PLATTFORM INDUSTRIE 4.0

DISKUSSIONSPAPIER

Sichere Kommunikation für Industrie 4.0

Impressum

Herausgeber
Bundesministerium für Wirtschaft
und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Gestaltung und Produktion
PRpetuum GmbH, München

Stand
Juni 2017

Bildnachweis
Mimi Potter – Fotolia (Titel)

Das Bundesministerium für Wirtschaft und Energie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

Abbildungsverzeichnis

Einleitung

Industrie 4.0 schafft mit innovativen Konzepten und Vorgehensweisen völlig neue Möglichkeiten in der Zusammenarbeit – insbesondere auch auf technischer Ebene. Anlagen, Maschinen und Produkte interagieren, tauschen Daten aus und korrespondieren stets. Dabei spielt es keine Rolle, ob mit einer Maschine in derselben Fabrikhalle oder mit einer Anlage in einem Betrieb auf der anderen Seite der Welt kommuniziert wird. Doch das funktioniert nur, wenn technische Kommunikationsmechanismen dafür sorgen, dass Industrie 4.0-Komponenten (Assets) sicher und interoperabel in Kontakt treten können.

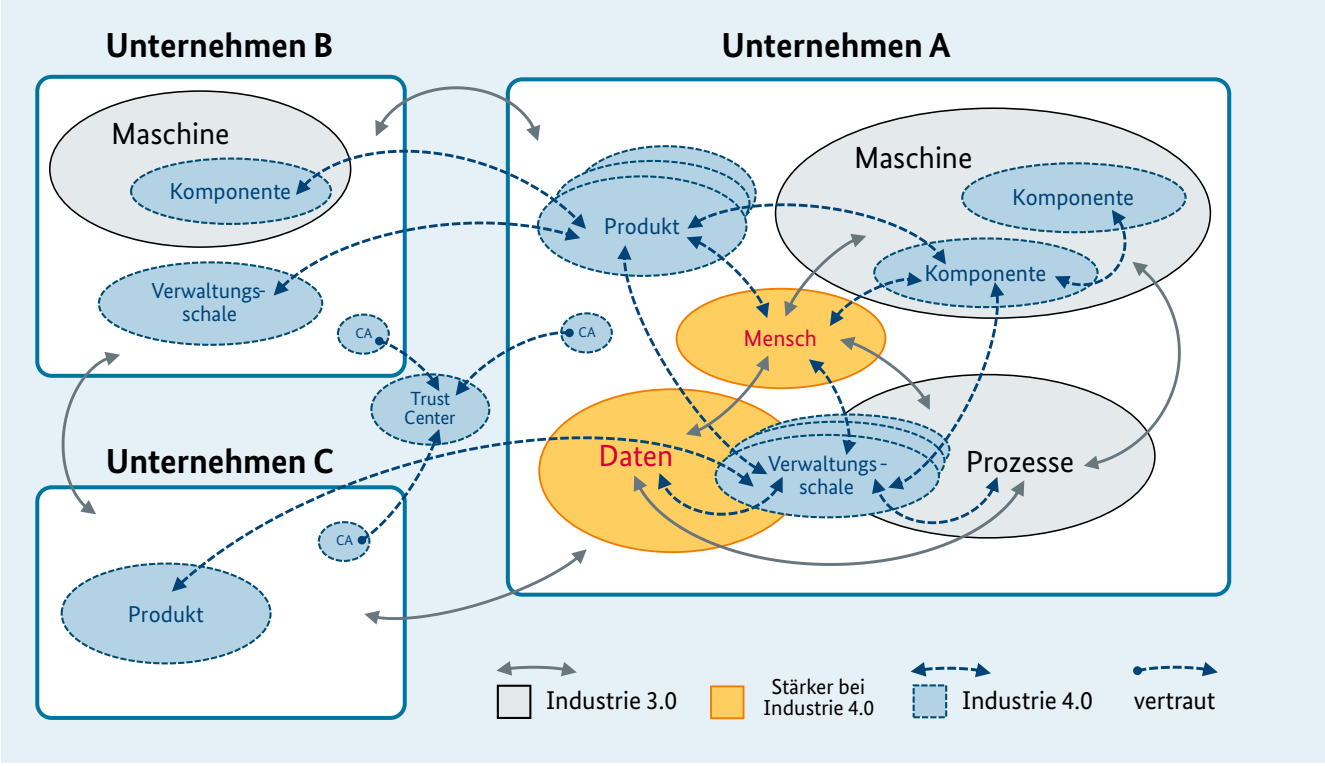
Eine solche Industrie 4.0-konforme Kommunikation zu erörtern – das ist Ziel des vorliegenden Diskussionspapiers. Dabei liegt der Fokus klar auf den technischen Aspekten der sicheren Kommunikation. Anforderungen an die Organisation werden weitestgehend nicht betrachtet. Das Dokument richtet sich an Entscheider und Anwender im Industrie 4.0-Kontext. Neben Rahmenbedingungen und Leitprinzipien werden ihnen exemplarisch gewonnene Erkenntnisse zur Industrie 4.0-Kommunikation dargestellt, die die Ansprüche an eine sichere IT-Infrastruktur berücksichtigen.

Was ist neu bei Industrie 4.0?

Während Automatisierungskomponenten wie zum Beispiel Sensoren in Industrie 3.0 meistens im unternehmenseigenen Umfeld, also innerhalb der internen Sicherheitsdomäne, kommunizieren, interagieren sie bei Industrie 4.0 über Unternehmensgrenzen hinweg (1) (Abbildung 1). Dabei müssen Kommunikationsbeziehungen erlauben, zwischen allen Beteiligten Informationen auszutauschen oder Services bereitzustellen. Services sind beispielsweise Aktionen wie: „Bitte messe die Temperatur“ oder „Fahre den Schlitten zehn Zentimeter vor“. Eine Ende-zu-Ende-Netzwerkverbindung ist dabei jedoch nicht zwingend Voraussetzung.

Funktionalität und Sicherheit – das sind die ausschlaggebenden Aspekte, die die Kommunikation berücksichtigen muss. Im vorliegenden Dokument wird genau das diskutiert: Wie muss die Art der Kommunikation ausgeprägt sein, um zu funktionieren und sicher zu sein? Berücksichtigt werden der Office-Bereich (Information Technology (IT)) und die Produktionsebene (Operations Technology (OT)). Die IT-Security des Office-Bereichs sichert die unternehmensbezogenen Aufgaben und orientiert sich bei der

Abbildung 1: Kommunikationsbeziehungen bei Industrie 4.0



Kommunikation bisher vor allem auf den Schutz der Daten. Die Produktionsebene hingegen deckt die Automatisierungsaufgaben ab, bei denen vor allem die Kommunikation im Vordergrund steht, die echtzeitfähig und verfügbar sein muss. Denn: Ohne Kommunikation keine Produktion. Bei Industrie 4.0 interagieren diese Bereiche immer stärker und wachsen zunehmend zusammen. Neben den bestehenden Anforderungen an die Sicherheit in beiden Bereichen entstehen durch Industrie 4.0 weitere spezifische Bedarfe. Der Grund: Die Kommunikation läuft verstärkt automatisiert und unternehmensübergreifend ab (Abbildung 2).

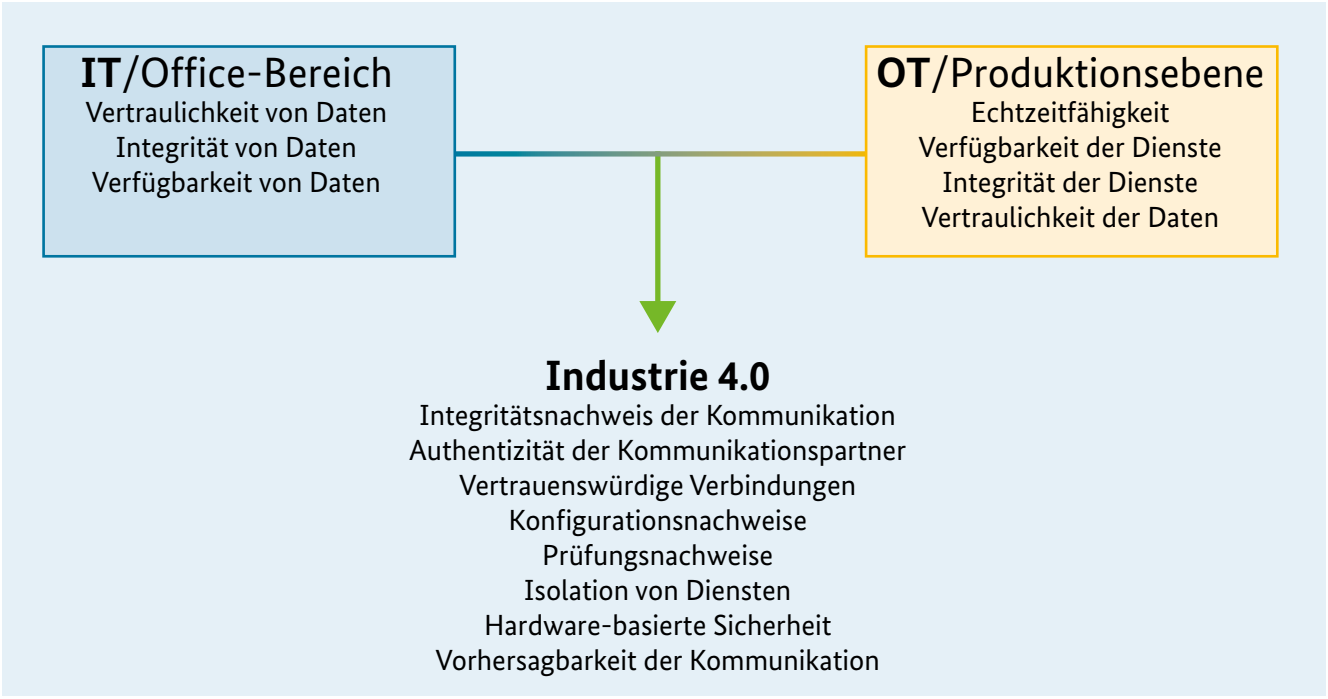
Herausforderungen

So wird die Art der Kommunikation zwischen verschiedenen Unternehmen, Staaten und Kontinenten zum kritischen Erfolgsfaktor: Sichere, vertrauenswürdige technische Prozesse bzw. Protokollstrukturen bei künftigen, durch die Vernetzung ermöglichten „Connected Services“ (zum Beispiel vorausschauende Wartung) nehmen eine Schlüsselrolle ein. Dabei sind neue nationale Einflüsse einzelner Handelspartner auf technische Sicherheits- und Vertrauensregeln von Bedeutung: Es gibt Länder, die beispielsweise Verschlüsselung verbieten. Werden globale Ende-zu-Ende-Security-Lösungen implementiert, müssen Vertrauensbeziehungen neu definiert werden und für die Beteiligten transparent erkennbar und behandelbar sein. Vorhandene Kommunikationstechnologien werden zu einem globalen industriellen Vertrauensmodell weiterentwickelt. Dabei gilt es, alle Seiten zu berücksichtigen: die Sicherheitsbedürfnisse der industriellen Partner und die Ansprüche auf nationaler Ebene.

Die Herausforderung für eine sichere Industrie 4.0-Kommunikation: Es müssen Lösungen gefunden werden, die einerseits auf vertrauenswürdigen Standards aufbauen, die langfristig mit der gesetzlich geregelten Norm übereinstimmen. Andererseits müssen die Lösungen ausreichend flexibel sein, um die Industrie mit ihren neuen Geschäftsmodellen zu unterstützen. Daher ist es wichtig, regelmäßig neue Angriffsmöglichkeiten im Blick zu haben und zu behandeln.

Ergänzend bauen Maschine-zu-Maschine-Kommunikationen (M2M) künftig auf global anerkannten und durchgängigen Sicherheitskonzepten auf. Dazu erhalten Komponenten, die als vertrauenswürdig eingestuft werden, definierte

Abbildung 2: Office-Bereich und Produktionsebene wirken verstärkt zusammen



Kennzeichen, so dass andere Anlagen oder Maschinen in Produktions- und Wertschöpfungsketten sie als geeignet und sicher identifizieren können. Anhand dieser Kennzeichen wird nachgewiesen, ob sie sich anforderungskonform verhalten und somit eine Kommunikation stattfinden kann und soll. In sicheren und hochverfügbaren Kommunikationsinfrastrukturen sind sie daher wesentliche Grundlage künftiger Business Continuity für Unternehmen. Denn sie stellen den Fortbestand der Unternehmen im Sinne ökonomischer Nachhaltigkeit sicher. Folglich sind nationale Alleingänge riskant: Isolation und keine Möglichkeit, an globalen hochautomatisierten Wertschöpfungsketten und Mehrwertdiensten teilzuhaben, können die Folge sein.

Wie begegnen wir dieser Herausforderung?

Idealerweise sind Plattform-Services direkter Bestandteil sicherer Kommunikation und können künftig selbst Produktionsdaten wirksam vor unerwünschter Einsichtnahme oder Veränderung schützen bzw. Knowhow- und IP-Schutz auf der Basis vertrauenswürdiger Digital-Rights-Management-Technologien (DRM) durchsetzen. Vertrauensanforderungen in elektronische Verträge zwischen Maschinen einzubetten – dies wird künftig in der M2M-Kommunikation eine entscheidende Rolle spielen [1].

Darüber hinaus wird es immer wichtiger, während und auch nach einer Kommunikation technisch zu erkennen, ob sich die beteiligten Entitäten vertrauenswürdig verhalten – und nicht nur vor beziehungsweise während des Kommunikationsaufbaus. Vor allem zum Schutz der Kommunikationspartner rückt die durchgängige, automatisierte Überwachung der Semantik stärker in den Fokus. Sie beschreibt, was mit der jeweiligen Kommunikation bezweckt werden soll. Globale Trust- und Plattform-Services müssen dafür sorgen, dass Hersteller, Systeme und Komponenten technisch bewertet werden (Scoring), um vor, während, aber auch nach einer erfolgten Kommunikation automatisiert Gefahrenquellen, wie eingeschleuste Viren, zu erkennen.

1 OpenFog Consortium (https://www.openfogconsortium.org/) – [Draft work on machine contracting]

Kommunikationsbeziehungen

Im Leitfaden für Geräteprofile in der Automatisierungstechnik IEC TR 62390 (3) werden Profile für eine Geräteklasse (zum Beispiel Temperatursensor) mit einer gemeinsamen Menge von Funktionalitäten in einem vorgegebenen industriellen Gebiet definiert. In Anlehnung daran hat die Unterarbeitsgruppe „UAG Sichere Kommunikation für Industrie 4.0“ das Verständnis für eine Sicherheitsrichtlinie (Security Policy) für Industrie 4.0 entwickelt (Abbildung 3).

Die Security Policy spricht alle Beziehungsebenen zwischen Industrie 4.0-Komponenten an. Sie soll die Interoperabilität auf allen Ebenen, die der IEC TR 62390 adressiert, sicherstellen. Beispielhafte Ausprägungen für diese Interoperabilität wären:

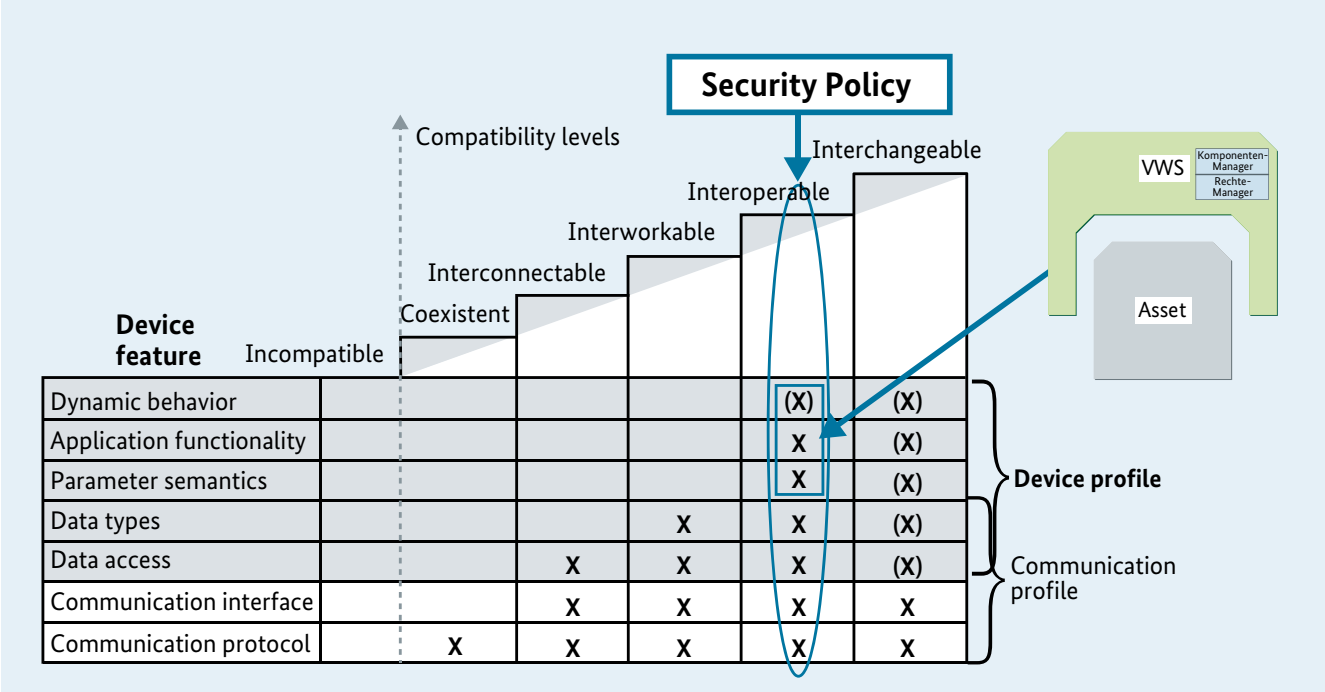
- Dynamic behaviour: Vertrauen in den gleichen neutralen Trustanker, Security-Profile
- Application functionality: Rechte eines Tenants/ Mandanten
- Parameter semantics: Benutzer- und Rollenmodell
- Data types: Zertifikate, Security-Token
- Data access: rollenspezifischer Zugriff (Lesen, Lesen/ Schreiben, Schreiben)
- Communication interface (Ebene 5 – 7): OPC UA
- Communication protocol (Ebenen 1 – 4): TLS

Für Industrie 4.0-Komponenten, die durch ihre Verwaltungsschalen (VWS) abgebildet werden, ist es nicht mehr ausreichend, die Kommunikation auf Protokollebene abzustimmen (Abbildung 3). Auch Vereinbarungen über Rechte (Wer darf was?), Vertrauensanker (zum Beispiel elektronische Schüssel) und Security-Profile sind notwendig.

Um eine Kooperation starten zu können, muss die Verwaltungsschale Informationen über die Security-Fähigkeiten der Industrie 4.0-Komponenten bereitstellen. Nur so kann gegenseitig geprüft werden, ob eine Zusammenarbeit möglich ist (etwa bezüglich des noch zu definierenden Niveaus der Vertrauenswürdigkeit/Trustworthiness, wie im Dokument „Security der Verwaltungsschale“, Plattform Industrie 4.0/ZVEI 2017, diskutiert (4)).

Security-Anforderungen können technisch und soweit erforderlich auch auf organisatorischer Ebene, zum Beispiel durch Richtlinien, umgesetzt werden.

Abbildung 3: Security Policy für Industrie 4.0



Um eine Industrie 4.0-konforme Kommunikation zu beschreiben, muss künftig ein Industrie 4.0-Kommunikationsstack betrachtet werden (Abbildung 11), der sich nicht ausschließlich auf die unteren Schichten des OSI-Schichtenmodells beschränkt. Vielmehr gilt es, verstärkt die gesamte Interaktion und die ausgetauschten Inhalte zu betrachten (Abbildung 4).

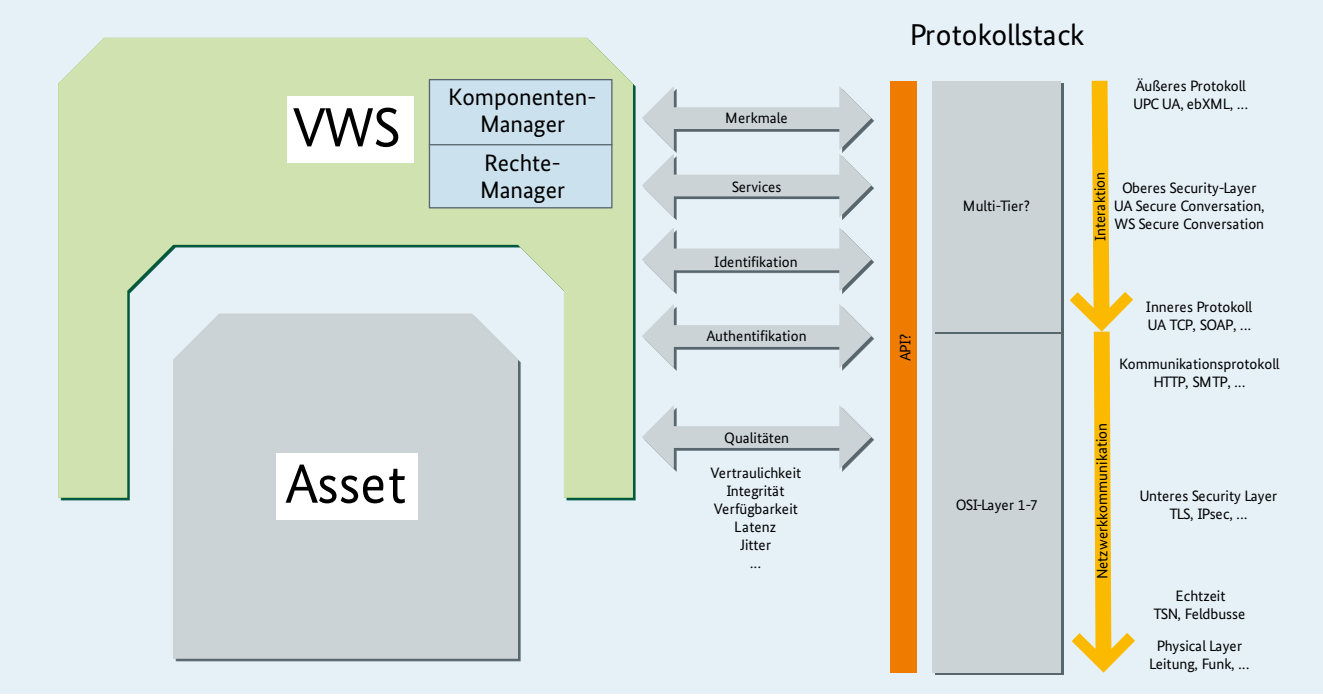
Ein Beispiel: Ein Messwert soll von Maschine A zu Maschine B übertragen werden. Um den Wert auf Netzwerkebene zuverlässig und sicher zu übertragen, stehen verschiedenste Protokolle zur Verfügung. Der Messwert könnte nun zum Beispiel durch eine sichere Übertragung und einen beglaubigten Empfang authentifiziert werden. Die Beglaubigung findet bereits an der Quelle statt, so dass die übertragene Nachricht nicht nur den Messwert selbst, sondern auch die Beglaubigung enthält und somit die Echtheit des Messwerts bestätigt. Dadurch wäre es möglich, Anforderungen an die sichere Übertragung zu reduzieren. Die Auswahl einer geeigneten Kombination von Sicherheit der Information und Sicherheit des Transports hängt vom Anwendungsfall ab. Im genannten Beispiel könnten es Informationen beziehungsweise Bedingungen zum Zeitverhalten oder zur verfügbaren Rechenleistung sein oder die Möglichkeiten der späteren Nachweisführung.

Allgemeine Anforderungen an die Kommunikation und Architektur

Die Kommunikationsbeziehungen zwischen Industrie 4.0-Komponenten müssen eine Interaktion ermöglichen, die es den Komponenten gestattet, Daten auszutauschen und Dienste, die eine Automatisierung erlauben, mit den notwendigen Eigenschaften bereitzustellen. Die vorliegenden Arbeiten hierzu beziehen sich auf das Interaktionsmodell (5), die Netzkommunikation (6) und Servicearchitekturen (7). Ausgangspunkt ist die Abbildung jeder Industrie 4.0-Komponente durch deren Verwaltungsschale (8), die die Industrie 4.0-Komponente beschreibt und Angebote wie Daten, Informationen und Dienste bereitstellt. Um diese Angebote zu verwenden, gibt es bestimmte Anforderungen an die Kommunikation:

- Prinzipiell kann davon ausgegangen werden, dass der wesentliche Teil der Kommunikation über ein **TCP/IP-Netzwerk erfolgen** wird. Auf der Netzwerkschicht wird zukünftig das Protokoll IPv6 eingesetzt (heute überwiegend noch das Protokoll IPv4). Dieses Protokoll ist die **Basis für die Vernetzung von Industrie 4.0-Netzwerken**, denn es ermöglicht, dass beliebige Systeme des Office-Bereichs und der Produktionsebene lokal und global

Abbildung 4: Industrie 4.0-Komponente verwendet Protokollstack



kommunizieren können. Auf dem IP-Protokoll setzen verschiedene Protokolle der TCP/IP-Protokoll-Suite auf. Über TCP oder UDP können Daten zuverlässig oder unzuverlässig übertragen werden. Weitere Protokolle erlauben es darüber hinaus, erste Interaktionsmodelle abzubilden. Architekturen wie OPC UA in der Produktionsebene oder Technologien wie Webservices und SOAP sorgen dafür, dass formatierte Daten weitergegeben und Aktionen angestoßen werden.

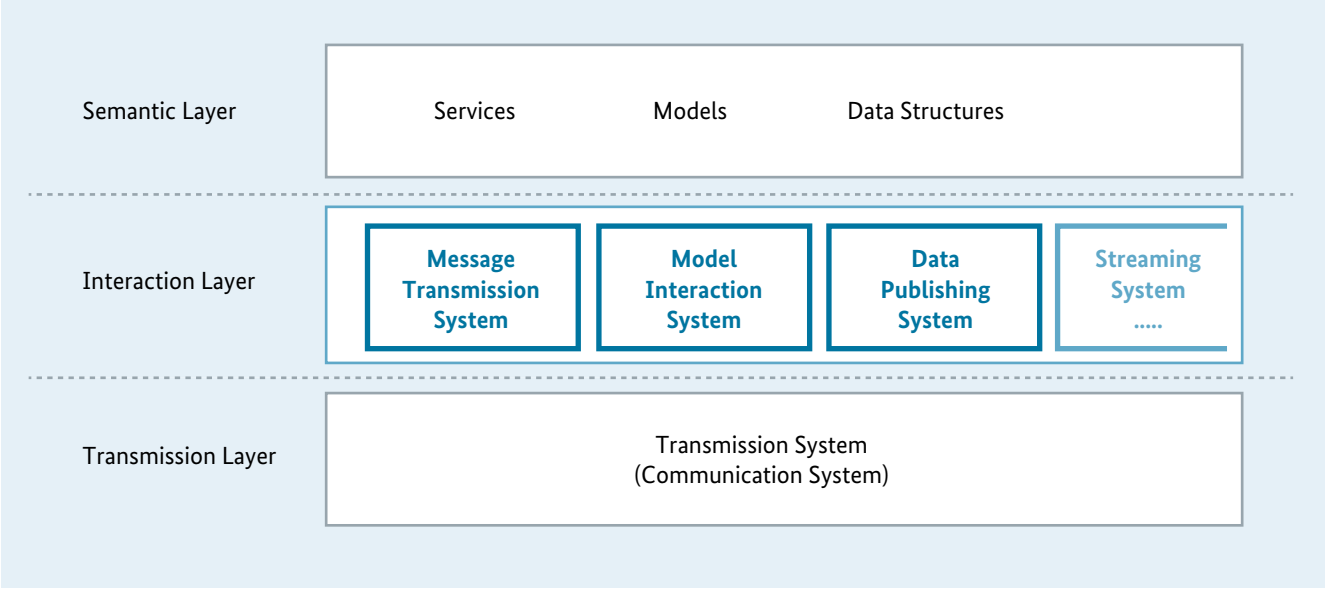
- Da die grundlegende Netzwerkstruktur der TCP/IP-Netzwerke für Industrie 4.0-Kommunikation übernommen wird, sind auch die damit zusammenhängenden Voraussetzungen und Sicherheitsgedanken zu beachten. Im Office-Bereich existieren bereits jahrzehntelang etablierte Modelle, um diese Netze zu verwalten und zu sichern (siehe Abschnitt „Verwendbarkeit verschiedener Protokolle“). Netzplanerische Aspekte wie eine restriktive Netzwerksegmentierung durch Firewalls, Access-Control-Lists, VLANs und Network Access Control sind ebenso zu betrachten wie eine effektive operative Ereignisüberwachung, mit der das Netzwerk systematisch beobachtet wird, um bei Auffälligkeiten zu reagieren. Zusätzlich spielt auch die Sicherheit der unteren Schichten im ISO/OSI-Modell eine Rolle (beispielsweise Verschlüsselung von drahtlosen Netzwerken und Verbindungen über öffentliche Netzwerke wie VPN).

Industrie 4.0-Komponenten tauschen sich aus

Sobald eine Ende-zu-Ende-Verbindung auf Netzwerk- und Transportschicht besteht – indem TCP/IP und etwa OPC UA verwendet wurde –, können die logischen Schnittstellen der Industrie 4.0-Kommunikation – die Verwaltungsschalen – miteinander in Kontakt treten. Auch hier muss ein Augenmerk auf Sicherheit und Effizienz gelegt werden. Wer auf die Angebote (Daten, Informationen und Services) der Verwaltungsschale zugreifen darf, wird durch ein Rechtemodell geregelt (4), das im Konzept der Verwaltungsschale enthalten ist. Dafür muss der Kommunikationspartner identifiziert und authentifiziert werden. Wichtig ist also, dass das zu verwendende Kommunikationsprotokoll und der einzusetzende Kommunikationsstack entsprechende Sicherheitsmechanismen bereitstellen.

Wie genau Kommunikationsbeziehungen aussehen, wird über Anforderungen geregelt, die sich zum Beispiel im Zeitverhalten oder in Security-Anforderungen zu Vertraulichkeit oder Integrität ausdrücken. Diese Anforderungen, wie etwa „Ich brauche eine Antwort unter einer Millisekunde und sie muss digital signiert sein“, müssen sich, falls notwendig, im Kommunikationsstack einstellen und während des gesamten Kommunikationsprozesses prüfen lassen: bei Aufbau, Verwendung (Statusabfrage) und nach Beendigung der Verbindung (Protokollierung). Das Kommunikations-

Abbildung 5: Kommunikationsaspekte nach Com4.0-Basic



stack muss dabei auch die Aushandlung/Bewertung höherwertiger Eigenschaften wie zum Beispiel die eines Sicherheitsprofils des Kommunikationspartners im Sinn einer „Vertrauenswürdigkeit/Trustworthiness“ (1) unterstützen und sie mit dem Rechtemanagement der Verwaltungsschale (VWS) verknüpfen.

Im Dokument zu Kommunikationsmodellen des OpenAAS-Projekts, Com4.0-Basic (9), ist eine solche Struktur definiert (Abbildung 5). Es gilt nun, die darin genannten „Interaction und Transmission“-Layer in der weiteren Diskussion mit der Darstellung in Abbildung 4 zu betrachten und zu einem abgestimmten Gesamtbild weiterzuentwickeln.

Kommunikationsstrukturen

In der Praxis ergeben sich unterschiedlichste Strukturen, die die Kommunikation unterstützen muss – je nach Anforderungen und eingesetzten Anwendungen.

Ende-zu-Ende-Kommunikation

Im einfachsten Fall kommunizieren zwei Industrie 4.0-Komponenten direkt miteinander (Abbildung 6). Dafür muss die notwendige Infrastruktur aus Netzwerk und unterstützenden Diensten bereitgestellt werden – etwa zur Namensauflösung in IP-Adressen oder zum Identitätsmanagement.

Kommunikation über Gateways

In vielen Organisationen wird Kommunikation über Gateways geleitet, die ermöglichen, dass der Datenfluss kontrolliert und Domänen getrennt werden (Abbildung 7).

Komponenten oder Teilsysteme, die selbst nicht Industrie 4.0-konform kommunizieren, können über entsprechende Industrie 4.0-Gateways angebunden werden (Abbildung 8). Diese Art der Anbindung ist notwendig, um bereits existierende Installationen in die zukünftige Industrie 4.0-Welt zu überführen.

Ein weiterer Fall: Es gibt Komponenten, die zu wenig Rechenleistung und Speicher haben, um selbst aufwändig zu kommunizieren. Speziell im lokalen Umfeld kann es hier sinnvoll sein, andere Protokolle zu nutzen. Dabei muss berücksichtigt werden, dass diese Komponenten in den Netzwerken vor einem entsprechenden Industrie 4.0-Gateway selbst keine oder nur eingeschränkte Eigenschaften einer eigenständigen Industrie 4.0-Komponente aufweisen

Abbildung 6: Industrie 4.0-Komponenten kommunizieren Ende-zu-Ende

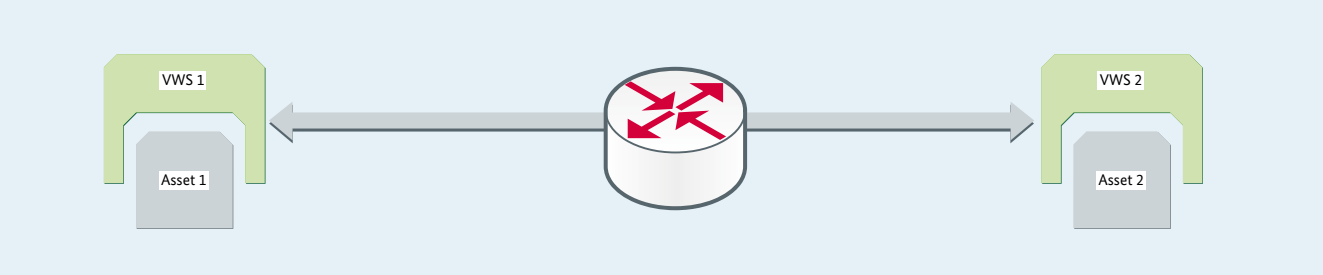


Abbildung 7: Industrie 4.0-Komponenten kommunizieren über Firewalls, Proxys oder Gateways

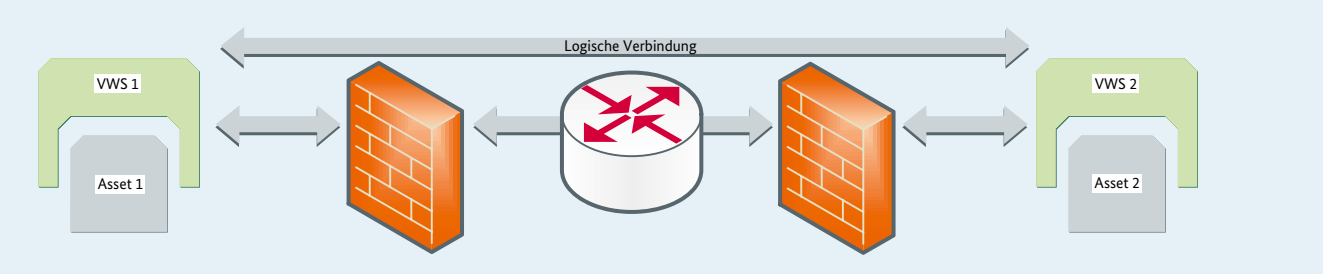
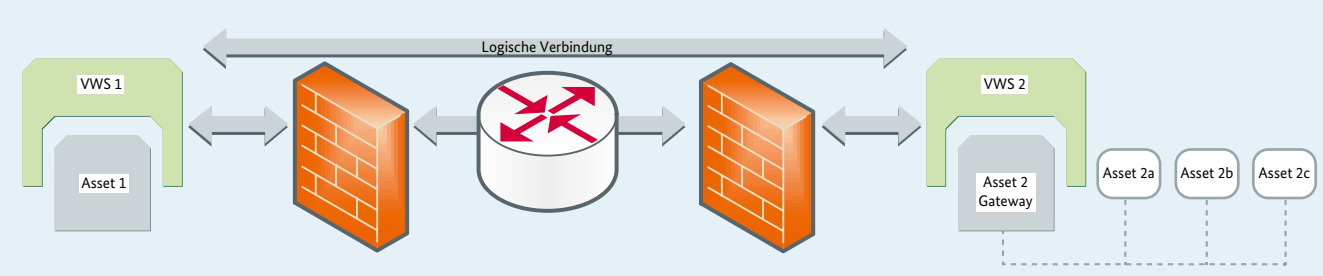


Abbildung 8: Anbindung weiterer Komponenten über Industrie 4.0-Gateways



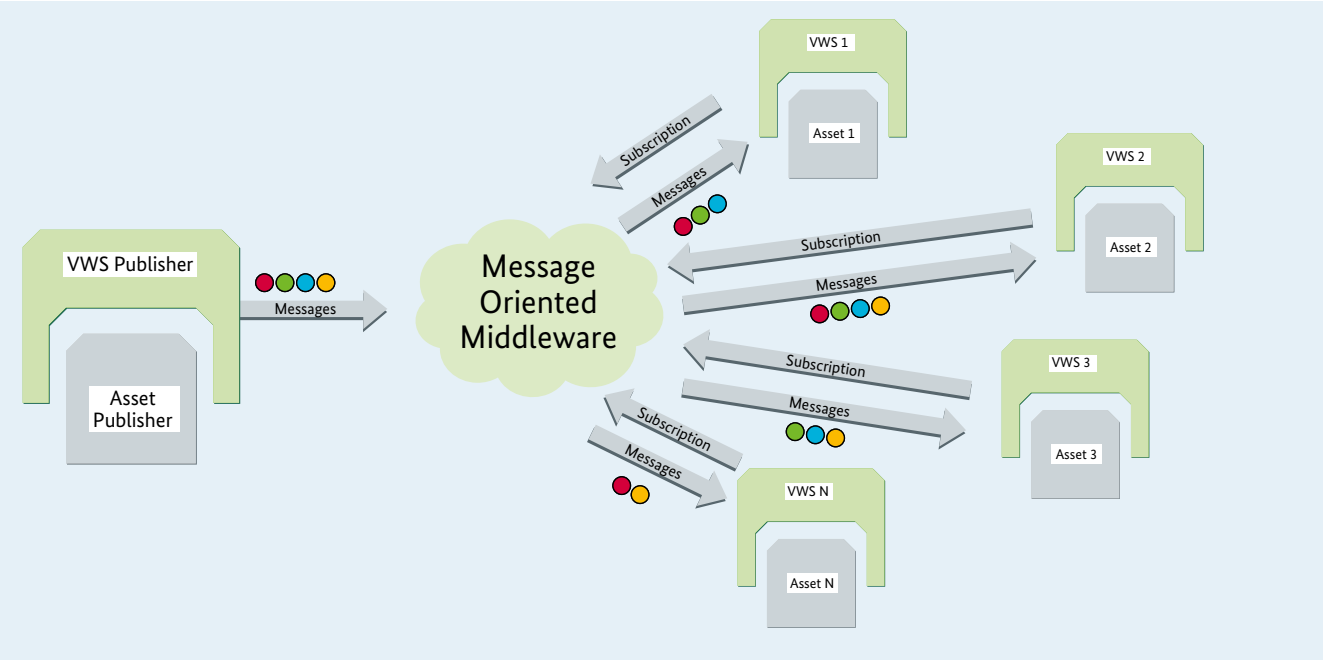
und daher das Industrie 4.0-Gateway entsprechend die Kommunikation unterstützen muss. Industrie 4.0-Gateways bieten sich ferner an, wenn z. B. kleine und mittlere Unternehmen nicht die Ressourcen für Einführung und Betrieb von Industrie 4.0-Komponenten im Hause haben, aber dennoch daran partizipieren möchten. In diesem Fall kann ein Industrie 4.0-Gateway zum sicheren Datenaustausch von einem Dienstleister betrieben werden.

Grundsätzlich müssen Industrie 4.0-Gateways in der Lage sein, alle dahinterliegenden Systeme zu schützen. Das schließt nicht aus, dass ein Industrie 4.0-Gateway selbst hinter einem anderen Gateway im Netzwerk liegen kann.

Publish-Subscribe-Modell

Um Informationen an mehrere Partner zu verteilen, bieten sich Publish-Subscriber-Modelle an. Die Empfänger (Subscriber) melden sich beim Sender (Publisher) oder einem Verteildienst an, um am Informationsfluss teilzunehmen. Die Empfänger wählen die Nachrichtentypen aus, die sie empfangen möchten (Abbildung 9). Durch die lose Kopplung zwischen Sender und Empfänger, bei dem es technisch keine Rolle spielt, wie viele Empfänger sich anmelden, lässt sich die Informationsverteilung gut skalieren. Entsprechende Modelle verwenden häufig Datentelegramme ohne Quittung (UDP) und sind daher entweder so gestaltet, dass verlorene Telegramme toleriert werden, wie

Abbildung 9: Publish-Subscribe-Modell



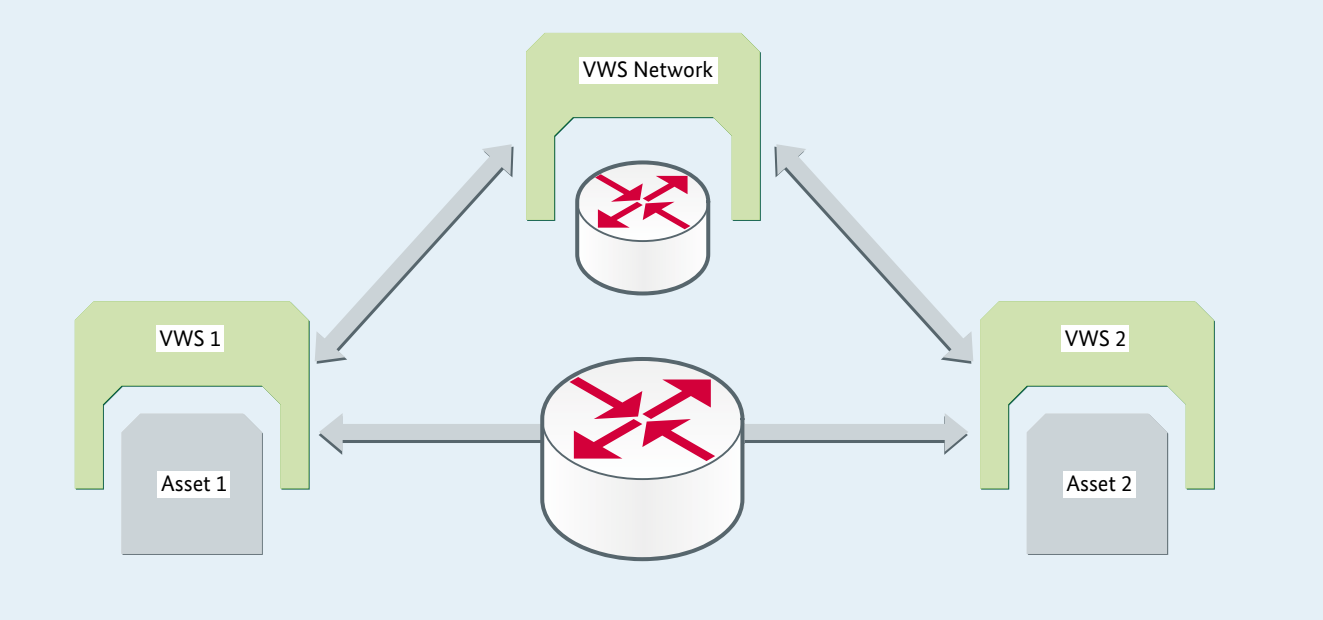
bei Audio- oder Video-Anwendungen, oder dass sie eine sehr zuverlässige Netzwerkinfrastruktur voraussetzen, wie sie in der Automatisierung häufig durch hohe Bandbreitenreserven geschaffen wird. Ergänzend gibt es einen sicheren Modus, in dem der Empfänger alle bisher nicht abgeholten Telegramme konsistent empfangen kann. Diese Kommunikationsmethode ist allerdings zeitaufwändiger und wird üblicherweise in echtzeitunkritischen Anwendungen genutzt, in denen allein die Datenkonsistenz von Bedeutung ist (Business-Prozesse, Verträge, Produktionsaufträge, Alarmmeldungen).

Kommunikation mit dem Netzwerk als Partner

Zeitkritische Automatisierungsanwendungen, die zum Beispiel synchron laufen müssen, um zusammenarbeiten zu können, verlangen häufig besondere Netzwerkeigenschaften wie etwa Latenz (Verzögerung) oder Jitter (deterministisches Zeitverhalten). Sie werden heute im Engineering, also in der Planung und Umsetzung der Automatisierungsanwendung, festgelegt und in alle Komponenten einschließlich der betroffenen Netzwerkkomponenten eingestellt.

Da Industrie 4.0-Konzepte hochflexibel sind, müssen Industrie 4.0-Komponenten die besonderen Eigenschaften beim Netzwerk anfordern können. Daher ist es sinnvoll, dass die Netzwerkinfrastruktur eine eigene Industrie 4.0-konforme Schnittstelle in Form einer Verwaltungsschale bereitstellt (10) (Abbildung 10). So kann die Infrastruktur vollständig in die Industrie 4.0-Welt integriert werden. Je nach Anwendungsfall können auch einzelne Netzwerkelemente, etwa Router oder Switches, durch eigene Verwaltungsschalen repräsentiert sein. Beispiele hierfür sind im Bereich von TSN (Time Sensitive Network), SDN (Software Defined Networks) oder NFV (Network Function Virtualization) zu finden.

Abbildung 10: Industrie 4.0-Komponenten kommunizieren mit dem Netzwerk über erforderliche Eigenschaften



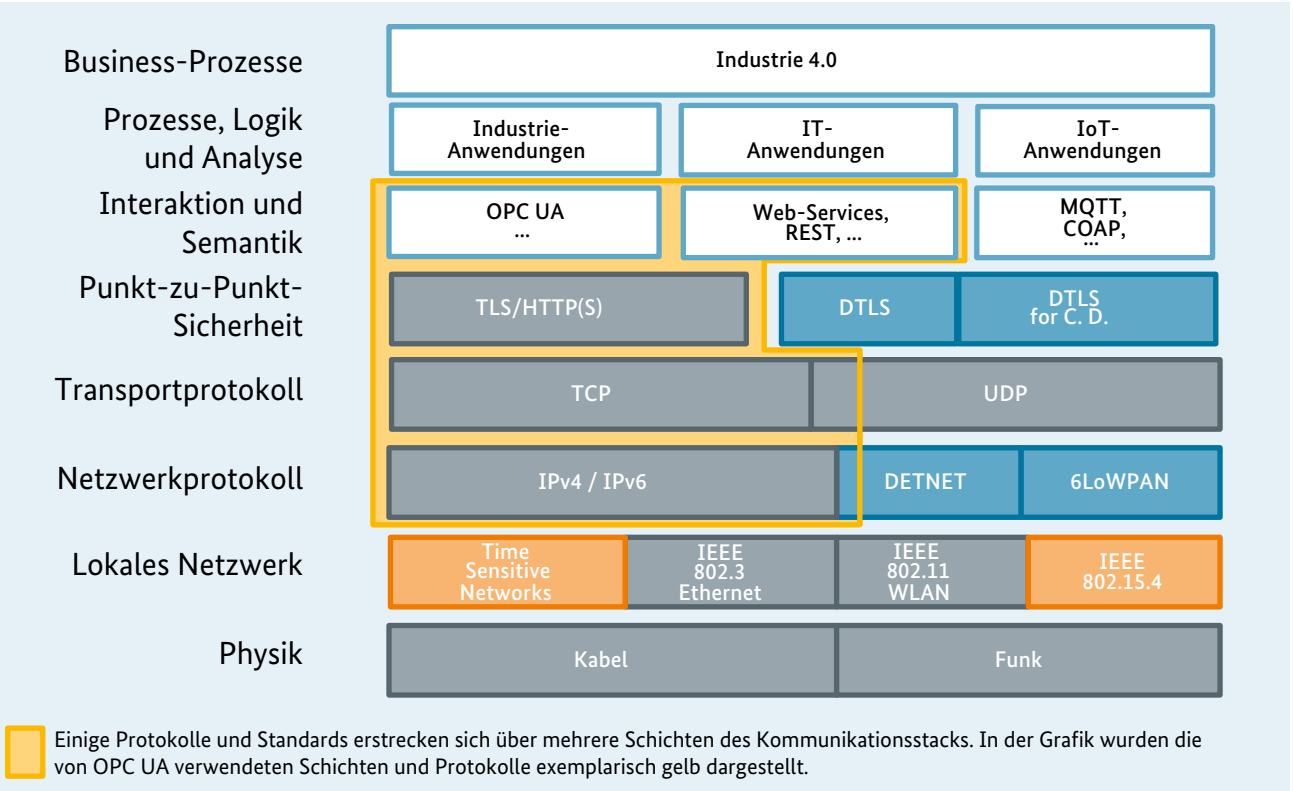
Verwendbarkeit verschiedener Protokolle

Seit Jahrzehnten wird die Netzwerkkommunikation erfolgreich in Protokollschichten und Protokollen gegliedert. Die Protokollschichten beschreiben Dienste, die die Protokolle, die auf diesen Schichten implementiert sind, erbringen müssen. Die Protokolle stellen je nach Zweck oder Umgebung passende Dienste bereit. Dazu gehört zum Beispiel die Namensauflösung. In der Regel sind die Schnittstellen zwischen den einzelnen Protokollschichten generisch, sodass mehrere mögliche Kombinationen aus verschiedenen Protokollen verwendet werden können. So ist es zum Beispiel möglich, eine TCP/IP-Kommunikation sowohl über kabelgebundene Netzwerktypen wie zum Beispiel IEEE 802.3 Ethernet als auch über drahtlose Netzwerke wie etwa IEEE 802.11 WLAN aufzubauen – ohne die darüberliegenden Protokolle und Anwendungslogiken ändern zu müssen. Diese Pluralität der Protokolle wird auch ein Teil von Industrie 4.0 sein, da es erforderlich sein wird, einheitlich zwischen Verwaltungsschalen über verschiedenste Netzwerktypen zu kommunizieren – das machen auch Anwendungsfälle der Industrie deutlich:

- Für eine schnelle Kommunikation in **Closed-Loop-Systemen** beispielsweise kann es bedeutend sein, über echtzeitfähige TSN-Ethernet-Netzwerke zu kommunizieren
- Für den **Datenverkehr mit geringeren Anforderungen an eine deterministische Kommunikation**, bei dem es nicht so wichtig ist, ob ein Datenpaket zu einem vordefinierten Zeitpunkt eintrifft, sind leistungsfähige Ethernet-Netzwerke ohne TSN oder flexible drahtlose Netzwerke mit WLAN sinnvoll.
- In Anwendungen, in denen vor allem **lange Laufzeiten von batteriebetriebenen Geräten** nötig sind (Sensoren oder smarte Geräte-Tags), wird aller Voraussicht auf 802.15.4 Low-Power-Netzwerke in Kombination mit Low-Power-Netzwerkprotokollen wie zum Beispiel 6LoWPAN und COAP gesetzt werden müssen.

Selbst Technologien (etwa deterministische Funkkommunikation), die heute noch nicht verfügbar sind, können durch ein klares Schichtenmodell bereits berücksichtigt und später problemlos eingeführt werden. Auf der Anwendungsschicht werden verschiedene Protokolle und Architekturen parallel existieren, da domänenspezifisch entwe-

Abbildung 11: Pluralität von Netzwerkprotokollen in Industrie 4.0-Anwendungen



Einige Protokolle und Standards erstrecken sich über mehrere Schichten des Kommunikationsstacks. In der Grafik wurden die von OPC UA verwendeten Schichten und Protokolle exemplarisch gelb dargestellt.

der vornehmlich Technologien des Office-Bereichs (zum Beispiel Webservices) oder der Automatisierungstechnik (zum Beispiel OPC UA) eingesetzt werden.

In der Automatisierung und der IT haben sich unterschiedliche Technologien durchgesetzt, die aus technischen und menschlichen Gründen nicht einfach zu ändern sind. Daher ist auch hier anzunehmen, dass es unterschiedliche Protokolle und Architekturen parallel geben wird (Pluralismus).

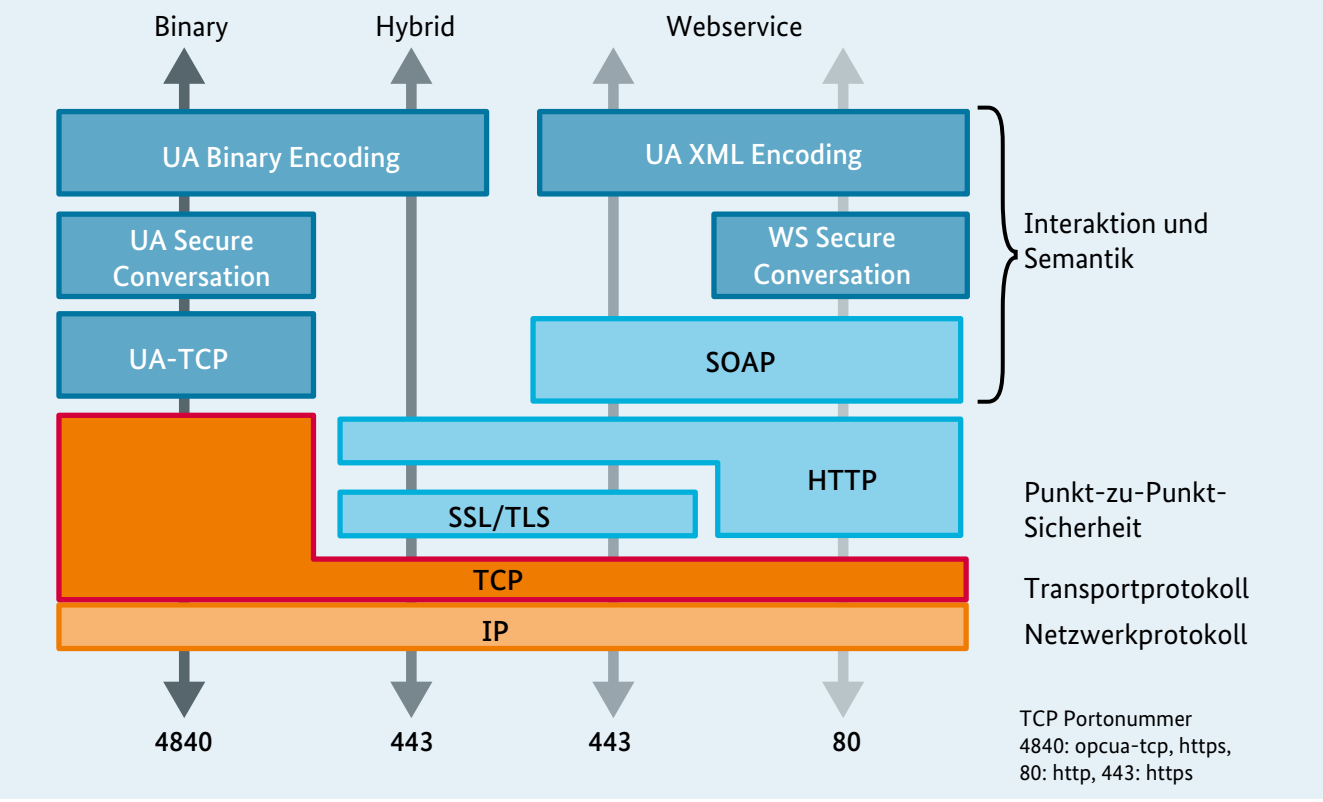
Es scheint, dass die obige Beschreibung eines Protokollpluralismus chaotisch und unnötig komplex ist. Doch: Aufgrund klarer Übergabepunkte an den Protokollschichten lassen sich die Protokolle gut miteinander kombinieren und betreiben. In der Praxis gibt es daneben aber auch bereits Kommunikationsmöglichkeiten zwischen den Domänen: So sieht OPC UA bereits Interaktionen zum Office-Bereich vor und setzt diese um – wie etwa die Verwendung von Webservices und den Einsatz des Sicherheitsprotokolls TLS.

Wie Kommunikationsstacks ausgeprägt sein können, zeigt Abbildung 11. (Weitere Protokolle innerhalb dieser Kommunikationsstacks sind denkbar und nicht unwahrscheinlich.)

Aus Sicht der Protokollpluralität ist es wichtig, die Sicherheitsmechanismen, die auf den einzelnen Schichten verfügbar sind, effektiv einzusetzen. Generell erlauben es viele dieser Protokolle, Authentifizierung, Verschlüsselung und Integritätsschutz einzusetzen. Zusätzlich dazu können auf den Schichten verschiedene Mechanismen eingerichtet werden, die den Zugriff kontrollieren.

Abbildung 12 zeigt den geschichteten Aufbau von OPC UA. Auch hier wird deutlich: OPC UA bedient sich der Funktionen verschiedener Schichten. Selbst innerhalb dieses Standards gibt es gleichberechtigte austauschbare Protokolle (zum Beispiel SOAP und UA TCP). In den unteren Schichten bedient sich OPC UA ebenfalls der Funktionen von TCP/IP-Netzwerken. Da OPC UA unabhängig von spezifischen Netzwerktypen (Ethernet oder WLAN) spezifiziert ist, lässt sich OPC UA in vielen Umgebungen einsetzen. Die Mindestanforderung für den Betrieb ist lediglich, dass ein IP-Netzwerk verfügbar ist. In den meisten industriellen Anwendungen lässt sich das bewerkstelligen.

Abbildung 12: OPC UA hebt Security auf Applikationsebene

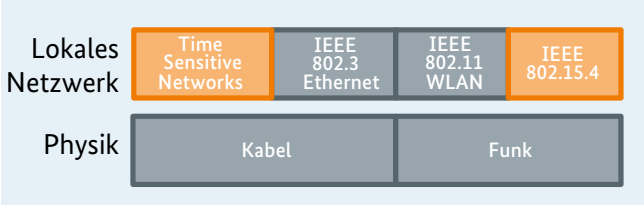


Sicherheitsanforderungen und -mechanismen auf den Schichten der Kommunikationsstacks

Die Sicherheit eines Gesamtsystems kann nicht auf einer einzigen Schicht oder an einer einzigen Stelle gewährleistet werden. Stattdessen müssen alle Stellen des Kommunikationsstacks sicher gestaltet sein. Das bedeutet: Sowohl die Funktionen und Managementmechanismen der Protokolle als auch die Vertraulichkeit und Integrität der Daten, die mittels der Protokolle transportiert werden, sind zu berücksichtigen. Wie Sicherheitsanforderungen und -mechanismen der einzelnen Schichten aussehen können, wird im Folgenden skizziert:

Netzwerks-Zugangs-Schicht (Data-Link Layer und Physical Layer)

Die Netzwerk-Zugangs-Schicht (OSI-Layer 1+2) umspannt die physische Übertragung eines Signals und die Vermittlung von Daten in einem lokalen Netzwerk. Dominante Technologien in OSI-Layer 1+2 sind IEEE 802.3 (Ethernet), IEEE 802.11 (Wireless LAN) sowie IEEE 802.15.4.



Eine zentrale sicherheitsrelevante Frage ist es, **welche Geräte am Netzwerk teilnehmen dürfen**. Es muss sichergestellt werden, dass nur berechtigte Teilnehmer Daten- oder Netzwerkpakete an das Netzwerk senden bzw. Daten vom Netzwerk empfangen können. Eine Verschlüsselung der Datenkommunikation (wie zum Beispiel bei WLAN) sowie die Authentisierung der Teilnehmer (beispielsweise über IEEE 802.1X/RADIUS) können dafür sorgen. Ein neuer Netzwerkteilnehmer weist sich zum Beispiel mit einer teilnehmerspezifischen Benutzerkennung und einem Passwort oder Zertifikat gegenüber dem Netzwerk aus. Greifen die Netzwerkzugangskontrollmechanismen, dann können unberechtigte Teilnehmer (etwa ein Angreifer mit einem eigenen Laptop) nicht am Netzwerk teilnehmen beziehungsweise den Datenverkehr im Netzwerk nicht entschlüsseln.

Auch der **physischen Sicherheit** (zum Beispiel Zugang zu Routern, Switches und Endsystemen durch unbefugte Personen) kommt auf der Netzwerk-Zugangs-Schicht eine große Bedeutung zu. Geeignete Schutzmaßnahmen reichen von abschließbaren Schränken für Netzwerkgeräte bis hin zum Abschalten von nicht verwendeten Ethernet-Ports in der Software.

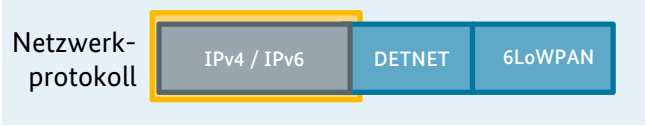
Die Netzwerk-Zugangs-Schicht hat eine weitere wichtige Aufgabe: Sie muss die **Quality of Service-Merkmale** erfüllen. Mit Technologien wie TSN ist es zum Beispiel möglich, Datenpakete in echtzeitkritischen Applikationen deterministisch auszuliefern. Jedoch sind auch hier Sicherheitsmechanismen einzubauen, um den echtzeitkritischen Verkehr vor Überlastungen durch andere Verkehrsarten zu schützen. Denn: Ein „Klassiker“ in der Automatisierungswelt ist eine fehlerhafte Komponente, die durch ein Übermaß an Datenverkehr eine Netzwerküberlast erzeugt und damit die Produktion lahmlegt.

Weitere mögliche Ziele eines Angreifers sind Protokolle, die die Vorgänge in der Netzwerk-Zugangs-Schicht verwalten. Manipuliert ein Angreifer diese Protokolle, kann das die Funktion eines Netzwerks empfindlich stören. Daher müssen **Funktionen der Verwaltungsprotokolle** wie zum Beispiel das Address Resolution Protocol (ARP), das Dynamic Host Configuration Protocol (DHCP), Multicast-Protokolle und QoS-Protokolle mithilfe geeigneter Maßnahmen (beispielsweise Port Security und DHCP snooping) vor Veränderungen und Störungen geschützt werden.

Wie auf allen anderen Schichten fallen auf der Netzwerk-Zugangs-Schicht **Betriebsdaten** an, die wichtige Hinweise geben, um Angriffe zu erkennen. Sie zeichnen beispielsweise auf, wann ein Gerät wo mit dem Netzwerk verbunden war oder welche anderen Netzwerkteilnehmer Pakete von einem Gerät erhalten (haben).

Netzwerkschicht

Die Netzwerkschicht mit ihrem prominenten Vertreter Internet Protocol (IP) verbindet einzelne IP-fähige Geräte auch über Netzwerkgrenzen hinweg: Durch sie können Geräte unternehmens- oder weltweit adressiert und erreicht werden. Umso unerlässlicher ist es, gewollte und nötige von ungewollten und gegebenenfalls schädlichen Kommunikationsverbindungen zu trennen.



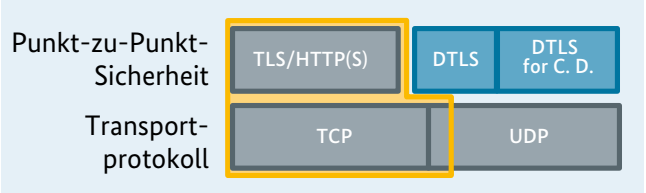
Um diese Verbindungen restriktiv zu gestalten, werden zum Beispiel **Access Control Lists, Firewalls und Gateways** eingesetzt. Mithilfe dieser Technologien und Geräte lassen sich Schutzkonzepte (zum Beispiel Zones & Conduits) wie in ISO/IEC 62443 beschrieben umsetzen. Geräte werden zu sinnvollen Funktionsgruppen zusammengefasst (zum Beispiel alle Geräte eines speziellen Anlagenteils), in denen die Kommunikation zwischen den Geräten selektiv erlaubt wird. Gleichzeitig kann die Kommunikation mit anderen Geräten unterbunden werden, wie etwa mit dem Notebook des Angreifers, auch wenn er sich im gleichen Unternehmen befindet. Diese Einteilung schränkt die Bewegungsmöglichkeiten des Angreifers im Netzwerk stark ein und schützt verwundbare Systeme davor, dass sie durch kompromittierte Komponenten beeinflusst werden. Das Eindringen in das System wird deutlich erschwert.

Darüber hinaus gibt es die Möglichkeit, auf der Netzwerkschicht **verschiedene sichere Netzwerke über unsichere Netzwerke zu verbinden**: mithilfe von Virtual Private Network (VPN)-Technologien. So lassen sich zum Beispiel Außenstellen einer Anlage über das Internet per VPN an eine zentrale Stelle im Unternehmen – meist bei der zentralen IT – anbinden. Auch hier ist darauf zu achten, dass die einzelnen Kommunikationsbeziehungen segmentiert werden (zum Beispiel durch Firewalls und Gateways).

Auch auf der Netzwerkschicht fallen **Daten an, die für den sicheren Betrieb relevant** sind. Sie können dazu verwendet werden, um Angriffe zu erkennen. Wenn etwa ungewöhnliche Kommunikation zwischen Geräten ohne Funktionsbezug stattfindet oder ungewöhnliche Kommunikationsmuster auftreten, ist Vorsicht geboten – das können Hinweise auf einen Angriff sein.

Transportschicht und Ende-zu-Ende-Sicherheit

Die Transportschicht verbindet einzelne Anwendungen auf unterschiedlichen Geräten. Um auf ihr Sicherheit zu gewährleisten, ist die Frage der Identität von Geräten und Diensten essenziell.



Im Internet haben sich zwei starke Vertreter für sichere Transportschicht-Verbindungen etabliert: die Protokolle **Transport Layer Security (TLS) und Datagram Transport Layer Security (DTLS)**. Auch Industrieprotokolle (wie zum Beispiel OPC UA) sind in der Lage, diese Protokolle zu verwenden.

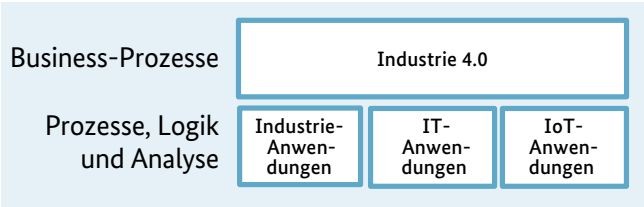
Die genannten Protokolle verwenden X.509-Zertifikate, um die **Identität eines Endsystems und die Zugehörigkeit zu einer bestimmten Organisation kryptografisch sicher zu bestimmen**. Zwischen den so authentifizierten Kommunikationsendpunkten wird eine Ende-zu-Ende-Verschlüsselung bzw. ein Ende-zu-Ende-Integritätsschutz etabliert. Das verhindert Angriffsversuche: Das Abhören von Verbindungen sowie die Veränderung von Daten durch einen Angreifer kann – bei geeigneter Wahl der kryptografischen Mechanismen – effektiv abgewehrt werden.

Die **Ende-zu-Ende-Verschlüsselung birgt jedoch nicht nur Vorteile** für die Sicherheit: Geräte wie Firewalls, die den weiterzuleitenden Verkehr auf Widrigkeiten untersuchen, können aufgrund der Verschlüsselung den weiterzuleitenden Verkehr nicht einsehen und so Angriffsmuster nicht mehr erkennen. Angriffe bleiben unentdeckt. Um eine Ende-zu-Ende-Sicherheit und gleichzeitig die Inspizierbarkeit des Verkehrs zu erreichen, gibt es Mittelwege: Der Verkehr kann in einem vertrauenswürdigen Gateway entschlüsselt werden. Dafür bricht das Gateway die gesicherte Verbindung auf und inspiziert die Daten. Dieser Ansatz hat jedoch Schwächen, vor allem bei der Frage, welchem Gateway zu trauen ist. Darüber hinaus ist er nicht für alle Protokolle verfügbar.

Auch auf der Transportschicht fallen Daten an, die für Überwachung und Angriffserkennung genutzt werden können. Dies sind insbesondere die Identitäten der Kommunikationsendpunkte und ihre Kommunikationsmuster.

Prozess- und Businesslogik

Oberhalb der beschriebenen Schichten befinden sich die Teile der Industrie 4.0-Kommunikation, die anwendungsspezifisch sind. Dazu gehören die Prozesslogik bzw. modellierte Geschäftsprozesse.



Schon seit Jahren existieren Darstellungsweisen, mit denen Prozess- und Businesslogiken genormt beschrieben und ausgetauscht werden, zum Beispiel **UML (Unified Modeling Language), BPMN (Business Process Model and Notation) und BPEL (Business Process Execution Language)**. Darüber hinaus haben sich in der Industrie entsprechende Modelle im Office-Bereich und auf der Produktionsebene etabliert, wie etwa **SOA (Service-oriented Architecture)** und wesentlich digitalisierte Ausführungssysteme wie **MES (Manufacturing Execution System)** und **ERP (Enterprise Resource Planning)**.

Eine einheitliche Form, um in der Industrie 4.0 mit den Vorgängen und Daten dieser Schichten umzugehen, ist die **Verwaltungsschale** (Administration Shell). Sie verbindet Daten- und Interaktionsmodelle und stellt essenzielle Sicherheitsfunktionen zur Verfügung (zum Beispiel Authentisierung, Integritätsschutz, Zugriffsschutz und Ereignisprotokollierung). Auch auf diesen beiden Schichten sind **Identitäten der Teilnehmer, die in eine Industrie 4.0-Kommunikation** einbezogen sind, ihre Rollen und Rechte zentral. Da auf den oberen Schichten Industrieprozesse und Geschäftslogik modelliert und umgesetzt werden, sind geeignete Maßnahmen essenziell, die Zuverlässigkeit und Rechtssicherheit schaffen. Insbesondere müssen Vorgänge auditierbar und das System oder eine Partei nachweisbar vertrauenswürdig sein.

Da bereits viele Unternehmenssysteme existieren, die Geschäftsprozesse und Informationen verwalten und modellieren, müssen hier gegebenenfalls viele **bestehende Legacy-Systeme durch Adapter und Gateways miteinander verbunden** werden. Wichtig ist: Bei einer solchen Verbindung gilt es, Sicherheitseigenschaften und die Nachvollziehbarkeit von Aktionen zu erhalten. Also zu erfahren, wer wann mit wem und worüber kommuniziert hat.

Teile der Prozess- und Businesslogik können auch **unternehmensübergreifend** implementiert werden. Denkbar ist, dass IT-Systeme anderer Unternehmen (zum Beispiel Zulieferer oder Kunden) oder Systeme von Drittanbietern (zum Beispiel Cloud-Systeme) auf dieser Ebene mit den eigenen Anwendungen verwoben werden. Insbesondere bei der unternehmensübergreifenden Kommunikation ist darauf zu achten, dass geeignete Schutzmechanismen existieren, dass die Kommunikationsvorgänge und Transaktionen nachvollzogen werden können und dass das Unternehmen in einem rechtssicheren Rahmen agiert.

Anwendungsbeispiel: Auftragsgesteuerte Produktion

Auf den vorherigen Seiten wurden Kommunikationsstacks und mögliche Protokolle betrachtet. Doch um sicherzustellen, dass alle zentralen Aspekte der sicheren Kommunikation berücksichtigt werden, gilt es auch, relevante Industrie 4.0-Anwendungsfälle genauer zu betrachten.

Das Anwendungsbeispiel zeigt unter anderem die Kommunikationsbeziehungen einer „Auftragsgesteuerten Produktion eines individuellen Fahrradlenkers“ der Plattform Industrie 4.0 (11) (Abbildung 13[2]). In Abbildung 14 ist das Sequenzdiagramm für die Kommunikationsschritte dargestellt:

Schritt 1: Fahrradhersteller überträgt Ausschreibung an Vermittlungsdienst

Schritt 2: Vermittlungsdienst verteilt Ausschreibung an mögliche Zulieferer

Schritt 3: Interessierte Zulieferer unterbreiten Angebote an Vermittlungsdienst

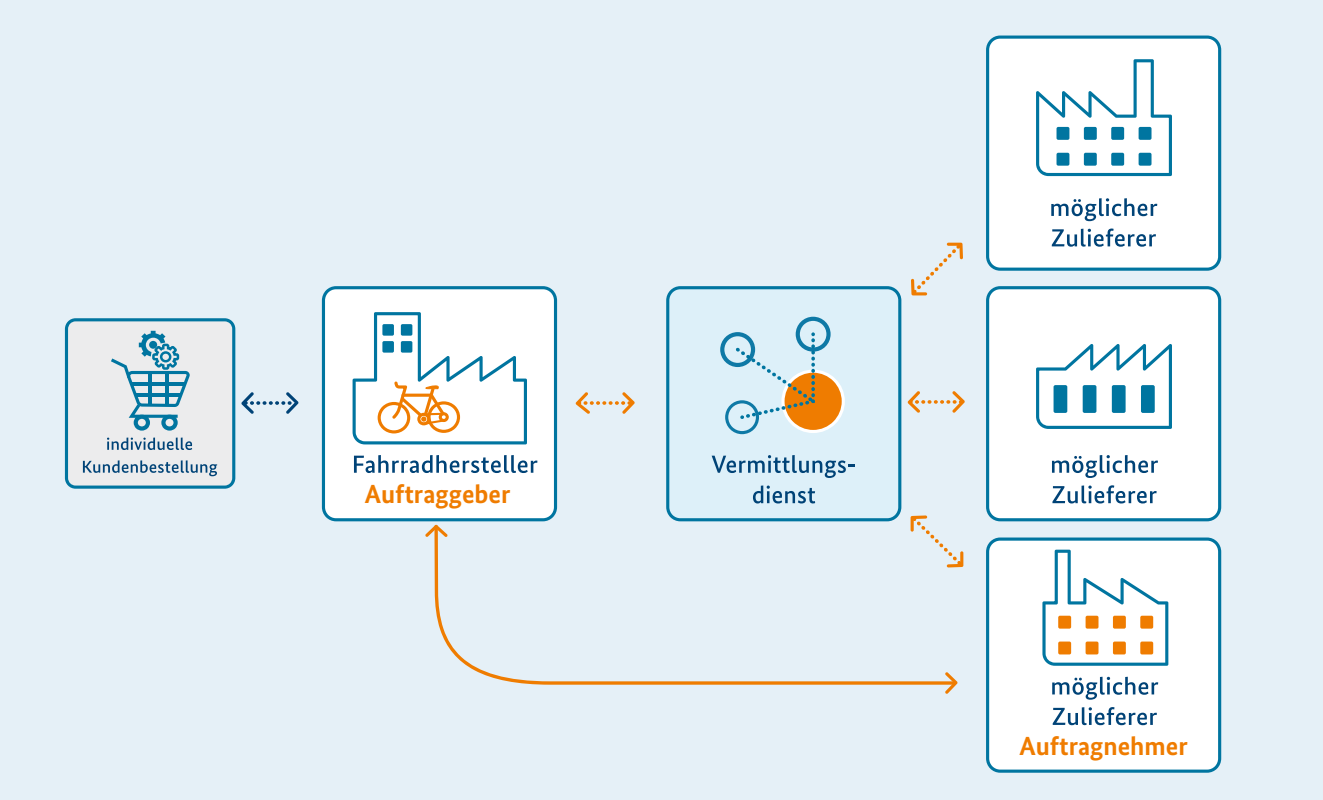
Schritt 4: Vermittlungsdienst übermittelt vorgefilterte Angebote an den Fahrradhersteller

Schritt 5: Fahrradhersteller (Auftraggeber) erteilt Auftrag direkt an ausgewählten Zulieferer (Auftragnehmer)

Schritt 6: Auftragnehmer übermittelt dem Auftraggeber zugesagte Daten über das individuell gefertigte Produkt als Teil des Produktgedächtnisses

Schritt 7: *Physisches Produkt wird ausgeliefert*

Abbildung 13: Auftragsgesteuerte Produktion eines kundenindividuellen Fahrradlenkers



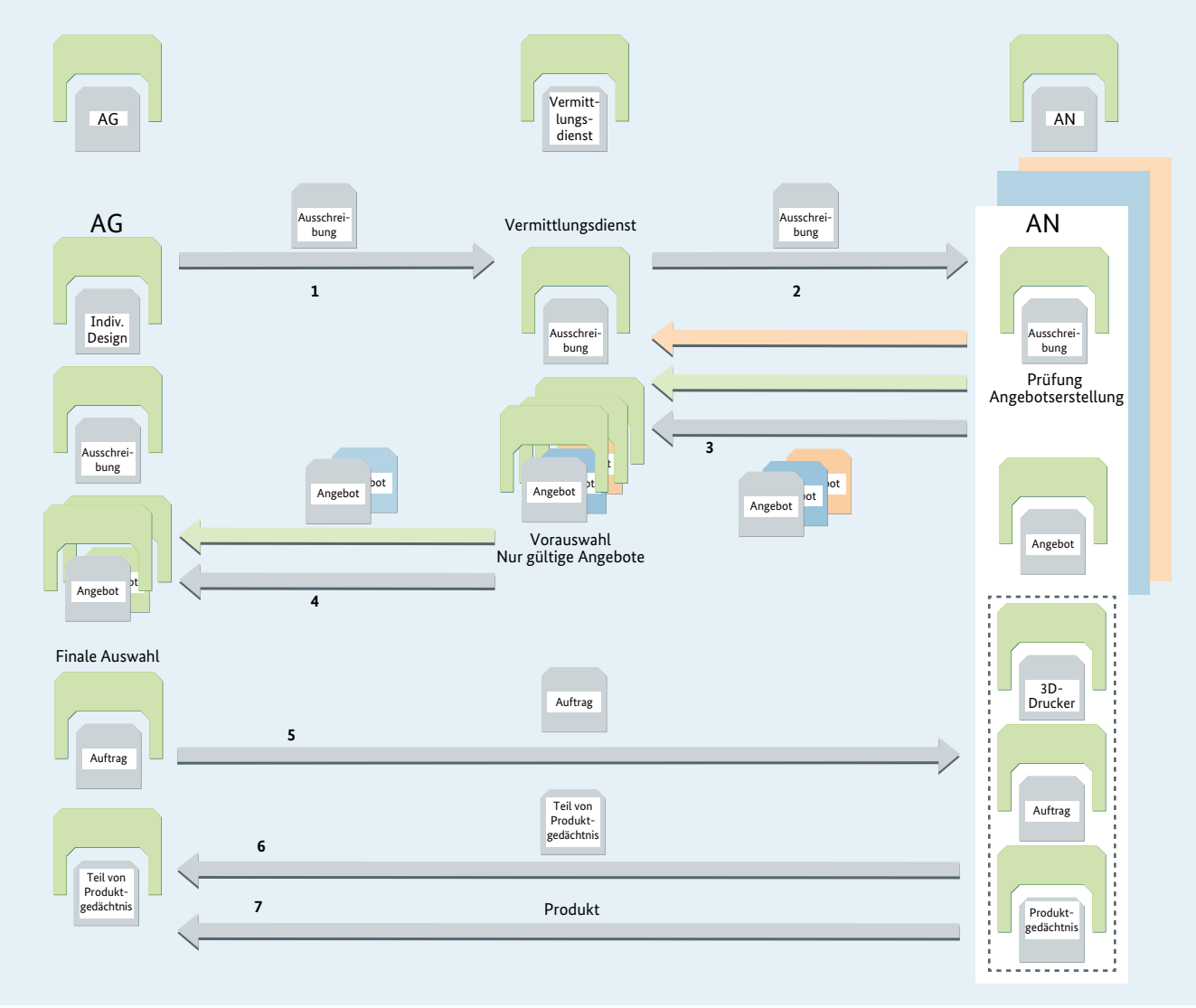
2 Im Anwendungsbeispiel wird eine Ausschreibung betrachtet, die neben den technischen Anforderungen an das Produkt auch alle kommerziellen und rechtlichen Randbedingungen enthält. Diese Ausschreibung wird vom Vermittlungsdienst, häufig auch als Broker bezeichnet, an mögliche Zulieferer weiterverteilt. Die möglichen Zulieferer sind vorab vom Vermittlungsdienst qualifiziert, was auch eine Bewertung der Vertrauenswürdigkeit/Trustworthiness bezüglich der IT-Security beinhaltet. Schließlich sind viele der ausgetauschten Daten, u.a. die 3D-Druckdaten des kundenindividuellen Fahrradlenkers, schützenswerte Informationen.

Für jeden dieser Schritte können nun Anforderungen an die Kommunikation beschrieben werden. So lässt sich feststellen, welche Protokolle sich eignen. Außerdem können anhand dieser Schritte entsprechende Weiterentwicklungen bestehender Protokolle angegangen werden.

Wie die Ausschreibung vom Fahrradhersteller an den Vermittlungsdienst übertragen wird (erster Kommunikationsschritt), wurde beispielhaft in Abbildung 15 betrachtet. Es wird deutlich: Für die rechtssichere Abwicklung sind hauptsächlich Security-Themen relevant. Technische Anforderungen an den Kommunikationsprozess hingegen, wie sie im automationsnahen Bereich typischerweise im Zeitverhalten bestehen, sind für den hier betrachteten Fall weniger relevant. Die Abwicklung darf mehrere Sekunden dauern, ohne dass der Ablauf dadurch scheitert.

Um die Ausschreibung zu übertragen, ist sicherzustellen, dass die darin enthaltenen Daten in allen Belangen integritätsgeschützt und gegebenenfalls durch eine elektronische Unterschrift authentifiziert sind. So wird gewährleistet, dass die Ausschreibung nicht verfälscht werden kann – weder bei der Übertragung an den Vermittlungsdienst noch bei der Weiterverteilung an die möglichen Zulieferer. Darüber hinaus kann es sinnvoll sein, auf der Übertragungsstrecke zum Vermittlungsdienst und bei der anschlie-

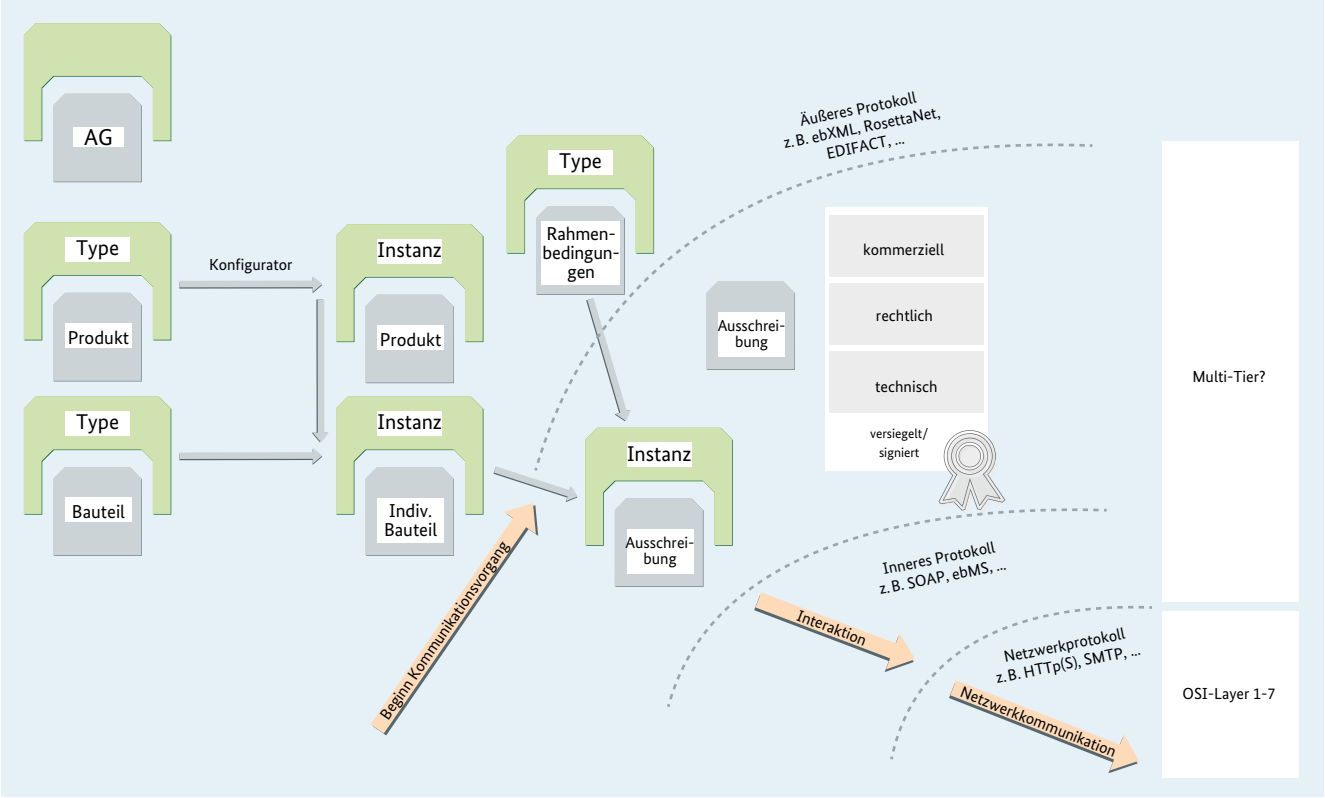
Abbildung 14: Kommunikationssequenz der Auftragsabwicklung



ßenden Weiterverteilung auf eine vertrauliche Übermittlung zu setzen. Allerdings sollten dabei die Anforderungen und Umsetzungen getrennt betrachtet und für die eingesetzten Protokolle bewertet werden: zum einen die der Vertraulichkeit auf dem Kommunikationsweg, zum anderen die des Integritätsschutzes der Information selbst.

Abbildung 15 zeigt eine Möglichkeit, wie das technisch umgesetzt werden könnte (Hinweis: Sie nennt beispielhaft Protokolle, die im Bereich des Electronic Business eingesetzt werden, ohne tiefergehend zu betrachten, ob sie sich tatsächlich eignen.): Im ersten Schritt wird die Ausschreibung als Nachricht erstellt und digital signiert. Auf dem Weg zum Vermittlungsdienst wird diese Nachricht verschlüsselt. Da die digitale Signatur der Ausschreibung immer zur Verfügung steht, bleiben sowohl beim Vermittlungsdienst als auch bei einer weiteren Übertragung Integrität und Authentizität immer erhalten.

Abbildung 15: Kommunikationsschritt 1 – Mögliche Übertragung einer Ausschreibung



Zusammenfassung und Ausblick

Das Diskussionspapier zeigt: Um eine sichere Kommunikation zu gewährleisten, müssen die verschiedenen Schichten der Kommunikationsprotokolle betrachtet werden. Wichtig ist, dass dafür viele verschiedene Anwendungsfälle analysiert werden, denn nur so lassen sich mögliche Protokolle und Umsetzungsstrukturen vergleichen und bewerten, um die Kriterien für Industrie 4.0-konforme Kommunikation zu erarbeiten.

Das oben dargestellte Beispiel aus dem Anwendungsszenario „Auftragsgesteuerte Produktion" behandelt einen Geschäftsvorfall. Kommen technische Prozesse hinzu, dann werden darüber hinaus weitere Aspekte wichtig sein, die besonders die sicherheitstechnische und laufzeitdynamische Ausgestaltung der Kommunikation (zum Beispiel Latenz) beeinflussen.

Daher soll in der weiteren UAG-Arbeit unter anderem ein Szenario auf der Automatisierungsebene beschrieben und untersucht werden, bei dem Echtzeitkommunikation und das Zusammenwirken von Systemen verschiedener Hersteller relevant sind. Darüber hinaus wird ein weiterer wichtiger Baustein sein, unternehmensübergreifende Kommunikation und die Einbindung von Cloud-Diensten genauer zu beleuchten. Denn hier steht die Industriewelt vor der Herausforderung, die Kommunikation so zu gestalten, dass sie flexibel ist und organisatorische, also manuelle, Aufgaben im Betrieb minimiert. Dabei empfiehlt es sich, die Erkenntnisse anderer Expertengruppen zum Thema, wie etwa das IIC Connectivity Framework (12), das IIC Security Framework (13) oder die Referenzarchitektur des Industrial Data Space (14), in die künftigen Betrachtungen einzubeziehen.

Literaturverzeichnis

1. *Technischer Überblick „Sichere unternehmensübergreifende Kommunikation".* Berlin: Plattform Industrie 4.0, 2016.

2. *Facilitating International Cooperation for Secure Industrial Internet of Things/Industrie 4.0.* Berlin: Plattform Industrie 4.0, 2017.

3. Common automation device – Profile guideline. IEC TR 62390:2005.

4. *Security der Verwaltungsschale.* Berlin/Frankfurt: Plattform Industrie 4.0/ZVEI, 2017.

5. *Interaktionsmodell für Industrie 4.0-Komponenten.* Berlin: Plattform Industrie 4.0, 2016.

6. *Netzkommunikation für Industrie 4.0.* Berlin: Plattform Industrie 4.0, 2016.

7. Reference Model for Industrie 4.0 Service architectures – Basic concepts of an interaction-based architecture. DIN SPEC 16593, 2017.

8. *Technischer Überblick „Struktur der Verwaltungsschale".* s.l.: Plattform Industrie 4.0, 2016.

9. *Com4.0-Basic: Basic Models of Communication.* Aachen: RWTH Aachen, 2016.

10. *Network-based Communication for Industrie 4.0: Proposal for an Administration Shell.* Berlin: Plattform Industrie 4.0, 2016.

11. *Anwendungsszenario trifft Praxis: Auftragsgesteuerte Produktion eines individuellen Fahrradlenkers.* Berlin: Plattform Industrie 4.0, 2017.

12. *The Industrial Internet of Things/Volume G5: Connectivity Framework*. Needham, MA, USA: Industrial Internet Consortium, 2017.

13. I*ndustrial Internet of Things/Volume G4: Security Framework.* Needham, MA, USA: Industrial Internet Consortium, 2016.

14. *Reference Architecture Model for the Industrial Data Space.* München/Berlin: Fraunhofer Gesellschaft/Industrial Data Space e.V., 2017.

AUTOREN:
Prof. Dr. Tobias Heer, Hirschmann Automation & Control GmbH; Markus Heintel, Siemens AG; Stefan Hiensch, Bundesnetzagentur; Dr. Lutz Jänicke (Leitung), Phoenix Contact GmbH & Co KG; Michael Jochem, Robert Bosch GmbH; Bernd Kärcher, Festo AG & Co. KG; Marcel Kisch, IBM Deutschland GmbH; Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik; Gerhard Oeynhausen, Telekom AG; Tobias Pfeiffer, Festo AG & Co. KG; Frank Schewe, Phoenix Contact Electronics GmbH; Dr. Michael Schmitt, SAP SE; Dr. Dirk Schulz, ABB AG; Detlef Tenhagen, HARTING AG & Co KG; Klaus Theuerkauf, IFAK Institut für Automation und Kommunikation e.V.; Andreas Teuscher, SICK AG; Thomas Walloschke, Fujitsu Technology Solutions GmbH

Diese Publikation ist ein gemeinsames Ergebnis der Arbeitsgruppen „Sicherheit vernetzter Systeme“ und „Referenzarchitekturen, Standards und Normung“ (Plattform Industrie 4.0).

www.plattform-i40.de