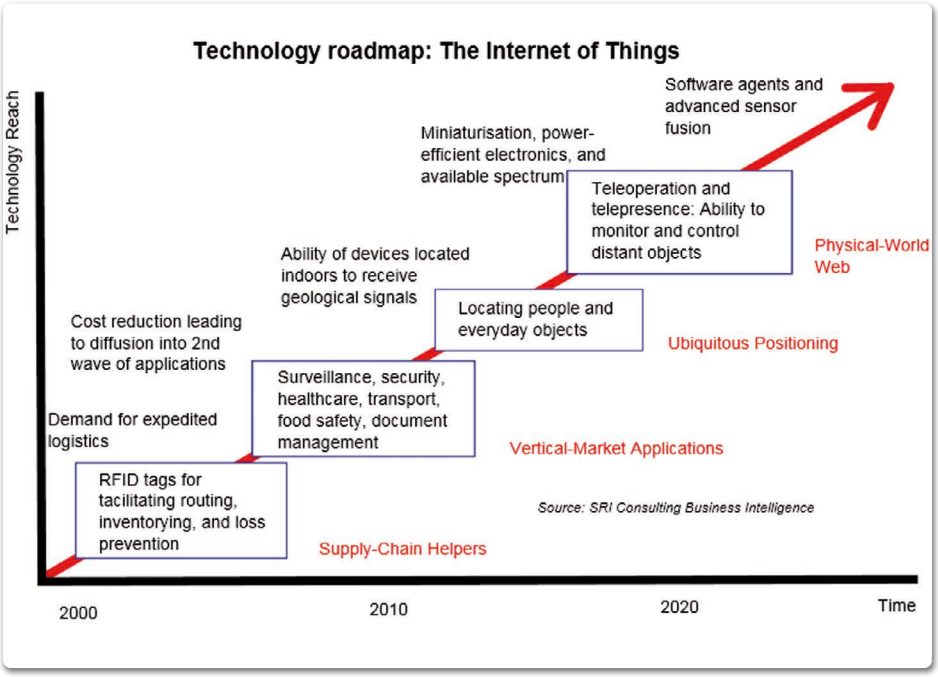
Das IIoT – Grundlagen, Protokolle und Umsetzung

Eine IIoT-Applikation lässt sich nicht einfach nebenbei realisieren. Man benötigt Basiswissen, muss zwecks optimaler Auswahl Protokolle kennen und schließlich imstande sein, die Anwendung einzurichten.



Internet of Things (IoT) bedeutet im Wesentlichen die Vernetzung eines Haushalts oder Unternehmens und seine Anbindung an das Internet. 1999 wurde der Begriff am Auto-ID Center am Massachusetts Institute of Technology geboren. Die Vision dahinter: Computer sollen in der Lage sein, sich unabhängig vom Menschen Informationen zu beschaffen. Die reale Welt muss für die PCs zugänglich sein – ohne Zutun der Menschen. Dies ist heute im großen Maßstab möglich. Tendenz steigend.

Das Industrial Internet of Things (IIoT)

IIoT-Projekte gibt es bereits in vielen Unternehmen. Bis 2029 sind laut Gartner bis zu 15 Milliarden IoT-Geräte mit Unternehmensinfrastrukturen verbunden und erledigen dabei vielfältige Aufgaben. Das IIoT ist die Nutzung der IoT-Technologien in Produktion und Industrie mit folgenden Zielen:

- Verbesserung der betrieblichen Effizienz
- Kostensenkungen in der Produktion
- Beschleunigung von (Produktions-) Prozessen
- Produktionsausfallkontrolle
- Verkürzung von Ausfallzeiten durch Fernwartung
- Produktentwicklung auf Basis rein digital vorliegender Anforderungen
- kostengünstigere Einzel- oder Kleinserienproduktion
- verbesserte Sicherheit für Mensch und Maschine
- Transport der Produkte mit höherer betrieblicher Effizienz
- Optimierung des Geschäftsmodells
- Ermöglichung neuer Geschäftsmodelle

Diese Ziele sind heute erreichbar, weil smarte, vernetzte Maschinen schneller, exakter, kostengünstiger und effizienter arbeiten können als von Menschen gesteuerte Maschinen.

Das IIoT ist in vielen Industriesparten einsetzbar. Produzierende Betriebe erreichen damit Effizienzsteigerungen durch flexiblere Produktionstechniken und die Nutzung intelligent vernetzter industrieller Systeme.

Eine zentrale Rolle dabei spielen Sensoren und ihre Daten, da diese die Basis für die Automation und selbstlernende Maschinen darstellen. Und da ein funktionierendes IIoT große Datenmengen in hoher Geschwindigkeit verarbeiten muss, spielen Big-Data-Technologien darin eine wichtige Rolle. Sind diese implementiert, dann kann man Produktionsprozesse auf Basis der erhobenen und verarbeiteten Daten automatisieren und sogar ohne Betriebsunterbrechung flexibel und unverzüglich an veränderte Anforderungen anpassen. Die Datenbasis und die laufende Verarbeitung aktueller Sensordaten erlaubt es den eingesetzten Maschinen sogar, quasi selbstständig zu erkennen, wann Bedarf an Wartung besteht.

IoT und IIoT benötigen intelligente und vernetzte Geräte. Das IoT soll den Komfort für Benutzer steigern und günstig sein. Das IIoT nutzt hochwertige Devices mit präzisen Sensoren und soll helfen, Produktionsprozesse optimal zu steuern und zu überwachen.

Protokolle/Standards

Je komplexer IIoT-Infrastrukturen werden, desto wichtiger ist es, dass Protokolle und Standards harmonieren. Wer das IIoT nutzen will, braucht darüber gründliche Kenntnisse. Denn IIoT-Protokolle steuern die Kommunikation zwischen den IoT-Geräten, Servern und Diensten, die die einzelnen Geräte miteinander verbinden und deren Daten analysieren. Die Kommunikation spielt zwischen den IIoT-Geräten eine genauso wichtige Rolle wie zwischen Endgeräten und Gateways. (Ein Gateway stellt eine Verbindung zwischen zwei Systemen her bzw. ein IT-System, das seinen Kommunikationspartner nicht direkt kennt, wendet sich an sein Gateway.) Dadurch entstehen oft vielschichtige Infrastrukturen, die vom eingesetzten IIoT-Protokoll abhängen.

Häufig kommt in IIoT-Infrastrukturen das OSI-Schichtenmodell zum Einsatz. OSI steht für Open Systems Interconnection Model. Das ist ein Referenzmodell, mit dem sich die Kommunikation zwischen Systemen beschreiben und definieren lässt. Es besitzt sieben hierarchischen Schichten (Layers) mit jeweils klar voneinander abgegrenzten Aufgaben. Die Schnittstellen zwischen den Schichten sind exakt beschrieben. Jede Schicht bietet der direkt über ihr liegenden Schicht Dienste zur Nutzung an. Kommunizieren zwei Systeme miteinander, werden alle sieben Schichten mindestens zweimal durchlaufen, da sowohl der Sender als auch der Empfänger das Modell zu berücksichtigen hat. Netzwerkelemente und Zwischenstationen basieren je nach Funktion nur auf einer begrenzten Anzahl an Layers. So arbeitet beispielsweise ein Router auf den Schichten 1 bis 3. Die Schichten 5 bis 7 sind anwendungsorientiert.

In jeder Schicht eines Referenzmodells sind Protokolle definiert. Das sind Zusammenstellungen von Regeln zur Kommunikation in der jeweiligen Schicht. Gegenüber den Protokollen der darüber oder darunter liegenden Layers sind sie transparent. An den Übergängen der Schichten kommunizieren die Protokolle über Schnittstellen.

Einige Protokolle erfüllen Aufgaben mehrerer Schichten und erstrecken sich über zwei oder mehr Layers. Es ist aber auch durchaus möglich, mehrere Protokolle zu verwenden, wenn Bandbreite und Verbindungsqualität im IIoT-Netzwerk nicht homogen sind und die Qualität der Verbindungen manchmal nachlässt. Weiter sollte man wissen, dass bestimmte Protokolle einen gewissen Overhead erzeugen, mit denen die Endgeräte klarkommen müssen. Und last not least darf man natürlich die Sicherheit nicht vernachlässigen.

Advanced Message Queuing Protocol

Das AMQP bietet sich an, wenn verschiedene Standards im Nachrichtenformat vorhanden sind. Damit ist ein sicherer und schneller Austausch von sehr vielen Nachrichten möglich.

Das Protokoll ist auch eine gute Wahl, wenn die verschiedenen Devices nicht mit schnellen Netzwerken verbunden sind oder wenn nicht alle Geräte jederzeit verfügbar sind. Viele IoT-Dienste von Cloud-Plattformen unterstützen AMQP.

Bluetooth und WLAN

Diese bekannten Technologien werden vor allem in den unteren Schichten genutzt.

Bluetooth in der Ausprägung Low Energy (LE) erlaubt dabei besonders energiesparende Netzwerke. Die Bluetooth-Technologie nutzt das 2,4-GHz-ISM-Band (2400 bis 2483,5 MHz), das ein gutes Gleichgewicht zwischen Reichweite und Durchsatz ermöglicht.

WLAN steht für Wireless Local Area Network. WLANs stellen Anpassungen der Schicht 1 und 2 des OSI-Referenzmodells (s. Kasten) dar.

Der Frequenzbereich im 2,4-GHz-Band wurde in 14 Kanäle aufgeteilt. Für überlappungsfreie Funkzellen sind in Europa vorgeschriebene Kanalkombinationen zu verwenden. Die Frequenzen 5755 bis 5925 MHz sind in Deutschland von der Bundesnetzagentur für Broadband Fixed Wireless Access (BFWA) für gewerbliche öffentliche Netze freigegeben und meldepflichtig. Die Reichweite ist stets auf einige 10 m im Gebäude begrenzt.

Übrigens: Neuerdings tragen WLAN-Standards einfache Bezeichnungen. So heißt die neue Variante einfach WiFi 6 statt 802.11ax, während für den Vorgänger 802.11ac WiFi 5 verwendet wird. Gerade in sogenannten High-Density-Bereichen, z.B. in Bereichen, wo mehrere IoT-Devices gleichzeitig auf das WLAN zugreifen, sorgt WiFi 6 für eine zuverlässigere Netzwerkverbindung. Zum Einsatz kommen wie gewohnt Bänder bei 2,4 und 5 GHz. WiFi 6E verwendet den Frequenzbereich zwischen 5,925 und 7,125 GHz.

Einbettung in den Mobilfunk

Die IIoT-Technologie lässt sich auch mithilfe der bestehenden Mobilfunktechnologie umsetzen. Mit aktuell vierten Generation 4G und der sich entwickelnden fünften Generation 5G kann man die IIoT-Daten sehr schnell versenden. Dabei sind im Gegensatz zu Bluetooth und WLAN auch große Netzwerke möglich.

Den Vorteilen „bereits bestehendes System“, „hohe Geschwindigkeit“ und „Möglichkeit großer Netzwerke“ stehen jedoch als Nachteile laufend anfallende Kosten und ein höher Energieverbrauch gegenüber.

Mit Ethernet „auf Draht“

„Seit dem Aufkommen des Industrial IoT war die Verbindung aller Produktionsanlagen, wie Sensoren, Aktoren, Roboter und unzählige andere Geräte, jedoch in der Regel mit proprietären, herstellerspezifischen Netzwerken verbunden.

Allerdings wird sich diese überholte Herangehensweise mit der Verfügbarkeit von Single-Pair Ethernet (SPE) ändern.“ So steht es in unserem Beitrag „Der Aufstieg von Single-Pair Ethernet im IIoT“ in elefab 3/2022 S. 30ff, wo Sie mehr erfahren.

Abstecher: TCP und UDP

TCP steht für Transmission Control Protocol und ist ein sogenanntes verbindungsorientiertes Protokoll, was bedeutet, dass es maßgeblich Datenverluste verhindert durch Bestätigungen beim Datenempfang, dass es Dateien und Datenströme aufteilen und Datenpakete den Anwendungen zuordnen kann. Aus Sicht der Anwendungen ist TCP transparent. Diese übergeben ihren Datenstrom an den TCP/IP-Stack und nehmen ihn von dort auch wieder entgegen. (Ein Stack ist eine häufig verwendete hierarchische Grundstruktur. Sie besteht in der Regel aus logisch übereinander gestapelten Software-Funktionskomponenten.)

Mit der für die Übertragung nötigen TCP-Paketstruktur und mit den Parametern der ausgehandelten Verbindung haben die Anwendungen nichts zu tun.

UDP steht für User Datagram Protocol und ist ein sogenanntes verbindungsloses Protokoll, angesiedelt auf der Schicht 4, der Transportschicht des OSI-Schichtenmodells. Es hat damit eine vergleichbare Aufgabe wie das verbindungsorientierte TCP, arbeitet dabei aber nicht so sicher. Denn der Absender weiß nicht, ob seine verschickten Datenpakete angekommen sind, weil keine Bestätigungen beim Datenempfang erfolgt.

Das hat aber den Vorteil, dass der Paket-Header viel kleiner ist und dass es auf der Übertragungsstrecke keine zeitverzögernden Bestätigungen gibt. (Man spricht von einem Header, wenn ein bestimmtes Element immer wieder vor anderen verwendet oder als Standardelement von etwas anderem eingesetzt wird.)

Constrained Application Protocol

Das CoAP nutzt generell UDP und kann dadurch eine schnelle Kommunikation aufbauen. Vor allem bei geringen Bandbreiten kann es die richtige Wahl sein, wenn IIoT-Geräte untereinander kommunizieren sollen. Der Energiebedarf ist niedriger als beim Einsatz von Mobilfunk-Technologien, daher bietet es sich für die Machine-to-Machine-Kommunikation (M2M) an.

Das CoAP eignet sich vor allem für sehr große und verteilte IIoT-Infrastrukturen mit schmaler Bandbreite und kurzen Nachrichten. Dabei lassen sich die Daten auch verschlüsseln und über HTTP-Proxys versenden. HTTP steht für Hypertext Transfer Protocol, ein Protokoll zur Übertragung von Daten auf der Anwendungsschicht über ein Rechnernetz. Es wird hauptsächlich eingesetzt bei Internet-Webseiten. Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk aus Rechnern in Form eines physischen Computers. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.

Data Distribution Service für die Echtzeitkommunikation

In vielen Fällen sollen Daten in Echtzeit verschickt werden. Dazu muss das eingesetzte Protokoll natürlich in der Lage sein. Data Distribution Service (DDS) ist dies und kann somit sicherstellen, dass IIoT-Geräte in einer IIoT-Infrastruktur mit sehr niedriger Latenz miteinander kommunizieren. Man verwendet das Protokoll daher vor allem in schnellen und zuverlässigen Netzwerken, die stabil miteinander verbunden sind und eine relativ hohe Bandbreite bieten.

Extensible Messaging and Presence Protocol (XMPP)

Auch auf Basis von XMPP ist eine Echtzeitkommunikation möglich. Für die Kommunikation nutzt das Protokoll die Extensible Markup Language, abgekürzt XML; das ist eine Auszeichnungssprache zur Darstellung hierarchisch strukturierter Daten im Format einer Textdatei, die sowohl von Menschen als auch von Maschinen lesbar ist.Früher war XMPP als Jabber bekannt und wurde vor allem für die Kommunikation zwischen Benutzern eingesetzt. Mittlerweile dient XMPP vor allem der Kommunikation zwischen Maschinen.

Da seine Basis XML ist, eignet sich das Protokoll nur für relativ leistungsfähige IIoT-Geräte, die mit dem entsprechenden Overhead (= Daten, die als Zusatzinformation benötigt werden) umgehen können.

Lightweight M2M

Auch Lightweight M2M (LWM2M) dient der Kommunikation zwischen Geräten in einer IIoT-Infrastruktur und eignet sich dabei vor allem für Telemetrie und zur Verwaltung der IIoT-Devices, wenn die Endgeräte keine hohe Leistung haben und wenig Energie verbrauchen sollen. Das hat LWM2M mittlerweile zu einem der wichtigsten Protokolle für die Verwaltung aus der Ferne gemacht. Die IoT-Geräte benötigen keine dauerhafte externe Stromversorgung. Eine mögliche Anwendung ist die Nachverfolgung von Waren.

LWM2M ist eine Ausprägung des Lightweight Data Access Protocols.

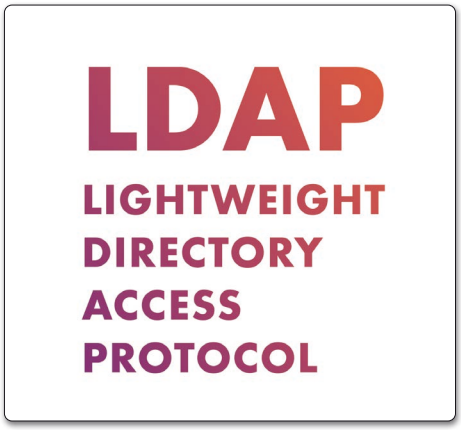
LoRa und LoRaWAN

Gemeinsam kommen LoRa und LoRaWAN vor allem im Bereich der Machine-to-Machine-Kommunikation (M2M) zum Einsatz. Die Nodes (Netzknotenpunkte) senden dabei im LoRaWAN Daten mit LoRa zum Gateway und zum verarbeitenden Server.

LoRa(WAN) steht für Long Range (Wide Area Network). Speziell für das IoT entwickelt, sorgt dieser Netzwerkstandard für energieeffizientes Senden und Empfangen über große Entfernungen und ist damit die Alternative für Fälle, wo Mobilfunknetze keine ausreichende Abdeckung bieten. Er nutzt quelloffener Software sowie nichtlizenzierter Frequenzbänder. LPWANs sind die am schnellsten wachsende Art drahtloser Netzwerke, die aktuell im zellulären IoT eingesetzt werden

Message Queuing Telemetry Transport

Der Standard MQTT erlaubt die Kommunikation zwischen Maschinen auch dann, wenn die Bandbreite nicht sehr hoch ist, verbunden mit



Geräten mit extrem hoher Latenzzeit. Somit ist es ein nahezu ideales Protokoll für die Machine-to-Machine-Kommunikation (M2M).

MQTT funktioniert nach dem Publisher/Subscriber-Prinzip und wird über einen zentralen Broker betrieben. Das bedeutet, dass Sender und Empfänger keine direkte Verbindung haben. Die Datenquellen melden ihre Daten über einen Publish, und alle Empfänger mit Interesse an gewissen Nachrichten bekommen die Daten zugestellt, wenn sie sich als Subscriber angemeldet haben. Somit kann MQTT z.B. auch bei Sensoren genutzt werden, die als Publisher Informationen zur Verfügung stellen und als Subscriber diese Daten nutzen. Im IIoT wird MQTT bis hin zu Anbindung von Cloud-Umgebungen eingesetzt.

Zigbee

Entwickelt für die Gebäudeautomatisierung, hat Zigbee seinen Schwerpunkt in der Kommunikation zwischen Geräten in einem Gebäude oder in einer Industrieanlage. Hier handelt es sich um ein Mesh-Protokoll (Mesh = Masche, Maschennetz) zur Verbindung von Devices über kurze Entfernungen. Dabei wurde auch auf einen sehr geringen Energieverbrauch geachtet. Auch Zigbee arbeitet im 2,4-GHz-Band.

Zur Einrichtung

Diese erfolgt schrittweise. In der Regel empfehlen sich folgende Schritte:

1. Anlage sicher verbinden (Konnektivität)
2. Service optimieren und Kunden involvieren
3. Umsetzen der Digitalisierung

Die Schritte 1 und 2 können als Vorbereitung für die letztendliche Implementierung des IIoTs angesehen werden. Sie sind die Grundlage für eine standardisierte Maschinenvernetzung. Hierbei sammeln Anlagenbetreiber erste Erfahrungen mit strukturierten Service-Angeboten auf Basis des Fernzugriffs. Und ist schließlich die Maschinenvernetzung mit einer offenen Lösung realisiert, die auch Schnittstellen für die Anbindung an gängige Cloud-Plattformen bietet, dann sind aller Voraussetzungen für die weitere Digitalisierung wie Asset-Optimierung und vorausschauende Wartung gegeben.

Anlage sicher verbinden

Zunächst gilt es, die Konnektivität der Anlage herzustellen. Lt. einer Studie der Arc Advisory Group können 63% aller routinemäßigen Instandhaltungsarbeiten auch aus der Ferne erfolgen, jedoch erlaubt ein Großteil industrieller Anlagen noch keinen Fernzugriff. Dabei ist dieser vielfach offensichtlich von Vorteil für den Anlagenbetreiber. Wenn der Betreiber im Interesse hoher Anlagenverfügbarkeit an einer zügigeren Fehlerbehebung und an einem direkten Kontakt zum Maschinenexperten interessiert ist sowie an geringeren Kosten für den Service, dann führt am Fernzugriff kein Weg vorbei.

Der Knackpunkt beim Fernzugriff sind – nicht unbegründete – Sicherheitsbedenken. Diese lassen sich nur durch intensive Beschäftigung und damit Kompetenzerwerb in punkto Sicherheit ausräumen. Der Anbieter hat plausibel zu erklären, warum der Fernzugriff sicher ist: Welche Sicherheitsstandards wurden wie implementiert, warum und weswegen. Die Einhaltung hoher Sicherheitsstandards kann als Grundvoraussetzung gelten.

Darüber hinaus macht es Sinn, wenn der Anlagenbetreiber die Möglichkeit hat, etwa über einen Schlüsselschalter direkt an der Maschine die Fernverbindung für den Fernzugriff freizugeben oder abzuschalten. Dies insbesondere, wenn der Fernzugriff nur im Fehlerfall genutzt wird.

Der Fernzugriff wurde in der Vergangenheit meist nur optional angeboten, was sich nun schrittweise zu ändern scheint.

Service optimieren und Kunden involvieren

Die Maschinenvernetzung bietet dem Anlagenbetreiber, seinem Produktionsleiter und/oder den Instandhaltungsmitarbeitern nicht automatisch Vorteile. Um hier einen optimalen Mehrwert zu generiert, ist vor allem der Maschinenbauer gefordert. Dieser könnte dem Betreiber etwa im Rahmen eines erweiterten Services Zugriffsrechte freischalten, die es dem Betreiber ermöglichen, sich selbst einen Überblick über den Maschinenzustand zu verschaffen, damit er schneller auf Abweichungen reagieren kann. Das sollte dann von überall her möglich sein, so wie ein Smart-Home-Besitzer per App aus der Ferne den Zustand seiner technischen Anlagen einsehen kann. Dabei sollte es zunächst genügen, dem Anlagenbetreiber und/oder dessen Mitarbeitern nur lesenden Zugriff zu gewähren. Mögliche weitere Schritte:

- Der Betreiber kann relevante Maschinendaten nur lokal abfragen, um Maschinenkennzahlen zu überwachen.
- Der Betreiber kann auf dieser Basis Benachrichtigungen oder gar Alarme bei Abweichungen von den Sollwerten versenden. Weil dabei die Maschinendaten innerhalb der Anlage verbleiben, ist noch keine aufwendige Anbindung an eine IIoT-Plattform notwendig.

Optimierter Service und das Zusammenrücken von Maschinenbauer, Anlagenbetreiber und Kunden bedeutet eine Erhöhung der Wettbewerbsfähigkeit von Maschinenbauer und Anlagenbetreiber und mehr Kundenzufriedenheit.

Umsetzen der Digitalisierung

In die Digitalisierung wächst der Anlagenbetreiber am besten nach und nach hinein. Daher ist es in der Regel sinnvoll, zunächst kleine Pilotprojekte aufzusetzen und diese dann Schritt für Schritt um weitere Bereiche zu erweitern. Dies wird nur dann gelingen, wenn der Maschinenbauer hier mitgeht, also die Herausforderung annimmt, sich entsprechend zu wandeln. Denn er hat nun die Chance, sich über seine traditionelle Rolle des Trouble-Shooters, der nur bei Problemen gerufen wird, zu erheben, indem er bereit und in der Lage ist, auch per Ferndiagnose hilfreich zu sein. Gelingt ihm dies, steigt seine Bedeutung, da für den Anlagenbetreiber nun Zeitverzögerungen kein Thema mehr sind. Der Maschinenbauer kann weiter auch die Prozessoptimierung unterstützen. Die Digitalisierung ermöglicht also eine optimale Kompetenznutzung, was den Anlagenbetreiber entlastet und dem Maschinenbauer einen höheren Stellenwert verschafft.

Der wichtigste Vorteil einer schrittweise für die ganze Anlage umgesetzten Digitalisierung besteht darin, dass sich unvorhergesehene Anlagenstillstände deutlich reduzieren lassen. Das spart nicht nur Kosten, sondern steigert auch die Produktivität. Ein weiterer Vorteil: Es ist nun möglich, gewisse Aufgaben komplett auszulagern, sodass Instandhalter einfach fokussierter arbeiten können.

Man sieht: Im Zuge des schrittweise umgesetzten Digitalisierungsprozesses verschieben sich die Aufgabenfelder von Maschinenbauer und Anlagenbetreiber mehr oder weniger zum Vorteil alle Beteiligten.

Mögliche Hürden seien nicht verschwiegen: So verursachen die Verwaltung und der Betrieb einer Vielzahl an verschiedenen vernetzten Geräten u.U. einen hohen Aufwand und benötigen viel Zeit. Und die Soft- und Firmware der Geräte ist aus Sicherheitsgründen stets auf dem neusten Stand zu halten. Die Verarbeitung, Absicherung und Speicherung der Daten kann Sicherheitslücken öffnen; diese sind zeitnah zu schließen. Einfaches Patchen der Software kann in einigen Bereichen nicht ausreichen. Etwa verschiedene eingesetzte Protokolle können verhindern, dass IIoT-Geräte verschiedener Hersteller miteinander kompatibel sind.

▶ *FS*