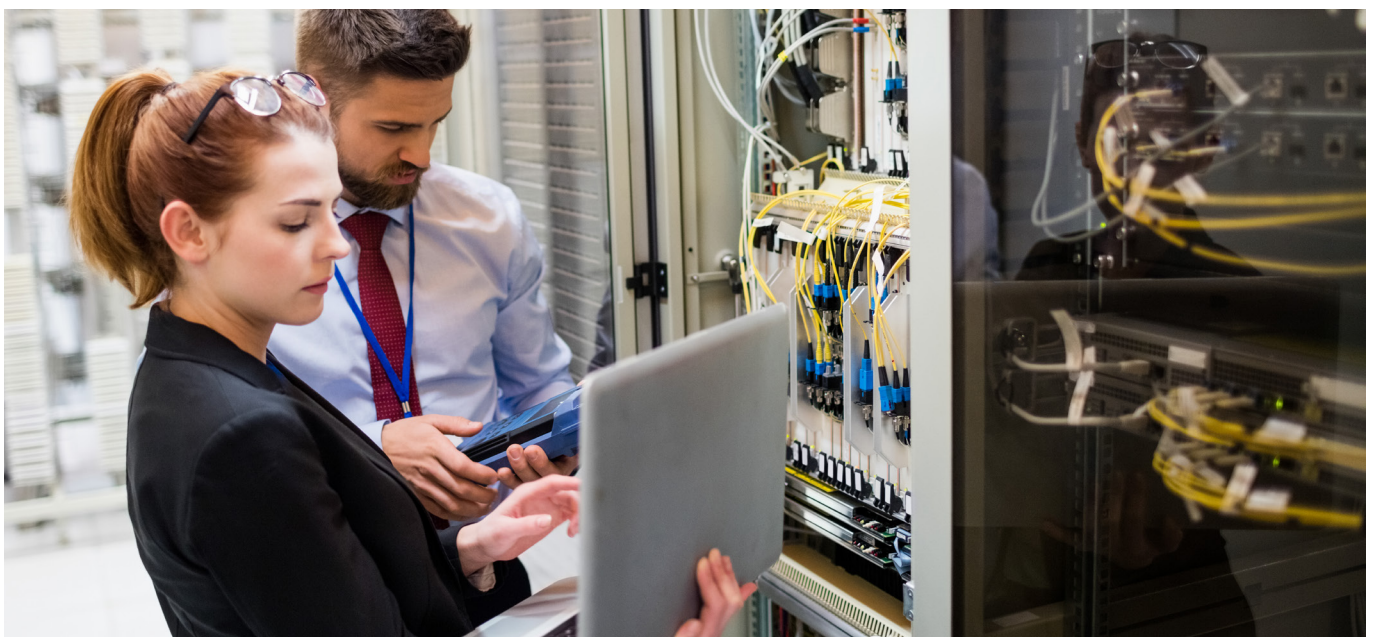
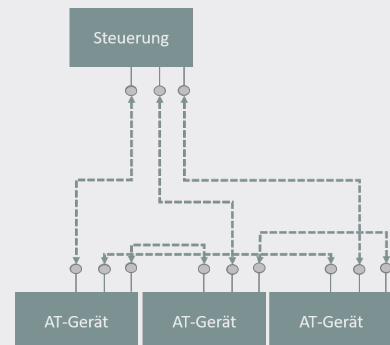
Ringtopologie

In der Ringtopologie steckt eine Erweiterung der Linientopologie, bei der in der Regel Daten über eine Verbindung gesendet und über die weitere Verbindung empfangen werden. Damit werden wie bei der Sterntopologie einfachere Verbindungen zwischen den Geräten möglich. Weitere Vorteile liegen darin, über beide Verbindungspunkte zu senden und zu empfangen, damit redundante Übertragungswege zu ermöglichen und die Fehlerdiagnose zu verbessern.



Vermaschte Topologie

Das vermaschte Netzwerk ist eine Erweiterung der Ringtopologie in der Art, dass es mehrere physische Verbindungen zwischen den Geräten gibt. Im Idealfall ist jedes Gerät mit jedem anderen verbunden, was natürlich bei größeren Netzwerken nicht mehr realisierbar und ökonomisch sinnvoll ist.





KAPITEL 3: KOMMUNIKATIONSSYSTEME UND INTEGRATIONSTECHNOLOGIEN

In diesem Kapitel geben wir Ihnen eine Übersicht an die Hand, die einen schnellen Überblick über typische Kommunikationsstandards für die Fertigungstechnik und die Prozesstechnik zulässt. Darüber hinaus nennt und beleuchtet der folgende

Überblick Technologien für die Integration der Geräte beziehungsweise Maschinen in die Leittechnik sowie Kommunikationstechnik für die Nutzung der Daten der Feld- und Produktionsebene in Ihrem Unternehmen.

PROFIBUS

Der Process Field Bus ist der Feldbus-basierte Automatisierungsstandard von PROFIBUS & PROFINET International. PROFIBUS verbindet Steuerungen beziehungsweise Leitsysteme mit den Sensoren und Aktoren der Feldebene. Die Abbildung zeigt die beiden Hauptklassen von PROFIBUS: PROFIBUS-DP steht für Dezentrale Peripherie und wird typischerweise in der Fertigungstechnik eingesetzt. PROFIBUS-PA bezeichnet die Lösung für die Prozessautomation. Beiden Auslegungen ist gemein, dass sie den gleichzeitigen und durchgängigen Datenaustausch mit übergeordneten Systemen ermöglichen.

Das grundlegende Protokoll bei PROFIBUS ist DP. Damit lässt sich ein modularer Aufbau ermöglichen, bei dem verschiedene Anwendungsprofile eingesetzt werden können. Die reine Datenübertragung kann für den Einsatzzweck entsprechend optimal ausgelegt werden. Es steht eine auf Kupferkabel basierte Übertragung entsprechend RS485 sowie Manchester Bus Powered (MBP) zur Verfügung. Für PROFIBUS-DP ist eine Bandbreite bis zu 12.000 Kbit/s bei 100 m Leitungslänge in der Fertigungstechnik spezifiziert. Bei 9,6 Kbit/s - 187,5 Kbit/s beträgt die zulässige Kabellänge 1000 m. Standardisiert ist PROFIBUS in der IEC 61158-2. Genutzt wird die Bustopologie.

Neben der kupferkabelbasierten Übertragung können auch Lichtwellenleiter (LWL) für eine Linientopologie eingesetzt werden. Häufig werden solche LWL-Lösungen eingesetzt, um neben der erhöhten EMV-Störsicherheit größere Distanzen bis zu 5 km zu überbrücken oder eine galvanische Trennung zwischen den Geräten vorzunehmen. In Ringtopologie aufgebaute LWL-Netze weisen außerdem eine Redundanz in der Kommunikation auf.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

Max Felser: PROFIBUS Handbuch: Eine Sammlung von Erläuterungen zu PROFIBUS Netzwerken.
Epubli, ISBN 978-3-7375-5470-1

Manfred Popp: Profibus-Dp/DPV1 Grundlagen, Tipps und Tricks für Anwender. Hüthig, ISBN 3-7785-2781-9

Standards, Spezifikationen:

IEC 61158-2

Nutzerorganisationen:

PROFIBUS Nutzerorganisation e.V. (PNO)
Haid-und-Neu-Straße 7, 76131 Karlsruhe
<https://de.profibus.com>

PROFINET

PROFINET ist der offene Industrial Ethernet Standard von PROFIBUS & PROFINET International für die Automatisierung. Bereits die Bezeichnung PROFINET zeigt, dass die langjährigen Erfahrungen mit PROFIBUS einen nahtlosen Übergang in die weltweit etablierte Kommunikation über ETHERNET ermöglicht haben. PROFINET verwendet etablierte Standards der Ethernet-Technologie, wie TCP/IP (RFC 1180), UDP (RFC 768) und IP (RFC 791) oder auf physikalischer Ebene IEEE 802.3 100 Base TX, 100 Base FX oder wireless. PROFINET ist in IEC 61158 für Anwendungsprofile und IEC 61784-2 für die Echtzeitkommunikation standardisiert.

Das PROFINET-Konzept ist modular aufgebaut, so dass der Anwender die kaskadierbare Funktionalität selbst nutzen kann. Dies unterscheidet sich im Wesentlichen durch die Art des Datenaustauschs, um den teilweise sehr hohen Anforderungen an die Geschwindigkeit gerecht zu werden. PROFINET definiert die Kommunikation zwischen einer Steuerung (z.B. SPS)/ einem Supervisor (z.B. HMI-Tool) und den dezentral angeschlossenen Peripheriegeräten. PROFINET beschreibt den gesamten Datenaustausch zwischen Steuerungen (Geräte mit so genannter „Masterfunktionalität“, so zum Beispiel die übergeordnete Steuerung) und den Geräten (Geräte mit so genannter „Slavefunktionalität“, die prozessbezogenen Feldgeräte) sowie die Parametrierung und Diagnose, die typischerweise von einem Supervisor durchgeführt werden. PROFINET folgt dem Producer/ Consumer-Modell.

Prozessdaten und Alarme werden immer in Echtzeit (RT) übertragen. In PROFINET basiert Real-Time auf der Definition von IEEE und IEC, die nur eine begrenzte Zeit für die Ausführung von Real-Time Diensten innerhalb eines Buszyklus zulassen. Die RT-Kommunikation ist die Grundlage für den Datenaustausch bei PROFINET. Echtzeitdaten werden als höhere Priorität behandelt als Nicht-Echtzeitdaten, die mittels IT-Kommunikationsprotokollen TCP (UDP) / IP übertragen werden. Wie eng dieses Fenster ist, hängt von den geforderten Echtzeit-Eigenschaften ab. Mit der RT-Kommunikation können Buszykluszeiten im Millisekundenbereich erreicht werden.

Für sehr hohe Echtzeitanforderungen, wie sie im Bereich von Druckmaschinen, Walzwerken oder Anwendungen mit einer synchronen Betriebsart erforderlich sind, hat PROFINET die Betriebsart des isochronen Datenaustauschs – Isochronous Real-Time (IRT) – definiert. Um die hohen Anforderungen an die Taktsynchronität zu gewährleisten, verfügen PROFINET-Feldgeräte mit IRT-Funktionalität über integrierte Switch-Ports. Die Datenaustauschzyklen liegen in der Regel im Bereich von wenigen hundert Mikrosekunden. Der Unterschied zur Echtzeitkommunikation liegt vor allem in der Taktsynchronität. Neben der kupferkabelbasierten Übertragung können für PROFINET auch Lichtwellenleiter (LWL) eingesetzt werden. Mit LWL lassen sich die gleichen Topologien umsetzen, erhöhen jedoch gegenüber kupferkabelbasierten Leitungen die EMV-Störfestigkeit und ermöglichen die Überbrückung größerer Distanzen zwischen den Geräten. PROFINET-Netzwerke werden als Stern-, Linientopologie oder in Mischformen erstellt.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

Manfred Popp: Industrielle Kommunikation mit PROFINET. PROFIBUS Nutzerorganisation e.V. (Best.-Nr. 4.181).

Manfred Popp: Das PROFINET IO-Buch. Grundlagen und Tipps für Anwender. Heidelberg, Hüthig 2005, ISBN 3-7785-2966-8.

Standards, Spezifikationen:

IEC 61158
IEC 61784-2

Nutzerorganisationen:

PROFIBUS Nutzerorganisation e.V. (PNO)
Haid-und-Neu-Straße 7, 76131 Karlsruhe
<https://de.profibus.com>

EtherCAT

Bei der Entwicklung des Ethernet for Control Automation Technology lag der Schwerpunkt auf der schnellen Übertragung von Daten mit einer Zykluszeit unter 100 µs, auf einem geringem Jitter bei der Datenübertragung und einer Uhrzeitsynchronisation der Geräte. Vornehmlich sollen mit EtherCAT Anlagen wie Verpackungsmaschinen, schnelle Pressen oder Hydraulikregelungen gesteuert werden. EtherCAT unterstützt Linien-, Baum-, Ring- und Sterntopologien, wobei logisch jeweils eine Master-Slave-Kommunikation stattfindet. In der Regel ist die Steuerung auch der Kommunikationsmaster. Aus Sicht der Übertragung werden Daten zyklisch, tasksynchron (dann mit Uhrzeitsynchronisation) oder bedarfsgerecht azyklisch übertragen. Die Besonderheit liegt in der Verwendung eines so genannten Ring-Telegramms. Beim Empfang entnehmen die Slaves für sie bestimmte Prozessdaten und fügen ihrerseits Sensordaten in das Telegramm ein, bevor das Telegramm weitergesendet wird. Für die Kommunikation mit Standard-IT, zum Beispiel aus der Office-Welt, sind Gateways beziehungsweise Umsetzer notwendig, um Standard IT-Pakete durch ein EtherCAT Netzwerk zu senden.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

Grardus Blokdyk: EtherCAT A Complete Guide - 2021 Edition, ISBN-13 : 978-1867416265

Standards, Spezifikationen:

IEC 61158

IEC 61784

Nutzerorganisationen:

EtherCAT Technology Group

Ostendstraße 196, 90482 Nürnberg

www.ethercat.org

MODBUS

Bereits 1979 wurde das Kommunikationsprotokoll Modbus entwickelt. Es ist sehr einfach aufgebaut und folgt dem Master-Slave oder der Client/Server-Architektur. Die physische Übertragung erfolgt entweder seriell über eine RS232 oder RS485-Schnittstelle oder über TCP für Ethernet-basierte Systeme.

Modbus richtete sich in erster Linie an die Kommunikation zwischen Steuerungen, wurde jedoch schnell auch für die Kommunikation zwischen Steuerung und Geräten eingesetzt. Die Rollen der Geräte sind nicht fest zugeordnet, so dass ein hohes Maß an Flexibilität bei dezentralen AT-Architekturen gegeben ist. Der Datenaustausch beruht auf dem Zugriff auf Daten über Funktionscodes, analog erfolgt die Auswahl der Operation auf diese Daten. Modbus wird unter anderem für die Fernwartung von Automatisierungssystemen oder auch zur Konfiguration von Firewalls im Automatisierungsumfeld eingesetzt.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

Rob Hulsebos: Modbus The Manual: Definitive guide on Modbus, ISBN-13 : 978-9463867641

Standards, Spezifikationen:

www.modbus.org/specs.php

Nutzerorganisationen:

Modbus Organization

PO Box 628 Hopkinton, MA 01748

www.modbus.org

CAN

Das Bussystem Controller Area Network wurde für die Fahrzeugindustrie entwickelt, als ISO 11898-2 standardisiert und fand auch in der Automatisierungstechnik eine weite Verbreitung, weil vor allem die Anschaltungen sehr kostengünstig sind. Geräte werden an CAN in Linientopologie angeschlossen, wobei Übertragungsraten von bis zu 1 MBaud bei kurzen Distanzen (< 25m) erreicht werden. Verbreitet in der Automatisierungstechnik ist das spezielle Protokoll CANopen, das vor allem die Kommunikationsobjekte in Servicedaten (wie für die Parameterisierung oder Konfiguration), Prozessdaten für den Austausch von Echtzeitdaten, Netzwerkmanagement zur Steuerung des Gerätezustands sowie Objekte zur Fehlerbenachrichtigung oder für die Synchronisation definiert.

Objekte werden in CAN über den Identifier im Bussystem eindeutig identifiziert. In der Abbildung ist das CAN-Format mit 11 Bit Identifier dargestellt, daneben gibt es auch noch die Möglichkeit, 29 Bit-Identifier zu benutzen. Dies muss jedoch im System einheitlich erfolgen.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

Wolfhard Lawrenz und Nils Obermüller: CAN: Controller Area Network: Grundlagen, Design, Anwendungen, Testtechnik, ISBN-13 : 978-3800733323

Holger Zeltwanger: CANopen: Das standardisierte, eingebettete Netzwerk, ISBN-13 : 978-3800728459

Standards, Spezifikationen:

CAN: ISO 11898-2

CANopen: EN 50325-4

Nutzerorganisationen:

CAN in Automation

Kontumazgarten 3, 90429 Nürnberg

www.can-cia.org

SERCOS

Das „Serial Real-time COmmunication System“ liegt seit 2005 in der Spezifikation SERCOS III für die Ethernet-basierte Übertragung vor. Es findet besonders im Bereich der Antriebsregelung seinen Einsatz. SERCOS III erlaubt den Aufbau von Ring- und Linientopologien, wobei die Ringtopologie eine redundante Datenübertragung ermöglicht. Der Vorteil der Linientopologie liegt hier in der Ausdehnung des Gesamtnetzwerkes zwischen den Geräten. SERCOS III erlaubt sehr schnelle Zykluszeiten bis hinunter zu 31,25µs, wobei ein Zyklus immer aus einem logischen Echtzeit- und einem logischen Nicht-Echtzeitkanal besteht. Weiterhin erlaubt SERCOS III den direkten Datenaustausch zwischen den Geräten, ohne den Umweg über die zentrale Steuerung (logischer Busmaster) zu nehmen. Damit ist ein Verbinden von modularen und vernetzten Maschinen möglich. Die folgende Abbildung zeigt den Aufbau eines Datenfeldes innerhalb eines Ethernet-Datenpakets.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

N. P. Mahalik: Fieldbus Technology: Industrial Network Standards for Real-Time Distributed Control, ISBN-13 : 978-3642072840

Standards, Spezifikationen:

IEC 61491

IEC 61784

IEC 61158

IEC 61800-7

Nutzerorganisationen:

Sercos Nutzerorganisation

www.sercos.de

Ethernet/IP

Das EtherNet Industrial Protocol ist ein für die Industrieautomation entwickeltes Kommunikationsprotokoll, das auf die IP-Standards TCP und UDP aufsetzt. Damit sind jedoch seine Einsatzmöglichkeiten hinsichtlich der umsetzbaren Echtzeitanforderungen eingeschränkt. Ethernet/IP-Netzwerke können als Stern- oder Ringtopologie bzw. in gemischter Form ausgelegt werden. Die Anwendungsdaten werden auf Basis des Common Industrial Protocol™ (CIP) kodiert und entsprechend Producer-Consumer-Prinzip verteilt. Der Vorteil dieses Ansatzes ist, dass aus Sicht der Automatisierungsanwendung (Steuerungsprogramm) die gleichen Zugriffsmechanismen genutzt werden, wie sie schon bei den Kommunikationssystemen ControlNet und DeviceNet definiert wurden.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

Kristof Obermann und Martin Horneffer: Datennetztechnologien für Next Generation Networks: Ethernet, IP, MPLS und andere, ISBN-13 : 978-3834813848

Linus Schleupner: Umstellung eines Feldbusses auf Ethernet/IP: Echtzeitkommunikation im Maschinenbau, ISBN-13 : 978-3639457582

Standards, Spezifikationen:

IEC 61158, CPF2/2 EtherNet/IP

Nutzerorganisationen:

ODVA, Inc., Michigan USA
www.odva.org

Industrial WLAN

Im Consumerbereich ist das Wireless Local Area Network auch unter dem Marketingnamen WiFi bekannt. WLAN nutzt Frequenzbereiche mit 2,4 GHz und 5 GHz und ermöglicht aus Sicht der Nutzer im nicht industriellen Bereich eine Übertragungsleistung, die bis zum Streaming von Audio- und Videodaten reicht. Die Technik setzt einen zentralen Zugangspunkt (Access Point) voraus, mit dem sich alle Geräte (PCs, Smartphones, TVs) etc. per Funk verbinden. Der WLAN Access Point dient als Übergang vom kabelgebundenen Netzwerk zum Funknetzwerk. Die Einrichtung des Funknetzwerkes erfolgt über vorgegebene Netzwerknamen und Schlüsselworte und richtet sich in der Regel nach kundenspezifischen Vorgaben, die sich aus der vorhandenen IT-Infrastruktur ableiten.

Das industrielle WLAN basiert auf der gleichen technischen Basis, ändert jedoch bestimmte Techniken der Medium-Zuordnung im Access Point für die Gerätekommunikation so ab, dass die geänderten Anforderungen an die Datenübertragung (in der Regel kleine Datenmengen, dies aber möglichst in gleichen Abständen) gewährleistet werden. Mitunter werden auch abgewandelte Verfahren zur Verschlüsselung der Kommunikation eingesetzt, da die üblicherweise eingesetzten Sicherheitsstandards nach IEEE 802.11a, b, g, n und ac durchaus angreifbar sind. Im Industrieumfeld laufen die Geräte jedoch ununterbrochen durch und sollen auch viele Jahre störungsfrei ihren Dienst versehen. Wichtig für die Einrichtung solcher Netzwerke ist zudem, eine praktikable Lösung anzubieten. Dies bedeutet, dass die Infrastrukturkomponenten wie Access Points des Industrial WLAN über die existierenden herstellerspezifischen Engineeringwerkzeuge konfigurierbar sind.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

https://de.wikipedia.org/wiki/Industrial_Wireless_Local_Area_Network

Standards, Spezifikationen:

Normenreihe IEEE 802.11

Typische Kommunikationsstandards für die Prozesstechnik

PROFIBUS-PA

Im Gegensatz zu PROFIBUS-DP nutzt PROFIBUS-PA eine an den Einsatzzweck angepasste Übertragungsschicht, bei der über eine Zweidrahtleitung die Energieversorgung der Geräte und die digitale Kommunikation nach dem Manchester Bus Powered-Verfahren erfolgt. Dabei kann die elektrische Leistungsübertragung so begrenzt werden, dass auch ein Einsatz im explosionsgefährdeten Raum ermöglicht wird. Insgesamt kann sich ein PROFIBUS-PA Strang über eine Länge von 1900 m erstrecken, wobei die Übertragungsrate auf 31,25 kBaud reduziert ist, die jedoch für verfahrenstechnische Prozesse in der Regel ausreichend ist. Aus Sicht der Steuerung können die gleichen Kommunikationsdienste wie bei PROFIBUS-DP benutzt werden.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

Christian Diedrich: PROFIBUS PA – Instrumentierungstechnologie für die Verfahrenstechnik. Oldenbourg, ISBN 3-8356-3056-3

Christian Diedrich, Thomas Bangemann: Profibus PA, Oldenbourg Industrieverlag, ISBN 978-3-8356-3125-0

Standards, Spezifikationen:

IEC 61158-2

Nutzerorganisationen:

PROFIBUS Nutzerorganisation e.V. (PNO)
Haid-und-Neu-Straße 7, 76131 Karlsruhe
<https://de.profibus.com>

HART

Mit dem Highway Addressable Remote Transducer wurde auf Basis der analogen 4-20mA Signalübertragung eine digitale Informationsübertragung ermöglicht, die nach dem Bell-202 Standard arbeitet. Damit können unter anderem parallel Mess- oder Sollwerte über den analogen Kanal und Parametrierungs- oder Diagnosedaten über den digitalen Kanal übertragen werden. Konzeptionell ist HART als eine bidirektionale Punkt-zu-Punkt-Verbindung, in der Regel zwischen einer Steuerung und einem Feldgerät, ausgelegt.

Aus Sicht der Kommunikation ist es wichtig, auch Geräte im explosionsgefährdeten Raum ansprechen zu können. Dies wird durch die geringe Übertragungsenergie ermöglicht, wobei bei einer Zweidrahtverbindung auch gleichzeitig die Energieversorgung des Feldgerätes mit übernommen wird. Neben der Punkt-zu-Punkt-Verbindung lassen sich auch Multidrop-Systeme aufbauen, bei denen dann die Energieversorgung der Feldgeräte separat erfolgt, aber die Feldgeräte wie an einer Art Bus parallel angeschaltet werden können.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

www.fieldcommgroup.org/de/technologien/hart/hart-technologie-im-detail

James Powell: HART Communication Protocol: A Practical Guide, ISBN-13 : 978-1655583711

Standards, Spezifikationen:

IEC 61158, CPF9 HART

Nutzerorganisationen:

FieldComm Group
9430 Research Blvd, Suite 1-120
Austin, TX 78759

WirelessHART

WirelessHART ist eine funkbasierte Lösung, die auf vermaschten Verbindungen zwischen den Netzwerkknoten aufbaut. Schwerpunkt bei der Entwicklung der Kommunikationslösungen ist die Überbrückung großer Distanzen, wie sie in der Prozessindustrie üblich sind. WirelessHART baut auf den Standard IEEE 802.15.4 und nutzt das ISM-Band, in dem eine lizenzfreie Kommunikation wie bei WLAN möglich ist. Die Übertragung selbst ist AES 128 kryptografisch gesichert.

In dem vermaschten Funknetz kann jedes Gerät als ein Router für Nachrichten von anderen Geräten dienen. Das bedeutet, es werden Nachrichten weitergeleitet. Dadurch wird die geforderte große Reichweite des Funknetzwerks erreicht. Die Funkanschlungen können entweder direkt in dem Feldgerät oder in Gateways integriert sein, die dann wiederum an die kabelgebundene Netzwerkstruktur des Unternehmens angebunden sind oder separate Teilnetze ermöglichen.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

www.fieldcommgroup.org/de/technologien/hart/hart-technologie

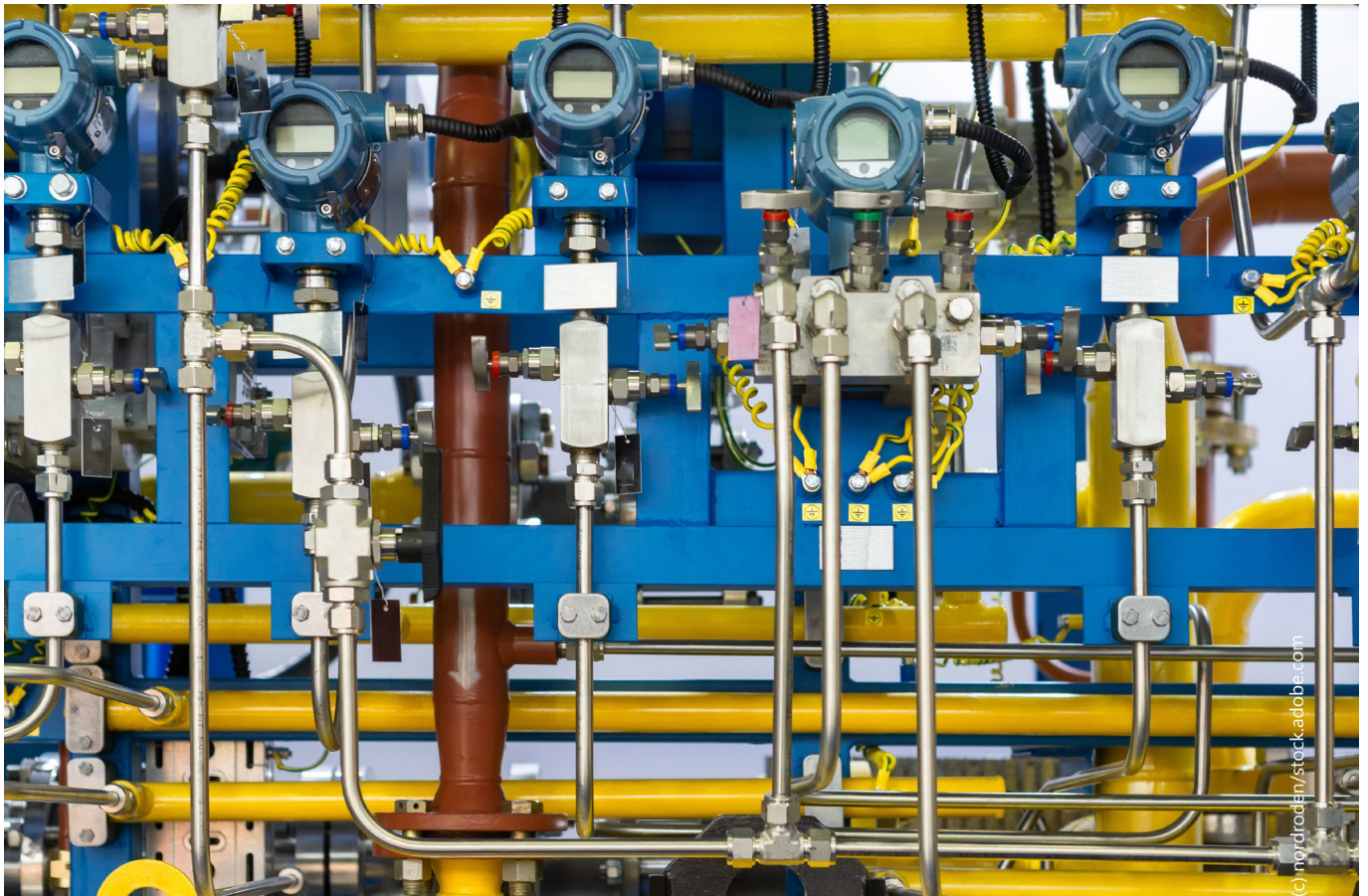
Deji Chen, Mark Nixon, et al.: WirelessHART™: Real-Time Mesh Network for Industrial Automation, ISBN-13 : 978-1441960467

Standards, Spezifikationen:

IEC 62591:2016 Industrial networks - Wireless communication network and communication profiles - WirelessHART™

Nutzerorganisationen:

FieldComm Group
9430 Research Blvd, Suite 1-120
Austin, TX 78759



Technologien für die Integration der Geräte und Maschinen in die Leittechnik

Moderne automatisierungstechnische Geräte mit Kommunikationsschnittstelle müssen aus zweierlei Sicht integriert werden. Zum einen betrifft das die Integration in das Kommunikationssystem. Dabei werden Festlegungen wie die Geräteadresse, die zu benutzende Übertragungsgeschwindigkeit oder Positionen von Gerätedaten innerhalb des Kommunikationsprotokolls vergeben. Häufig werden die damit verbundenen Arbeitsschritte auch als Parametrierung bezeichnet. Zum anderen muss ein Gerät in den Steuerungsprozess integriert werden. Damit verbunden ist die Anpassung des Gerätes selbst an den zu steuernden Prozess. Beispiele hierfür sind bei Füllstandssensoren die Bekanntgabe der Tankgeometrie, bei Temperatur-

transmittern die Maßeinheit (K, °C) oder der Verstellbereich bei Stellantrieben. Wurden diese Einstellungen vorgenommen, kann eine Steuerung oder ein Leitsystem, wie bei großen verfahrenstechnischen Anlagen, die übermittelten Daten richtig interpretieren und notwendige Eingriffe in den Produktionsprozess vornehmen. Sowohl für die Gerätehersteller als auch die Betreiber eines Produktionssystems ist es immens wichtig, diese Geräteintegration auf Basis von Standards durchzuführen. Damit ist eine Gerätetyp-übergreifende einheitliche Bedienung der notwendigen Arbeitsaufgaben möglich.

OPC UA

OPC UA ist die aktuelle Zusammenfassung von Spezifikationen zur Unterstützung des Datentransports von der Automatisierungsebene hin zu Softwarewerkzeugen, die auf bürotypischen Plattformen wie PCs laufen. Auf solchen Plattformen werden mitunter Aufgaben wie das Controlling oder das Produktionsmanagement wahrgenommen. In der langen Geschichte der Entwicklung der Spezifikationen, die unter der Obhut der OPC Foundation entstanden, wurde das Akronym OPC auch neu definiert und steht momentan für Open Platform Communications. Der Zusatz UA umreißt die Zusammenfassung verschiedener IT basierter Lösungen für die Datenmodellierung in Form eines generischen Informationsmodells und darauf arbeitenden Diensten wie Lesen, Schreiben von Datenpunktwerten, die automatische Benachrichtigung bei Wertänderungen oder die Ausführung einer bestimmten Funktion, die dann in der Regel Einfluss auf mehrere Datenpunkte im Informationsmodell ausübt. Damit lassen sich komplexere Zusammenhänge zwischen den Datenpunkten des Informationsmodells konsistent manipulieren oder bestimmte Aktionen ausführen. OPC UA setzt von der Architektur her auf eine Client-Server-Lösung, wobei der Server hier die Daten der Automatisierung bereitstellt und Clients diese Daten bei Bedarf anfragen beziehungsweise manipulieren. Die Kommunikation zwischen Client und Server beruht in der Regel auf Ethernet-IP und hier insbesondere TCP. Die Daten selbst können XML-formatiert oder in einem Binärformat übertragen werden. Letzteres steigert die Effizienz. Weiterhin kann die Übertragung durch SSL oder TLS gesichert erfolgen. OPC UA sieht hierfür die Nutzung von Zertifikaten vor, so dass nach deren Einrichtung ein automatischer Verbindungsaufbau erfolgen kann.

Neu im Fokus von OPC UA ist auch die Nutzung des Publisher/Subscriber Mechanismus zwischen OPC UA Komponenten. Hierbei werden die Daten auch nur übertragen, wenn sich die Werte in den Datenpunkten geändert haben. Die empfangende Komponente (Subscriber) meldet die interessierenden Daten zuvor beim Publisher an, so dass eine effiziente Kommunikation erfolgen kann. Die Kommunikation selbst kann wieder Ethernet-IP basiert erfolgen, wobei das zustandslose Protokoll UDP oder der Broker-Dienst von MQTT eingesetzt werden kann. Die Daten liegen dabei entweder wieder binär codiert oder im JSON-Format vor.

Das Informationsmodell in OPC UA kann anwendungsbezogen gestaltet werden. In der Regel werden Hierarchien von Datenpunkten (Variablen), Methoden und Attribute beschrieben und vom OPC UA Server zur Laufzeit genau in dieser Form bereitgestellt. Die OPC Foundation definiert in verschiedenen Spezifikationen Grundmodelle eines Informationsmodells, die dann in der Regel anwendungsspezifisch erweitert werden.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

Wolfgang Mahnke, Stefan-Helmut Leitner, Matthias Damm: OPC Unified Architecture, ISBN-13 : 978-3540688983

Standards, Spezifikationen:

Serie der IEC 62541

Nutzerorganisationen:

OPC Foundation
16101 N. 82nd Street, Suite 3B
Scottsdale, AZ 85260-1868 USA

Field Device Integration – FDI

Field Device Integration ist eine Geräteintegrationstechnologie, die in erster Linie für die Prozessindustrie entwickelt wurde, um die unterschiedlichen Gerätetypen verschiedener Hersteller einheitlich in übergeordnete Steuerungssysteme zu integrieren.

Die FDI-Technologie wurde von den führenden Technologieorganisationen der Automatisierungstechnik und deren Mitgliedern entwickelt und wird von der Automatisierungsbranche weltweit unterstützt. Mit FDI werden die Vorteile von FDT® (programmierbare Komponenten vornehmlich auf MS-Windows basierten Computern) mit denen von EDDL (interpretierbare, plattformunabhängige Gerätebeschreibung) in einer einzigen, skalierbaren Lösung kombiniert. FDI berücksichtigt die unterschiedlichen Aufgaben über den gesamten Lebenszyklus einfacher und komplexester Geräte, einschließlich Konfiguration, Inbetriebnahme, Diagnose und Kalibrierung. FDI ist in IEC 62769 standardisiert.

Eine FDI-fähige Lösung erfordert zwei Komponenten: 1) Ein Host-System, das FDI unterstützt. Host-Beispiele sind Steuerungssysteme, Konfiguratoren und Asset-Management-Software. Die zweite Komponente sind Automatisierungsgeräte beziehungsweise -komponenten, die in den Host integriert werden. Technisch erfolgt diese Integration über FDI-Packages. 2) Ein FDI-Paket repräsentiert einen Gerätetyp und es wird von allen Werkzeugen oder Systemen verwendet, von Handheld-Geräten und Einzel-PCs bis hin zu kompletten Prozessautomatisierungssystemen mit ausgefeilten Steuerungs- und Asset-Management-Funktionen. In der Regel sind komplexe Prozessautomatisierungssysteme modular aufgebaut. Die FDI Spezifikation sieht für die logische und räumliche Trennung von Softwarekomponenten eines FDI Hosts die Nutzung von OPC UA als Standardschnittstelle vor und definiert ein Informationsmodell zur eindeutigen Abbildung der verwalteten Automatisierungsgeräte und deren Parameter. Für FDI wurde das „Information Model for Devices“ als Basis herangezogen und darauf aufbauend wurden Konzepte für die Abbildung von Netzwerkstrukturen, deren Verschaltung, Sichten auf Feldgeräte und deren Parameter oder interne Strukturen wie Funktionsblöcke bis hin zur Beschreibung der Bedienoberflächen erstellt.

Der Einsatz solcher Tools ist auf dem neuesten Stand der Technik, auch bei einfachen Feldgeräten, die nicht viel Aufwand für die Integration in die Steuerungsarchitektur benötigen. Im Prinzip beschreibt ein Gerätepaket ein Feldgerät oder eine Infrastrukturkomponente wie Gateways in Bezug auf:

- Definition allgemeiner Aspekte eines Gerätes (Def)
- Die Geschäftslogik des Gerätes (BL)
- Struktur und Inhalt der Benutzeroberfläche (UID)
- Optionale Plug-Ins für die Benutzeroberfläche (UIP)
- Anhänge, wie Dokumentation oder signaturgeschützte Zertifikate.

Die Gerätedefinition (Def) beschreibt die Daten des Feldgerätes und die interne Struktur (zum Beispiel Blöcke). Die Geschäftslogik (BL) des Gerätes stellt in erster Linie sicher, dass die Gerätedaten konsistent bleiben (zum Beispiel Daten aktualisieren bei einem Gerätewechsel). Die User Interface Descriptions (UID) und User Interface Plug-ins (UIP) definieren die Benutzeroberflächen der Feldgeräte. Die obligatorische UID ermöglicht den vollständigen Betrieb eines Feldgerätes. Die optionalen User Interface Plug-ins (UIPs) bieten die Vorteile der von FDT bekannten, frei programmierbaren Benutzeroberflächen auf Basis der Windows Presentation Foundation (WPF). Aktuelle Spezifikationserweiterungen sehen auch eine Bereitstellung in HTML5 vor.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

Großmann, Daniel; Braun, Michael; Danzer, Benjamin; Riedl, Matthias: FDI - Field Device Integration, ISBN 978-3-8007-3513-6, E-Book: ISBN 978-3-8007-3815-1

www.fieldcommgroup.org/de/tags/technologies/field-device-integration

Standards, Spezifikationen:

Serie der IEC 62769

Nutzerorganisationen:

FieldComm Group
9430 Research Blvd, Suite 1-120
Austin, TX 78759
<https://fieldcommgroup.org>

FDT

Die FDT-Technologie ist ein offener Standard für die unternehmensweite Netzwerk- und Geräte-Integration und beschreibt die Art und Weise, wie in industriellen Automatisierungsarchitekturen Sensoren und Aktoren mit der Bedien- und Leittechnik kommunizieren können. Die kontinuierliche Weiterentwicklung dieser Technologie greift Entwicklungen wie das Industrial Internet of Things (IIoT) und Industrie 4.0 auf, um technologisch neue Aspekte für die vertikale Integration des Datenaustauschs zu berücksichtigen. Ebenso wie FDI ermöglicht eine auf FDT basierende Software-Infrastruktur die Interoperabilität, Integration sowie eine einheitliche Sicht auf alle Daten und Funktionen der Geräte und Steuerungsanwendungen.

FDT ist in IEC 62453 standardisiert. Es unterstützt eine offene Schnittstellenarchitektur für die Vernetzung der Automatisierungnetzwerke und Anlagen der industriellen Automatisierung. Erster Ansatzpunkt für die Entwicklungen war die unternehmensweite Weitergabe gerätespezifischer Diagnosedaten wie die Parametrierung der Geräte.

In FDT werden Geräte- und Infrastrukturkomponenten durch einen Device Type Manager (DTM) repräsentiert. Dieser wird als Softwarekomponente bereitgestellt und enthält alle Geräteparameter und Bedienoberflächen, die für den Umgang mit dem Automatisierungsgerät notwendig sind. Integriert wird der DTM in eine Rahmenapplikation (FDT-Frame), die die DTMs verwaltet und bei Bedarf startet.

Ergänzt wird FDT durch die Nutzung von OPC UA für die Integration der Automatisierungsdaten in größere Netzwerke, beispielsweise in höhere Unternehmensleitebenen.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

www.fdtgroup.org/category/articles

René Simon et al.: Field Device Tool - FDT

Standards, Spezifikationen:

Serie der IEC 62453

Nutzerorganisationen:

FDT Group AISBL

5 Industrieweg, 3001 Heverlee - Belgium

www.fdtgroup.org



Kommunikationstechnik für die Nutzung der Daten der Feld- und Produktionsebene im Unternehmen

Unabhängig von den Kommunikations- und Integrationstechnologien, die aus Sicht der etablierten Automatisierungshersteller vorangetrieben werden, haben Entwicklungen aus der IT durchaus ihren Einfluss auf die industrielle Kommunikation. Diese Kommunikationslösungen wurden aus anderen Blickwinkeln, Aufgabenstellungen und technischen Ressour-

cen heraus entwickelt. Mit den im Folgenden vorgestellten Kommunikationstechnologien lassen sich ebenfalls Daten aus der Feldebene verarbeiten, ohne jedoch auf Vorüberlegungen von Nutzerorganisationen oder Standards zurückgreifen zu können.

MQTT

Message Queue Telemetry Transport setzt als Applikationsprotokoll auf IP/TCP-Kommunikation auf. MQTT ist ein leichtgewichtiges Machine-to-Machine-Protokoll für den Nachrichtentransport. Es ist eine der derzeit populärsten Publish-Subscribe Lösungen und wurde ursprünglich für die Datenerfassung von sehr vielen Datenquellen/Geräten entwickelt. Dieses Protokoll ist eine zentralisierte Publisher/Subscriber-Implementierung und wird häufig im IoT-Umfeld eingesetzt. Zentraler Punkt ist ein dedizierter Broker, der themenbasierte Daten vom Publisher entgegennimmt und an Abonnenten weiterleitet, die sich für dieses Thema interessieren.

Darüber hinaus verwendet es das verbindungsorientierte Transportprotokoll TCP und TLS/SSL für die gesicherte Kommunikation. Es gibt eine Abwandlung von MQTT, die speziell für Sensornetze (SN) ausgelegt ist. Während MQTT eine verlustfreie Verbindung über TCP/IP erfordert, wurde MQTT-SN entwickelt, um unabhängiger vom zugrundeliegenden Netzwerkprotokoll zu sein. In der Regel wird dieses Derivat in Verbindung mit dem verbindungslosen IP-Protokoll UDP verwendet, das aufgrund fehlender Zuverlässigkeitsmechanismen weniger Kommunikationsaufwand auf der Transportschicht verursacht. Bei ressourcenbeschränkten eingebetteten Geräten wie Knoten in Sensornetzwerken können die zusätzlichen Energiekosten einer zuverlässigen verbindungsbasierten TCP-Übertragung einen großen Einfluss auf den Energieverbrauch und damit auf die Batterielaufzeit haben. In der Regel bleibt ein solches Gerät lange Zeit in einem Low-Power-Zustand (Sleep-Modus) und wacht nur durch die Unterbrechung eines externen Triggers oder Timers auf. In dieser Phase sendet das Gerät nur eine oder wenige Nachrichten und geht wieder in den Schlafmodus. Bei der Verwendung einer TCP-basierten Kommunikation müssen neben den Datennachrichten, aufgrund von Verbindungsaufbau, -pflege und -abbau, zusätzliche Management-Nachrichten gesendet werden. Im Vergleich dazu werden bei verbindungslosen Protokollen nur die notwendigen Datennachrichten übertragen. Ein wesentlicher Unterschied zum normalen MQTT ist neben dem Wechsel des Transportschichtprotokolls die Notwendigkeit eines Gateways zwischen Publisher/Subscriber und Broker. Die Geräte, auf denen ein Publisher oder Subscriber läuft, verwenden ein verbindungsloses Protokoll wie UDP. Die Kommunikation zwischen dem Broker und dem UDP-Gateway basiert jedoch weiterhin auf TCP-Kommunikation.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

<http://mqtt.org>

<https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html>

Gaston C. Hillar: MQTT Essentials - A Lightweight IoT Protocol (English Edition): Send and receive messages with the MQTT protocol for your IoT solutions., ISBN-13 : 978-1787287815

Standards, Spezifikationen:

OASIS Standard für MQTT 5.0

Nutzerorganisationen:

Die Spezifikation wird seit 2013 von der „Organization for the Advancement of Structured Information Standards (OASIS)“ gepflegt.

OPC UA

OPC-UA ist im Prinzip ein flexibles Machine-to-Machine-Kommunikationsprotokoll, das von der OPC-Foundation speziell für die industrielle Automatisierung mit dem Ziel entwickelt wurde, alle bisherigen beziehungsweise bestehenden Feldbus-Kommunikationsprotokolle auf einer höheren Abstraktionsebene nutzen zu können. Diese Abstraktion wird durch ein unabhängiges Informationsmodell erreicht. Softwarekomponenten und Programme, die über OPC UA auf Daten der Feldebene zugreifen möchten, nutzen Daten aus dem Informationsmodell in einer generischen Art. Dies erleichtert die Interoperabilität auf verschiedenen Ebenen der Informationsverarbeitung.

Das Hauptaugenmerk bei der Entwicklung von OPC UA liegt auf dem Austausch von beliebig komplexen Informationsmodellen. Diese sind technisch so gestaltet, dass sie selbstbeschreibend sind und eine Interoperabilität zwischen Maschinen auf semantischer Ebene ermöglichen. Es lässt sich damit eine breite Palette von Systemen unterstützen, die von Steuerungen bis hin zu einfachen Feldgeräten reichen und sich durch ihre Vielfalt in Bezug auf Größe, Leistung, Plattformen und Funktionsfähigkeiten auszeichnen. Zu diesem Zweck wurde OPC-UA speziell unter expliziter Berücksichtigung folgender Merkmale entwickelt:

- Unabhängigkeit von den Funktionalitäten des vorhandenen Geräte-Betriebssystems
- Die explizite Berücksichtigung von Sicherheitsaspekten der Kommunikation, so dass Datenmanipulationen verhindert werden können
- Daten semantisch so beschreiben, dass nicht nur einfache Bits oder Bytes, sondern auch komplexe Datentypen einfach ausgetauscht werden können

Das Protokoll unterstützt zwei verschiedene Arten von Kommunikationsparadigmen: Client/Server sowie Publish und Subscribe, wobei der OPC-UA-Server so konfiguriert ist, dass bestimmte Informationen automatisch an OPC-UA-Clients geliefert werden, die daran interessiert sind, Informationen zu erhalten. Beide Lösungen sind zudem unabhängig von der zugrundeliegenden Transportschicht und können je nach Anwendung und zu realisierender Performance über beispielsweise TCP, HTTP, HTTPS sowie UDP, AMQP oder MQTT durch die Implementierung unterschiedlicher Transportprofile genutzt werden.

Informationen im Detail, nützliche Links

Allgemeine Beschreibungen:

Wolfgang Mahnke, Stefan-Helmut Leitner, Matthias Damm: OPC Unified Architecture,
ISBN-13 : 978-3540688983

Standards, Spezifikationen:

Serie der IEC 62541

Nutzerorganisationen:

OPC Foundation
16101 N. 82nd Street, Suite 3B
Scottsdale, AZ 85260-1868 USA



Safety und Security in der industriellen Kommunikation

Die Beachtung von Sicherheitsanforderungen hat aus Sicht der Automatisierungstechnik vor allem aus dem Blickwinkel der funktionalen Sicherheit stattgefunden. Dabei soll vor allem sichergestellt werden, einen Schaden für Mensch und Ausrüstung zu vermeiden. Die Informationssicherheit hat lange Zeit nur eine untergeordnete Rolle im Rahmen der industriellen Kommunikation gespielt. Lediglich die Sicherstellung der korrekten Übertragung von Informationen wird sichergestellt, jedoch nicht authentifiziert. Die Authentifizierung ist aufgrund des Engineerings bisher auch nicht notwendig gewesen, da

bei den meisten Vorgehensweisen die Feldgeräte als Typ explizit durch den Planungsingenieur in das System integriert wurden, eine Zuordnung zu einer Adresse im Kommunikationssystem entweder manuell oder durch das Engineeringwerkzeug erfolgte oder nur eine direkte Kommunikation wie bei HART vorlag. Durch die Nutzung von IT im Produktionsumfeld sind die Anlagenbetreiber jedoch neuen Bedrohungen ausgesetzt. Die Auswirkungen, die Lücken in der Informationssicherheit hervorrufen, können beachtlich sein.



STRIDE

Eine Möglichkeit, sich über die daraus entstehenden Bedrohungen einen Überblick zu verschaffen, diese Bedrohungen einzuschätzen und Maßnahmen dagegen zu unternehmen, liefert die STRIDE-Analyse ([https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v=cs.20\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN)). Diese Analyse deckt die Empfehlungen ab, die das Bundesamt für Sicherheit und Informationstechnik (BSI) herausgegeben hat (https://www.bsi.bund.de/DE/Themen/ICS/Empfehlungen/ICS/empfehlungen_node.html). STRIDE wurde von Microsoft zunächst für die Analyse von Computersicherheitsbedrohungen entwickelt, kann aber auch für andere Systeme verwendet werden. Der Name kommt von den Initialen der verschiedenen Bedrohungskategorien, die das Modell abdeckt. Basis für eine informationstechnisch sichere Übertragung sind Verschlüsselungsprotokolle, die in Kommunikationsprotokolle integriert sind beziehungsweise diese nutzen.

TLS

Die Transport Layer Security, kurz TLS, ist eine der grundlegenden Techniken für die Verschlüsselung des Datenaustauschs bei Ethernet-basierter Kommunikation. Die Verschlüsselung baut auf Zertifikaten auf, um die Vertrauenswürdigkeit des Kommunikationspartners zu prüfen. Für die Verschlüsselung selbst werden asymmetrische und symmetrische Verfahren eingesetzt. Dabei werden öffentliche Schlüssel des Kommunikationspartners für die Verschlüsselung der Daten genutzt, wobei der eigentliche Sitzungsschlüssel ein nur einmalig nutzbarer symmetrischer Schlüssel ist, mit dessen Hilfe die Daten sowohl entschlüsselt als auch verschlüsselt werden.

HTTPS

Das Hypertext Transfer Protocol Secure Kommunikationsprotokoll nutzt TLS für die Verschlüsselung der Kommunikation des HTTP-Protokolls, das ursprünglich für die Kommunikation im World Wide Web entwickelt wurde, mittlerweile aber auch für die Machine-2-Machine-Kommunikation genutzt wird. Die grundlegenden Dienste bei HTTP sind sehr einfach gehalten, so dass darauf aufbauende Übertragungen, die Schnittstellen entsprechend REpresentational State Transfer (ReST) anbieten, einfach implementiert und auch weltweit genutzt werden können.





KAPITEL 4: HANDLUNGSEMPFEHLUNGEN

In diesem Kapitel beschäftigen wir uns mit der Vorgehensweise bei der Auswahl und Umsetzung einer Kommunikationslösung. Selbstverständlich müssen wir dabei klar unterscheiden zwischen der Herangehensweise eines Geräteherstellers und eines Anlagenbetreibers beziehungsweise Ingenieurbüros. Während es bei einem Gerätehersteller grundsätzlich darum geht, Automatisierungskomponenten zu entwickeln, liegt der

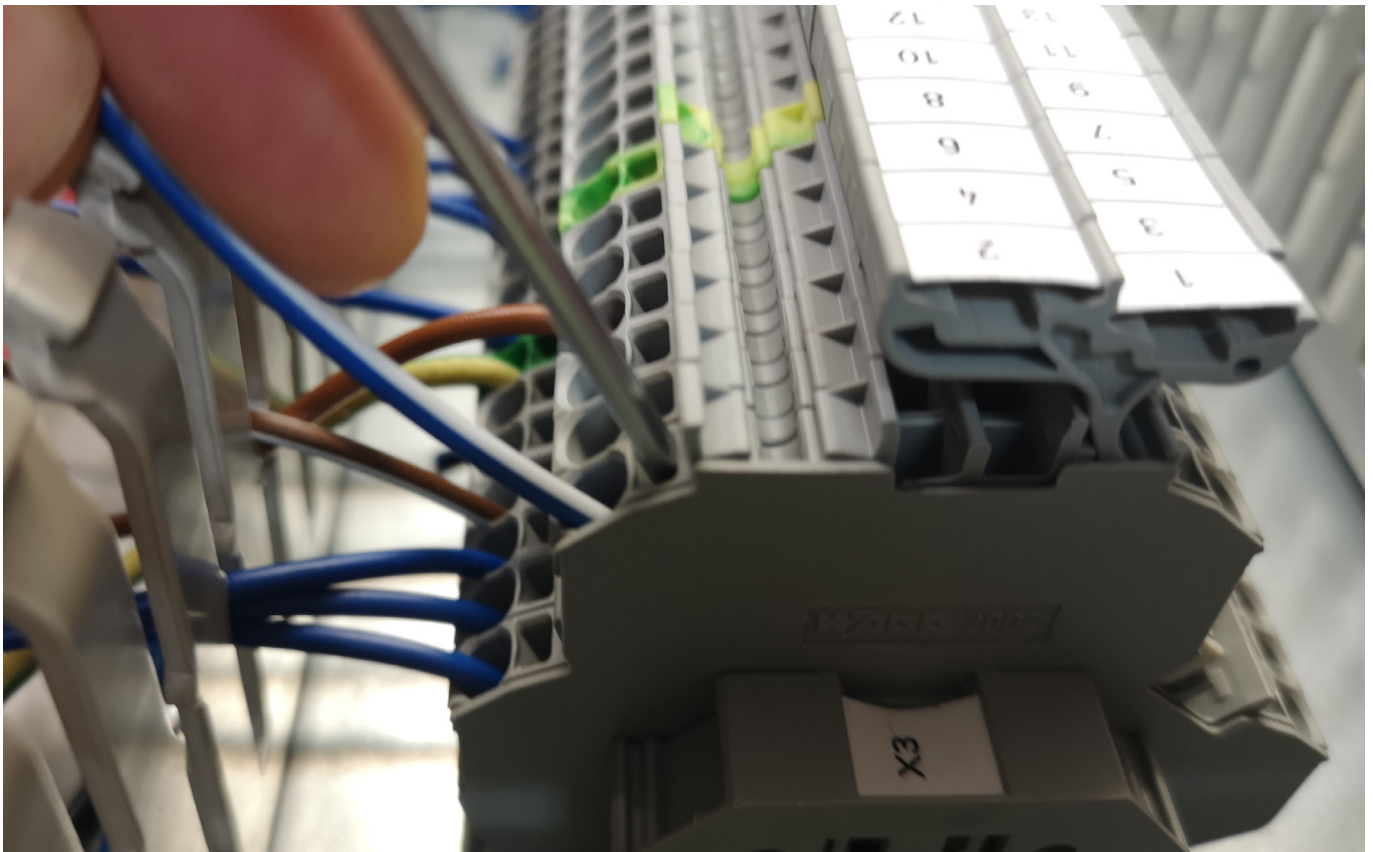
Fokus bei einem Anlagenbetreiber oder Ingenieurbüro auf der Realisierung von Systemen. Für beide Zielgruppen empfehlen wir einen jeweiligen Fragenkatalog, über den sich Hersteller oder Betreiber dem Thema grundsätzlich nähern können. Über die intensive Beschäftigung und Beantwortung der Fragen sollte sich eine jeweilige Handlungsempfehlung ergeben.

Checkliste für Gerätehersteller

- 1** Was sind meine Zielmärkte und Zielbranchen?
- 2** Welche Anforderungen werden durch meine Hauptkunden definiert (z.B. Einsatz einer bestimmten Technologie)?
- 3** Welche Protokolle und Integrationstechnologien dominieren meine Zielbranchen? Können Trends zum Einsatz neuer Technologien identifiziert werden?
- 4** Soll mein Gerät mit anderen Geräten interoperabel sein?
- 5** Soll mein Gerät eine geschlossene Lösung sein (Package Unit) und eventuell eine Schnittstelle zur Integration in übergeordnete Steuerungen oder Managementanwendungen besitzen?
- 6** Mit welchen Komponenten soll mein Gerät kommunizieren können?
 - Mit der steuernden SPS?
 - Mit Parametriergeräten im Netz?
 - Mit SCADA und höheren Managementsystemen (MES, ERP)?
 - Mit anderen Automatisierungsgeräten?
 - Ist ein Fernzugriff auf das Gerät vorgesehen?
 - Spezielles Protokoll
 - Über eine Cloud
- 7** Welche detaillierten Anforderungen gibt es?
 - Einsatz im explosionsgeschützten Bereich?
 - Speisung der Geräte über den Bus?
 - Ist der Einsatz in Safety-Anwendungen vorgesehen?
- 8** Entscheidung für einen oder mehrere Technologiekandidaten
 - Zukauf einer HW/SW-Lösung für die Kommunikationsanschaltung?
→ Integrierbarkeit in das Gerät muss gegeben sein.
 - Portierung eines Kommunikationsstacks auf die Gerätehardware?
 - Stehen auf der aktuellen Hardware ausreichend Ressourcen zur Verfügung?
 - Ist eine Erneuerung der Hardware notwendig?
 - Stehen eigene Entwicklungskapazitäten zur Verfügung?
 - Einbeziehen eines externen Entwicklungsdienstleisters?
- 9** Welche Zertifizierungen sind notwendig/möglich?
(Voraussetzung für Zulassung, Marketingargument zur Erhöhung der Marktchancen, Kundenwunsch)
- 10** Welche Schulungen sind für das Personal notwendig?
 - Einbeziehen eines externen Entwicklungsdienstleisters?

Checkliste für Anlagenbetreiber, Ingenieurbüros

- 1** Was sind die detaillierten Anforderungen der neuen Anlage?
 - Echtzeitanforderungen (Zykluszeiten, Antwortzeiten, Synchronität)
 - Zu übertragende Daten (Prozesswerte, Parameter, Streaming, ...)
 - Anzahl der Teilnehmer
 - Ausdehnung der Anlage (Einfluss auf Übertragungslängen)
 - Bestehen EX-Anforderungen?
 - Bestehen Safety-Anforderungen?
 - Soll ein Remote-Zugriff auf die Anlage möglich sein? (Cloud oder direkter Protokollzugriff?)
 - Ist die Integration der Kommunikation und der Daten mit anderen Anlagen erforderlich?
→ Gateways, Datenbanken, Integrationstechnologien
 - Sicherheitsanforderungen
- 2** Welche Kommunikationsprotokolle/Integrationstechnologien werden in der Anlage/im Unternehmen bereits eingesetzt? Sind diese Technologien für die neuen Aufgaben geeignet? Sind geeignete Komponenten am Markt verfügbar?
- 3** Welche Technologie(n) erfüllen die Anforderungen?
- 4** Welche Gerätevielfalt ist am Markt verfügbar?
- 5** Ist das aktuelle Personal in der Lage, die Technologie zu handhaben? Ist eine Schulung mit vertretbarem Aufwand möglich/notwendig?
- 6** Gibt es externe Dienstleister zur Unterstützung der Anlagenerrichtung beziehungsweise die Betriebsbetreuung?
- 7** Werden Einflüsse auf die Betriebs- und Wartungsabläufe erwartet?





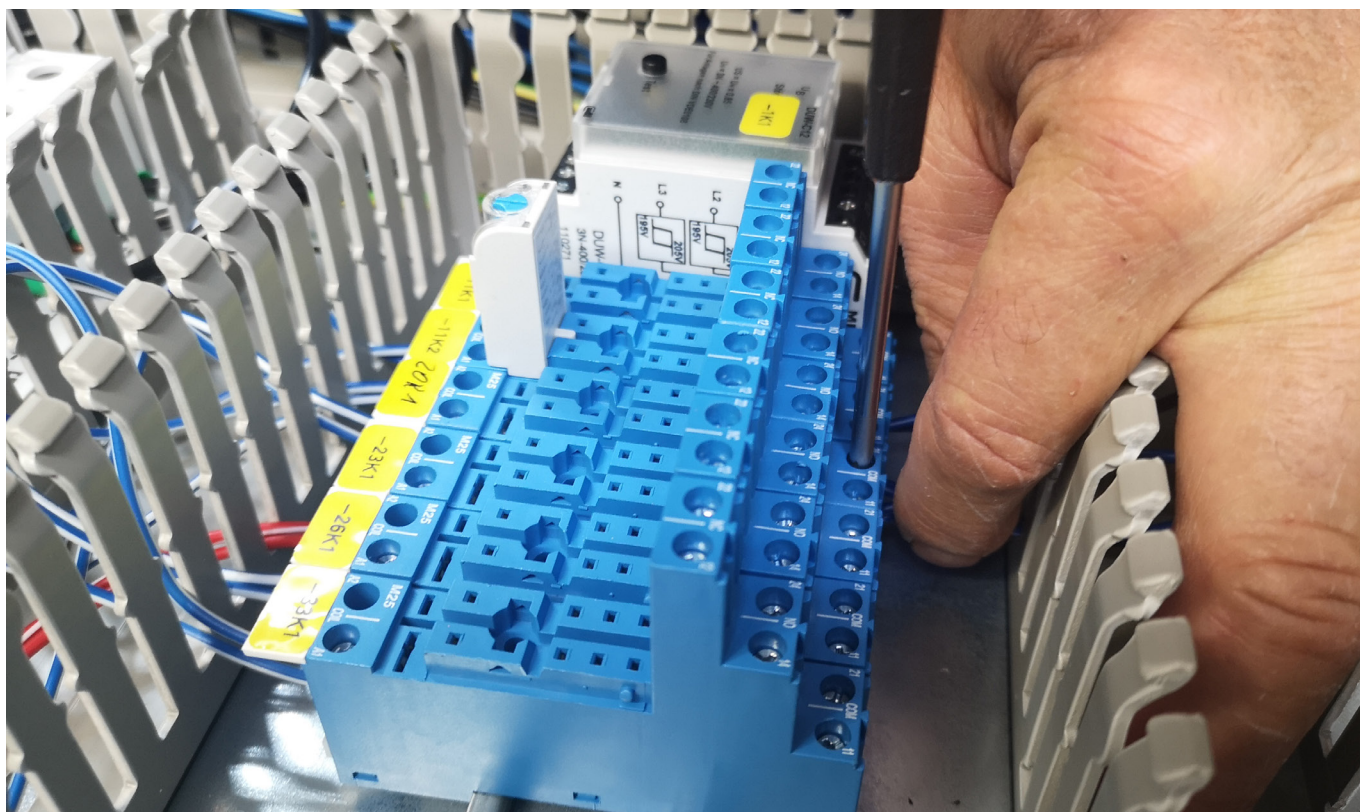
KAPITEL 5: PRAXISBEISPIEL

Die Nowus Automatisierungstechnik GmbH ist ein in Magdeburg ansässiges, 1992 gegründetes und überregional tätiges Unternehmen. Die anfängliche Mitarbeiteranzahl von 3 wuchs bis heute auf 11 an. In den ersten Jahren nach der Gründung wurden nur einfache Lüftungsanlagen und Heizungsverteiler automatisiert. Aktuell teilen sich die bis zu 100 Projekte im Jahr gleichermaßen auf Gebäudeautomation und industrielle Lösungen auf. Zusätzlich wird die Programmierung von Steuerungen und Controllern verschiedener Hersteller (Siemens, Beckhoff, WAGO, DEOS, Saia) unterstützt. Die Mitarbeiter des Unternehmens fertigen individuelle Schaltanlagen für die MSR Technik in den Bereichen Heizung, Lüftung, Klima – also für die technische Gebäudeausrüstung (TGA). Darüber hinaus stellt NOWUS Schaltanlagen für den Sondermaschinenbau (zum Beispiel Seilranganlagen) sowie die Prozessindustrie her.

Zur Realisierung der Mess-, Steuerungs- und Regelungstechnik (MSR) für TGA-Anlagen ist heutzutage ein enormer Planungs- und Verkabelungsaufwand vonnöten, da nicht nur ein Heizkreisverteiler oder eine Lüftungsanlage automatisiert werden soll, sondern auch Meldungen von anderen Gewerken eingesammelt werden müssen (beispielsweise eine Störmeldung von einer Wasseraufbereitungsanlage). Sollen im Lebenszyklus der Anlage Anpassungen vorgenommen oder Erweiterungen umgesetzt werden, ist das mit einem hohen Installationsaufwand verbunden, wenn zum Beispiel neue Kabel durch eine Brandschutzwand gezogen werden müssen.

Die Vielfalt der Lösungen sowie der stetige technische Fortschritt stellen die Mitarbeiter permanent vor neue Herausforderungen. Einerseits fordern Kunden die Wartung Jahrzehnte alter, installierter Technik. Andererseits werden in Ersatz- oder Neuinstallationen Lösungen erwartet, die einen Komfort bieten, wie wir ihn heute aus der Unterhaltungs- oder Telekommunikations-Sparte „gewöhnnt“ sind und nicht mehr missen wollen. Mit verschiedenen Komfortfunktionen versuchen sich die Wettbewerber am Markt voneinander abzugrenzen.

Für einen kleinen Dienstleister wie NOWUS stellt sich die Frage, mit welchen Technologien diese Komfortfunktionen einerseits handhabbar und im TGA-Umfeld einsetzbar sind. Gleichzeitig sollen sie aber auch die Voraussetzungen für die Entwicklung effizienter Dienstleistungen bieten, damit man sich künftig am Markt besser positionieren kann. Im Zeitalter von Industrie 4.0 müssen Anlagen und Geräte internetfähig sein und die Integration in weit verteilte Prozesssteuerungs- und Automationssysteme oder, wie hier im Fall von TGA-Anlagen, in ein verteiltes Facility Management ermöglichen. Dafür ist es jedoch notwendig, die Anlagen und Geräte um eine internetfähige Kommunikationseinheit zu erweitern. Damit stehen Diagnosedaten und Messwerte, welche an den Anlagen und Geräten ermittelt werden, jederzeit für entfernte Anwendungen zur Verfügung.



„In der Zukunft werden durch 5G leitungsgebundene Feldbusse teilweise ersetzt und die Verbindung zur IT und Cloud einfacher, direkter und schneller möglich sein. Auch die Verknüpfung unterschiedlicher beziehungsweise räumlich getrennter Anlagen und die damit verbundenen Vorteile werden problemlos umsetzbar sein und ganz neue Möglichkeiten bieten.“



André Schimschar, Geschäftsführer der Nowus Automatisierungstechnik GmbH

Die Geschäftsführung der NOWUS Automatisierungstechnik GmbH hat bereits begonnen, nach technischen Lösungen zu suchen, die:

- künftig eine durchgängige Vernetzung vom Sensor, über die Steuerung, zur Bedienung und im Bedarfsfall bis hin zum Dienstleister mit möglichst wenigen Netzübergängen ermöglichen
- also auch die weit gefächerten Anforderungen bezüglich der zu übertragenden Datenmengen und Zykluszeiten abdecken
- skalierbar bezüglich der anzuschließenden Teilnehmer sind
- den sicheren Zugriff auf Informationen von jedem beliebigen Ort aus ermöglichen
- die Integration von Bestandssystemen erlauben
- Nachhaltig effizient und zukunftssicher erscheint
- zur Reduzierung des manuellen Installationsaufwandes (Ersatz der manuellen Verkabelung durch drahtlose Kommunikation) führen

5G ist der neue Mobilfunkstandard für den Einsatz in den unterschiedlichsten Anwendungsfeldern von Mediastreaming, über Vernetzung von Sensoren bis hin zur Echtzeitsteuerung von Maschinen. ▼



(c) Sikov/stock.adobe.com

Das primäre Ziel lag nunmehr auf der Analyse der aktuellen Trends der drahtlosen Kommunikation insbesondere zum aktuellen Trendthema 5G, den Randbedingungen für die Einführung dieser neuen Technologie im TGA-Umfeld sowie der Konzeption für die praktische Nutzung.

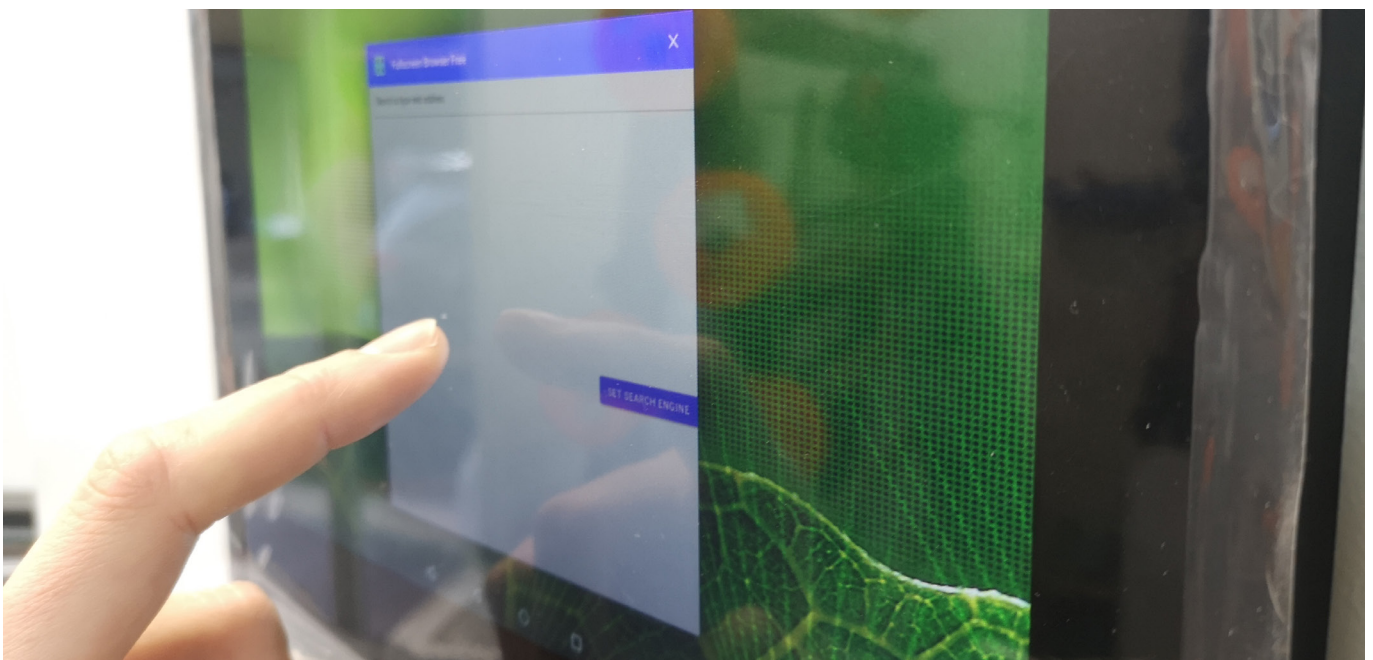
Unterstützung hat NOWUS beim Mittelstand 4.0 Kompetenzzentrum Magdeburg „vernetzt wachsen“ gefunden. Gemeinsam wurden die konkreten Anforderungen identifiziert und verschiedene Lösungsvarianten diskutiert. Sehr schnell wurde klar, dass die Lösung auf einer Standardtechnologie aufbauen soll, die das Potential hat, künftig von einer Vielzahl von Geräte- und Systemanbietern unterstützt zu werden.

Von den betrachteten Technologien verspricht 5G, die Anforderungen zu erfüllen, wenngleich die Technologieentwicklung noch nicht das finale Stadium erreicht hat. Potenziale sind beispielsweise:

- Migration von existierenden Funktechnologien der Telekommunikation oder lokalen Netzwerken ist möglich
- Geringerer Aufwand bei der Installation und Wartung durch den Einsatz einer drahtlosen Kommunikationstechnologie
- Konsequenter Remote-Zugriff ermöglicht neue Service-Konzepte
- Die online-Verfügbarkeit verschiedenster Daten ermöglicht neue Anwendungen
- Schnellere Reaktion auf Service-Anfragen führt zu höherer Kundenzufriedenheit



- ➔ In allen industriellen Wertschöpfungsketten fallen Daten an
- ➔ Digitale Datenübertragung ist Voraussetzung für eine Digitalisierung entlang der Wertschöpfungskette
- ➔ Für die verschiedenen Aufgabenstellungen wurden unterschiedliche industrielle Kommunikationstechnologien entwickelt
- ➔ Die Auswahl einer geeigneten Lösung ist Voraussetzung für nachhaltigen Erfolg



WER HILFT MIR WEITER?

Das Mittelstand 4.0-Kompetenzzentrum Magdeburg gehört zu Mittelstand-Digital. Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital. Der DLR Projektträger begleitet im Auftrag des BMWK die Kompetenzzentren fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weitere Informationen finden Sie unter www.mittelstand-digital.de

Mittelstand 4.0-Kompetenzzentrum Magdeburg „vernetzt wachsen“

c/o Zentrum für Produkt-, Verfahrens- und Prozeßinnovation GmbH
Experimentelle Fabrik I Sandtorstraße 23 I 39106 Magdeburg

 www.vernetzt-wachsen.de  info@vernetzt-wachsen.de  0391 544 86 220

Publikationen der Kompetenzzentren der Mittelstand Digital-Initiative

Mittelstand 4.0 Kompetenzzentrum Magdeburg (2019): Thementelegramm Trends in der digitalen Datenkommunikation im industriellen Umfeld,

<https://www.vernetzt-wachsen.de/wp-content/uploads/2019/01/Trends-in-der-digitalen-Datenkommunikation.pdf>

Mittelstand 4.0 Kompetenzzentrum eStandards: Faktenblatt Smart Building: Vernetzung und Automation in Gebäuden,

https://www.estandards-mittelstand.de/fileadmin/user_upload/Materialien/Wissensbox/Faktenblatt-Smart-Building.pdf

Mittelstand 4.0 Kompetenzzentrum Kaiserslautern: Die Fabrik der Zukunft – Vernetzte Produktion als Basis für erfolgreiche Digitalisierung im Betrieb (2017),

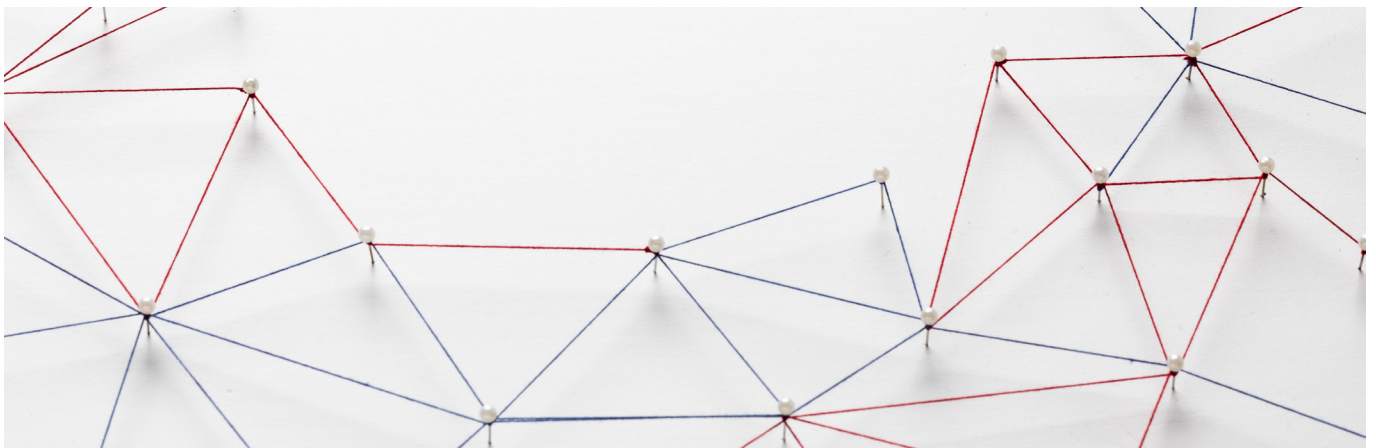
https://kompetenzzentrum-kaiserslautern.digital/wp-content/uploads/2017/11/MKK_Kurzleitfaden_WEB.pdf

Mittelstand-Digital Magazin WISSENSCHAFT TRIFFT PRAXIS – Ausgabe 12: Vernetzte Wertschöpfung – Plattformen, Wertschöpfungsnetzwerke und die Blockchain für Prozess- und Geschäftsmodellinnovationen (2019),

<https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/Wissenschaft-trifft-Praxis/magazin-wissenschaft-trifft-praxis-ausgabe-12.html>

Mittelstand 4.0 Agentur Cloud: Auswahl und Einführung von Cloud-Lösungen – Ein pragmatischer Wegweiser in die Cloud für kleine und mittlere Unternehmen und Coaches in Mittelstandsverbänden,

<https://digitales-kompetenzzentrum-stuttgart.de/wp-content/uploads/2019/02/agentur-cloud-kurzleitfaden-auswahl-und-einfuehrung-von-clou.pdf>

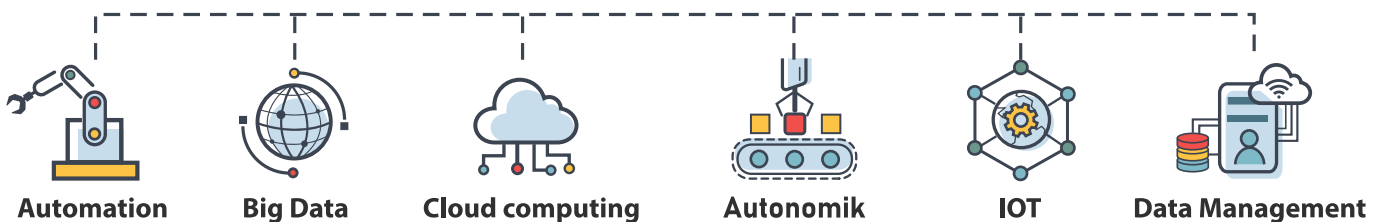


Glossar

AES	Advanced Encryption Standard
CAN	Controller Area Network
CSV	Comma-separated Values
DP	Dezentral Peripherie
DTM	Device Type Manager
EDDL	Electronic Device Description Language
ERP	Enterprise-Resource-Planning
FDI	Field Device Integration
FF	Foundation Fieldbus
HART	Highway Addressable Remote Transducer
HMI	Human Machine Interface
HTTP(S)	Hypertext Transfer Protocol (Secure)
IEC	International Electrotechnical Commission
IP	Internet Protocol
IRT	Isochronous Real Time
ISM	Industrial, Scientific and Medical Band
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
LWL	Lichtwellenleiter
MBP	Manchester Coded, Bus Powered
MQTT	Message Queuing Telemetry Transport
OPC	Open Platform Communications
PA	Process Automation
PROFIBUS	Process Field Bus
RFC	Requests for Comments
RT	Real-time
SPS	Speicherprogrammierbare Steuerung
SSL	Secure Sockets Layer
STRIDE	Spoofing of user identity, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UA	Unified Architecture
UDP	User Datagram Protocol
XML	Extensible Markup Language



INDUSTRIE 4.0







Aktuelle Informationen finden Sie auf www.vernetzt-wachsen.de



Mittelstand 4.0-Kompetenzzentrum Magdeburg „vernetzt wachsen“

c/o Zentrum für Produkt-, Verfahrens- und Prozessinnovation GmbH
Sandtorstraße 23 | 39106 Magdeburg



0391 544 86 220



info@vernetzt-wachsen.de

