SIEMENS

Industrial Communication

Cloud Connectivity für die Fabrikhalle:

Die notwendigen Schritte und Überlegungen zur Umsetzung

White Paper

Ausgabe 10/2019

siemens.de/cloudconnect

Inhaltsverzeichnis

Einleitung 2

Erste Schritte mit der Cloud 3

MQTT Überblick 5

Das Problem der Semantik 6

Die Grenzen der Cloud-Lösungen 7

Generationenkonflikt: Industrie 4.0 mit Technik 0.4 8

Die richtige Auswahl des industrial IoT Gateways 9

Einleitung

Cloudbasierte Lösungen finden bereits vielfältigen Einsatz in Fabrikhallen und in der Automatisierung. Die Anwendungsmöglichkeiten sind dabei sehr unterschiedlich: Von der Qualitätskontrolle der Erzeugnisse über Instandhaltung der dafür notwendigen Maschinen bis hin zur Fertigung von personalisierten Produkten, die der Kunde selbst gestaltet hat. Die Grundlage all dieser Anwendungen ist die Bereitstellung der Daten aus der Feldebene an cloudbasierte Server. In der Praxis besteht die Herausforderung hierbei ein möglichst reibungsloses Zusammenspiel der IT geprägten Cloud Services mit den klassisch OT (Operational Technology) geprägten Feldgeräten zu gewährleisten. Das White Paper behandelt die ersten Schritte die notwendig sind, um das Automatisierungsnetzwerk an die Cloud anzubinden.

Erste Schritte mit der Cloud

Der Begriff „Cloud" ist ein sehr unterschiedlich eingesetzter Begriff und bleibt ohne weitere Erklärung häufig ziemlich abstrakt. Ein etwas konkreteres Bild bekommt man meist erst wenn man die Angebote von Cloud-Providern studiert und die verfügbaren Dienste auch testweise benutzt. Erstaunlicher Weise sind die ersten Schritte dabei recht simpel. Häufig können Testaccounts online für einen begrenzten Zeitraum oder mit eingeschränktem Funktionsumfang schnell erstellt werden. Danach bekommt man eine Übersicht aller möglichen Dienste, die dann gegen entsprechende Gebühren gebucht werden können. Beispielhafte Kategorien für solche Dienste sind:

Cloud Service Kategorie	Beschreibung	Beispiel Dienste
Speicher	Online Speicherplatz zur Datenablage	Backup Sicherungen, Archivspeicher
Netzwerk	Dienste die für den Betrieb eines Netzwerkes notwendig sind	DNS Server, VPN Gateway, Webserver
Rechenleistung	Rechenleistung auf Virtuelle Maschinen auslagern	Virtual Machine Umgebungen
Internet of Things (IoT)	Vernetzung und Verwaltung von externen Datengebern	MQTT Broker, Streaming Analyse

Die Menge der Dienste wächst rasant und lässt einen schnell den Überblick verlieren. Je nach Branche und/oder Anwendung ist auch meistens nur ein Bruchteil dieser Dienste tatsächlich interessant für den Kunden.

Im Normalfall hat jeder einzelne Dienst wiederum ein variables Preismodell, welches von der Konfiguration des Dienstes selbst abhängt.

Wenn die konkrete Aufgabenstellung nun darin besteht, Daten aus dem Automatisierungsnetz in die Cloud zu schieben, um diese dort zu analysieren oder zu visualisieren, dann sind in erster Linie die Dienste aus der Kategorie „IoT" notwendig. Der erste Schritt ist dann einen Schnittstellendienst anzulegen und an dieser Schnittstelle Zugangspunkte einzurichten, die von den Feldgeräten genutzt werden können.

In den meisten Fällen wird dafür ein MQTT Broker instanziiert und Benutzergeräte angelegt, die dorthin publishen dürfen (siehe auch **„MQTT Überblick"**). Der Broker wird dann in einem (wählbaren) Rechenzentrum des Cloud-Anbieters gehostet und ist unter einer personalisierten URL erreichbar.

Die Kosten eines solchen Dienstes richten sich im Normalfall nach der Anzahl der „Messages", die (von Feldgeräten) in einem bestimmten Zeitraum an den Broker geschickt werden können. Zum Beispiel: 5000 Messages / Tag für monatliche Kosten in Höhe von 4,99 €.

Erste Schritte mit der Cloud

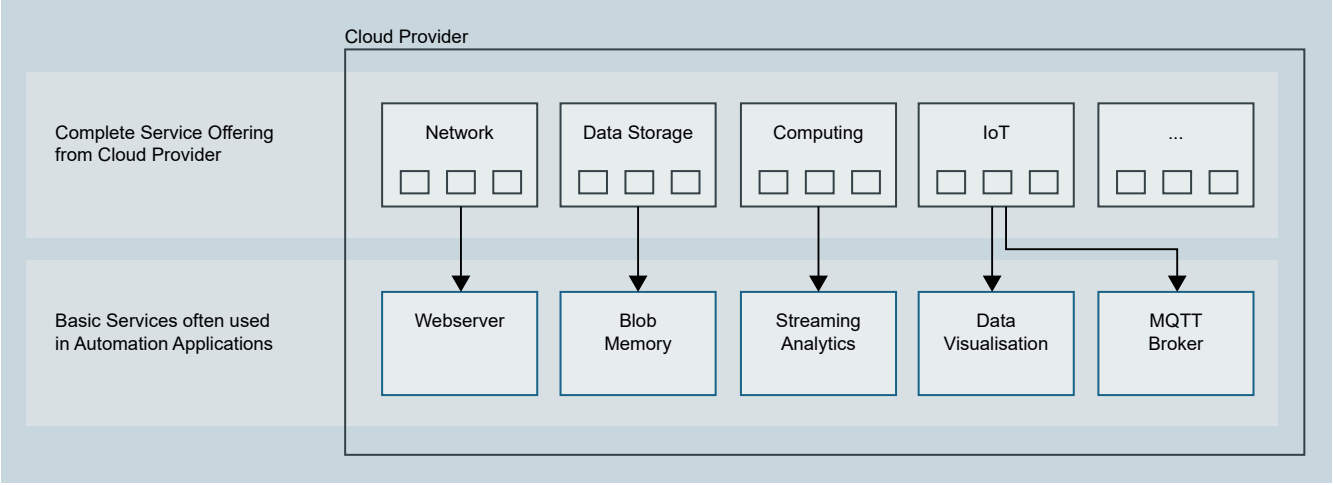
Nun ist es für MQTT-fähige Endgeräte möglich Daten an diesen Broker zu schicken bzw. von dort zu holen.

Die Umsetzung der tatsächlichen Cloud-Anwendung fängt aber jetzt erst an. Nun können weitere Dienste gebucht werden, die die Daten des Brokers (und damit der Feldgeräte) analysieren, filtern oder visualisieren. Zum Beispiel könnte nun ein Dienst zur Datenanalyse verwendet werden, der die Daten des Brokers untersucht und auf bestimmte Werte filtert. Dieses Ergebnis wiederum kann dann einer Visualisierung zugeführt werden, die auf einem (beim Cloud-Anbieter gehosteten) Webserver läuft und für den Kunden mit seinem Smartphone erreichbar ist.

So könnte man also den Anlagenzustand für den Servicemitarbeiter jederzeit verfügbar machen ohne eigene Infrastruktur aufzubauen.

Man erkennt jedoch auch, dass selbst dieser einfache Fall schon ein komplexes Zusammenspiel von mindestens 5 Diensten eines Cloud-Anbieters notwendig macht. (MQTT Broker, Datenanalyse, Visualisierung, Speicher, Webserver).

Da die Anbindung von Automatisierungsgeräten an einen MQTT Broker eine zentrale Rolle spielt, sind zur Umsetzung der industriellen Cloud-Anwendungen detaillierte Kenntnisse zum MQTT Protokoll notwendig.



IIoT spezifische Services der Cloud Provider

MQTT Überblick

MQTT steht für „Message Queuing Telemetry Transport“ und ist ein Kommunikationsprotokoll, welches ursprünglich 1999 von IBM Mitarbeitern erdacht wurde mit dem Ziel möglichst effizient über relativ instabile und wenig performante Netzwerke Daten auszutauschen. In den letzten Jahren hat das Protokoll jedoch sehr erfolgreich seinen Weg in IoT-Anwendungen gefunden und verdrängt dort weitestgehend alle anderen Protokolle. Die Spezifikation wird aktuell vom Konsortium OASIS (Organization for the Advancement of Structured Information Standards) weiterentwickelt und ist frei verfügbar.

Das MQTT-Protokoll arbeitet nach einem Publish-Subscribe (Pub/Sub)-Prinzip zum Datenaustausch zwischen beliebig vielen Teilnehmern. Dabei gibt es eine zentrale Instanz, den sogenannten „Broker“, der alle zirkulierenden Daten verwaltet und verteilt. Ein Teilnehmer, der Informationen teilen möchte tut dies, indem er seine Daten an den Broker „published“. Ein Teilnehmer, der sich für Daten interessiert kann sich beim Broker „subscriben“ und erhält vom Broker die Daten, für die er sich interessiert. Dabei können sich theoretisch beliebig viele Geräte als Publisher und Subscriber beim Broker melden. Ein Teilnehmer kann auch gleichzeitig Publisher und Subscriber sein.

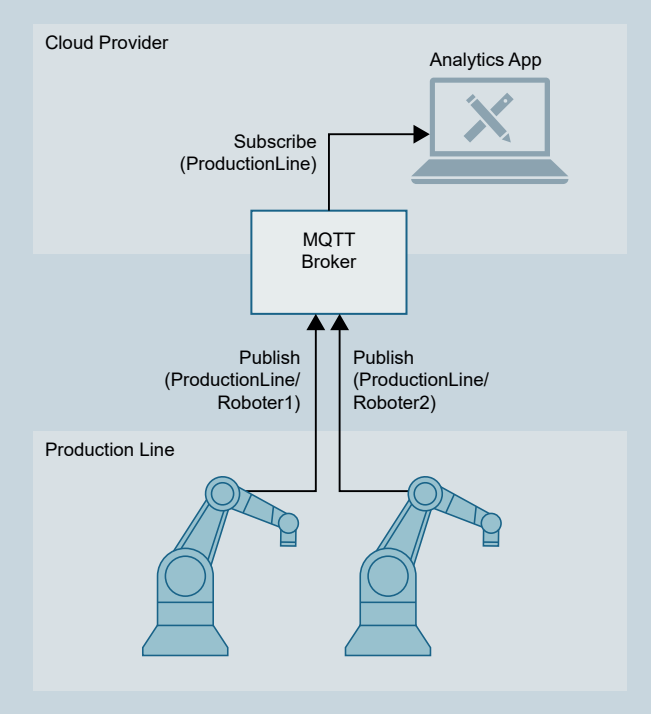
Der größte Vorteil besteht nun darin, dass keine Punkt-zu-Punkt-Verbindungen mehr notwendig sind und sich damit die Teilnehmer auf eine positive Art entkoppeln und die Komplexität reduziert wird. Dieses Konzept bietet neue „Freiheiten“, die sich hauptsächlich wie folgt auswirken:

Teilnehmer-Unabhängigkeit:
Ein Sender von Daten (Publisher) hat keine Kenntnis über die Endempfänger (Subscriber) und umgekehrt. Klassische Teilnehmeradressen und deren Verwaltung entfallen auf dieser Ebene also.

Zeitliche-Unabhängigkeit:
Ein Senden und Empfangen von Daten kann zu beliebigen- und vor allem unterschiedlichen Zeiten erfolgen. Einem Publisher ist es egal ob die Subscriber sich jetzt im Moment für die Daten interessieren oder ob diese gerade ausgeschaltet sind und deshalb erst später die Daten verwerten.

Durch diese 2 Eigenschaften bekommen Pub/Sub-System eine enorme Skalierbarkeit. Neue Teilnehmer können sich ohne große Aufwände in das Netzwerk einbinden oder abmelden ohne dass die anderen etwas davon mitbekommen. Genau dies ist eine der Hauptanforderungen bei industriellen IoT Anwendungen. Ein weiterer Vorteil ist der minimale Footprint eines MQTT Stacks. Mit einer Größe von wenigen Kilobyte kann dieser problemlos auf sehr vielen Geräten intergiert werden.

Damit der Broker weiß, welche Daten für wen interessant sind, werden sogenannte „Topics“ verwendet. Ein Topic ist im Grunde ein Thema oder eine Art Ordner, zu dem spezifische Daten abgelegt werden. Das Topic kann auch verschachtelt werden, um das Thema genauer einzuschränken. Als einfachstes Beispiel kann man einen Temperatursensor nehmen, der seinen Messwert bereitstellen möchte. Dazu würde er seine Daten auf dem Topic „Temperatur“ publishen. Da die Anwendung im Normalfall mehrere solcher Sensoren hat spezifiziert man dies nun noch etwas genauer, indem er auf das Topic „Temperatur/Halle_1“ published. Jeder Teilnehmer, der sich nun für diese Wert interessiert, subscribed sich auf das Topic „Temperatur/Halle_1“ und wird damit jedes Mal vom Broker mit den neuen Daten versorgt, wenn auf diesem Topic etwas gepublished wird.



Publish Subscriber Konzept von MQTT

Neben den vielen Vorteilen, die MQTT bietet, gibt es aus Anwendungssicht in der Industrie auch einen großen Nachteil: Die Nutzdaten (Payload) von MQTT sind ein beliebiger String und unterliegen keinen zusätzlichen Vorschriften zum Inhalt bzw. Semantik der enthaltenden Daten (Datenagnostisch).

Das Problem der Semantik

Bei der Übertragung von Daten kommt es immer relativ schnell zu der Frage auf welches Datenformat und Inhalte sich der Empfänger und Sender von Informationen einigen können, damit Sie kompatibel sind. Mit der Einführung von Cloud-Systemen hat sich diese Fragestellung noch weiter verschärft: Die Bereitsteller der Daten (im Fall der Automatisierungstechnik die Fabrikgeräte oder Maschinen) sind häufiger unabhängig von den Applikationen, die diese Daten verwerten. Umso wichtiger wäre es eigentlich ein festes Format vorzugeben, auf dass sich alle einigen können. Fakt ist aber, das bei Cloud-Systemen genau solches Format nicht existiert, und es auch fraglich ist, ob es dies jemals geben wird. Dafür gibt es mehrere Gründe. Zum einen liegt es daran, dass die Cloud-Anbieter eine riesige Menge an unterschiedlichen Kundengruppen haben: Die Cloud-Lösungen sollen von IT-Abteilungen, Maschinenbauern, Finanzdienstleistern, Marketingabteilungen und vielen mehr genutzt werden. Also muss die Plattform möglichst flexibel sein. Vereinheitlichte Datenformate sind aber immer eine Einschränkung, und deshalb hadern die Anbieter mit branchenspezifischen Detaillösungen bzgl. Datenformaten.

Für die Automatisierungstechnik stellt sich das Problem im Detail wie folgt dar: Die Informationen der Anlage liegen in den meisten Fällen in Form von Programmvariablen in einer Steuerung. Diese Variablen sind Abbilder von aktuellen Prozesswerten in bestimmten Datentypen wie zum Bsp. die Typen Real, Int oder Bool. Im einfachsten Fall, bei welchem so ein Prozesswert zyklisch übertragen werden soll an einen Cloud Server, müssen mindestens 3 Informationen in den Payload String von MQTT codiert werden:

1. Der aktuelle Prozesswert der Variablen
2. Der Typ der Variablen, damit der Empfänger diese interpretieren kann
3. Ein Zeitstempel wann dieser Wert gültig war, damit weiterverarbeitende Anwendungen Zeitreihen bilden können

Zusätzlich zu diesen 3, sind weitere Informationen wie z. B. ein QualityCode optional hinzuzufügen. Um die Anwendung zu vereinfachen werden in Normallfall auch eigene Strukturen verwendet, die den Zustand einer ganzen Maschine repräsentieren. Auch das muss wieder in die Payload von MQTT codiert werden.

Da hier kein einheitlicher Standard existiert ist es in der Praxis nun so, dass es quasi für jede Anwendung ein eigenes Format gibt, und damit auch eigene Parser dort notwendig werden, wo die Daten verwendet werden sollen.

Diese Tatsache ist aus Sicht der klassischen Automatisierungstechnik ein Rückschritt. In Zeiten von OPC UA und dazugehörige Companion Specifications, die die Interoperabilität verschiedener Geräte und Hersteller gewährleisten, stellt sich die MQTT-Schnittstelle eines Cloud-Anbieters als dysfunktional dar. Hier muss unnötige Arbeit in die Datenaufbereitung gesteckt werden.

Eine erste praktische Vereinfachung ist hier die Verwendung des Formates JSON, mit dem einige Regeln zu Datendarstellung zur Verfügung stehen, die das Lesen und Parsen des MQTT Payload String etwas einfacher machen. Das vereinfacht zwar das Parsing, aber ersetzt es nicht.

Um hier zu einer zufriedenstellenden Lösung zu kommen, müssen die Cloud-Anbieter und Automatisierungstechniker noch näher zusammenrücken und die zukünftigen Schnittstellen gemeinsam gestalten.

```
{
  "Timestamp":"2019.08.01 15:42:23",
  "DataItems":
  [
    {
      "Variable":"Temperature",
      "Type":"Real",
      "Value":"20°C",
      "QualityCode":"1"
    },
    {
      "Variable":"Overheat",
      "Type":"bool",
      "Value":"true",
      "QualityCode":"1"
    }
  ]

}
```

Beispiel MQTT Payload von 2 Prozesswerten im JSON Format

Die Grenzen der Cloud-Lösungen

Auch wenn aktuell eine neue Anwendung nach der anderen entsteht, die erst durch Cloud-basierte Ansätze möglich wurden: Im Zusammenspiel mit der Automatisierungswelt gibt es auch aktuell noch Grenzen über die man sich am besten schon im vornherein Gedanken macht, damit man im Nachhinein keine Überraschung erlebt.

In der klassischen Automatisierungstechnik liegt der Fokus bei der Datenübertragung seit jeher auf einem schnellen, zyklischen Austausch von relativ kleinen Datenmengen. Das fängt an mit digitalen oder analogen Eingängen, bei denen sehr simple Informationen wie „An" oder „Aus" im einstelligem Microsekundenbereich übermittelt werden. Danach folgen die Feldbusse wie PROFINET oder PROFIBUS mit deren Hilfe Prozessdaten mit gesicherten Übertragungszyklen in wenigen Millisekunden übertragen werden. Selbst die Ablaufprogramme in den Steuerungen, welche teilweise komplexe Algorithmen und Regelungen ausführen, haben Zykluszeiten im Millisekunden Bereich.

Bei der Übertragung dieser Daten aus dem Automatisierungsnetz in die Cloud ändern sich jedoch die Begebenheiten. Als erstes müssen die Daten mit zusätzlichen Informationen wie Zeitstempel und Datentypen (siehe auch **„Das Problem der Semantik"**) angereichert werden.

Zusätzlich ändern sich die Kommunikationsprotokolle hin zu den IT-typischen TCP/IP Stacks und Publish/Subscriber-Mechanismen, die weiteren Protokolloverhead hinzufügen und damit das Datenvolumen vergrößern. Da diese Protokolle auch keine gesicherten Zykluszeiten oder reservierte Bandbreiten garantieren, erhöhen sich die effektiven Zeiten, die benötigt werden um die tatsächlichen Nutzdaten von A nach B zu übertragen.

Es entsteht also eine Art Flaschenhals beim Übergang vom Automatisierungsnetz in die Cloud. Diesen gilt es zu beachten, wenn über mögliche Anwendungen in der Cloud diskutiert wird.

Ein klassisches Beispiel, bei dem man ganz sicher auf Grenzen stoßen wird, ist die Idee Verfahrwege von Fräsmaschinen in Echtzeit im Cloudserver zu analysieren. Der Prozess des Fräsens ist viel zu schnell, als das die dabei anfallenden Hochfrequenzdaten schnell genug in die Cloud übertragen werden könnten.

Genau aus diesem Grund wird von vielen Herstellern das Thema „Edge" - also die dezentrale Datenvorverarbeitung sehr nah am Prozess selbst – energisch vorangetrieben.

Trotz dieser Grenzen bleiben die Anwendungsfälle sehr vielfältig. Ein sekundengenaues Abrechnen der Nutzungsdauer der Fräsmaschine zum Beispiel ist problemlos möglich und ermöglicht dem Maschinenbauer das häufig angepriesene neue Geschäftsmodell.

Generationenkonflikt: Industrie 4.0 mit Technik 0.4

Auch wenn die Anzahl der Cloud-Anbieter und die dabei verfügbaren Dienste in den letzten Jahren einen enormen Sprung gemacht haben: In der Automatisierungstechnik bewegen sich sowohl die Investitionszyklen als auch die Innovationszyklen eher im Zehn-Jahres Zyklus. Die Gründe hierfür sind banal und einleuchtend: Änderungen kosten erstmal viel Aufwand und kommen immer mit vermeintlichen Problemen, die gegebenenfalls die Produktion und damit das gesamte Geschäft gefährden können.

Das führt in vielen Fällen nun zu einem konkreten Konflikt: Nachdem das Unternehmens-Management beschlossen hat im Rahmen seiner Industrie 4.0 Strategie auch alle Werke und Maschinen an das nun neue Cloud-System anzuschließen, muss sich der Produktionstechniker die Frage stellen, wie er seinen „Technik 0.4" Bestand mit 10-20 Jahre alten Geräten an dieses Cloud-System anbindet. Eine MQTT Schnittstelle haben diese Geräte sicherlich nicht. In vielen Fällen sind die notwendigen Daten auch in PROFIBUS- oder seriellen Netzwerken, die man schon rein physikalisch nicht direkt an IP-Netze anbinden kann.

Zusätzlich haben die Automatisierungsgeräte eine komplexe Projektierung und Programmierung, die nicht ohne Weiteres geändert werden kann. Das sind Aufwendungen, die von Ingenieuren gemacht werden müssen. Auch Extremfälle, in denen Geräte im Einsatz sind, deren Projektierung vor 20 Jahren gemacht wurde und heute aufgrund der fehlenden Dateien, Tools oder Know How Träger gar nicht mehr geändert werden können ist nicht so selten wie man anzunehmen vermag.

Eine installierte Basis an ein neues Cloud-System anzubinden erfordert also Aufwände, die in jeder Industrie 4.0 Strategie Berücksichtigung finden müssen, damit der Mehrwert korrekt kalkuliert werden kann.

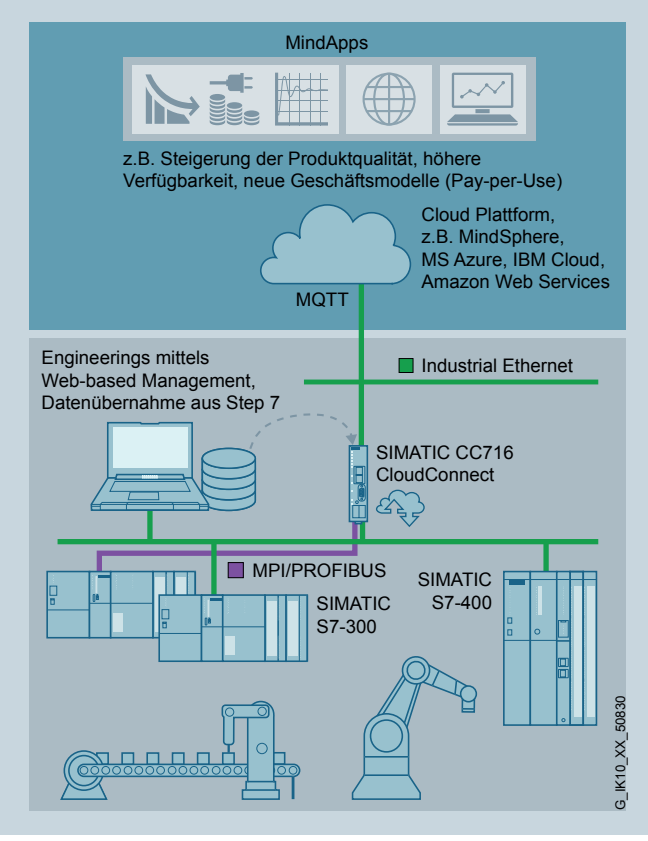
Zur Minimierung dieser Aufwände bieten viele Hersteller spezielle Geräte an, mit denen die Anbindung an die Cloud vereinfacht wird. In den meisten Fällen wird sich der Einsatz solcher Industrial IoT Gateways lohnen, jedoch gibt es die Geräte in sehr unterschiedlichsten Ausprägungen und variablen Funktionsumfang. Daher ist ein technischer Vergleich und Tests solcher Gateways im Vorfeld sehr zu empfehlen, damit der spätere Einsatz möglichst reibungslos funktioniert und für die Anwendung passt.

Die richtige Auswahl des Industrial IoT Gateways

Immer dann, wenn Geräte oder Maschinen, die keine native MQTT-Schnittstelle besitzen an einen Cloud-Service angebunden werden sollen, ist ein Industrial IoT Gateway notwendig.

Das Gateway übernimmt dabei folgende Grundfunktionen:

1. Aufnahme der Daten aus dem Automatisierungsnetz
2. Filterung von Inhalten und Umwandlung der Datenformate
3. Übertragung der Daten an die Cloud Schnittstelle



Anlagenkonfiguration mit IoT Gateway am Beispiel Siemens

Industrial IoT Gateways gibt es in verschiedensten Variationen von sehr unterschiedlichen Anbietern. Daher gibt es auch sehr große Varianz selbst bei den grundlegendsten Funktionen.

Folgende Überlegungen sollten bei der Auswahl des richtigen Industrial IoT Gateways eine Rolle spielen:

1. **Ist es ein Produkt oder eine Sandbox?**
   Als erstes sollte man ganz klar zwischen industriellen Produkten und offenen Sandbox-Systemen unterscheiden. Ein Industrial IoT Gateway kommt in einem Gehäuse und Montagemöglichkeiten, die speziell für den Schaltschrank und die entsprechenden Umgebungsbedingungen entworfen sind. Sandbox-Lösungen sind meist Raspberry Pi ähnliche Platinen mit einem passenden Gehäuse darum. Solche Lösungen kommen meist mit einer Entwicklungsumgebung, die es ermöglicht sehr flexibel eigene Programme zu entwickeln oder Open Source Anwendungen laufen zu lassen. Industrielle Geräte kommen hingegen mit einem festgelegtem Funktionsumfang, der über eine spezielle dafür angelegte Konfigurationsmöglichkeit (meistens Webserver) projektiert wird.
   Je nach Anwendung kann die Eine oder Andere Lösung besser passen. Wenn der Fokus im speziellen darauf liegt mit möglichst wenig Zusatzaufwand die Anwendung nach einem festen Schema umzusetzen, bietet sich ein industrielles Produkt an.

2. **Welche Schnittstellen in die Feldebene werden geboten?**
   Welche Feldgeräte wie zum Bsp. Steuerungen, Motoren, Sensoren angebunden werden können wird ein weiteres Hauptkriterium sein. Hier sollte man sich im ersten Schritt eine Liste aller Geräte erstellen, von welchen Daten in die Cloud geschickt werden sollen. Jedes dieser Geräte unterstützt spezielle Protokolle wie Modbus, S7 oder PROFBUS. Das Industrial IoT Gateway sollte also von Haus aus diese Protokolle ebenfalls unterstützen, damit keine Änderungen an den Feldgeräten vorgenommen werden müssen.

Die richtige Auswahl des Industrial IoT Gateways

3. **Ist die Cloud-Schnittstelle flexibel genug?**
   Nachdem die Anbindungsmöglichkeiten der Feldgeräte geklärt ist, sollte das Augenmerk auf die zu unterstützten Cloud-Anbieter gelegt werden. Die meisten Cloud-Anbieter unterstützen zwar MQTT Standard, jedoch kann es zu einigen spezifischen Einschränkungen kommen. In einigen Lösungen sind die Topic Namen und Formate (siehe **„MQTT Überblick"**) fest vorgegeben. Das IIoT Gateway sollte diese beherrschen können, man sollte also entweder darauf achten, dass die unterstützten Cloud-Systeme explizit in den Produkteigenschaften erwähnt sind oder das Gerät flexibel genug ist über die Konfiguration eine jeweilige Anpassung vornehmen zu können.
   Des Weiteren ist in vielen Anwendungsfällen eine zusätzliche Anforderung wichtig: Neben dem neuem Cloud-Server läuft parallel häufig auch noch das bisherige MES-System (Manufacturing Execution System) weiter. Auch hier werden gegebenenfalls neue Prozesswerte benötigt. Also sollte das IIoT Gateway auch in der Lage sein zusätzlich die Daten an ein MES-System zum Beispiel über ein OPC UA Interface bereitzustellen.

4. **Wie viele Geräte und Datenpunkte werden tatsächlich benötigt?**
   Die Frage nach dem Mengengerüst der notwendigen Daten ist wohl eine der häufigsten Punkte, die im Rahmen der Erstellung einer Industrie 4.0 Strategie zu lange unbeantwortet bleibt. Eine konkrete Frage hierzu wäre zum Beispiel: „Wie viele Prozesswerte werden aus einer Fertigungszelle benötigt?". Diese Frage muss im Vorfeld grob beantwortet werden, da ansonsten die Umsetzung in eine Sackgasse führen kann. Aus diesem Grund sind auch bei den IIoT Gateways auf die Angabe der Mengengerüste (Wie viele Datenpunkte werden pro Gerät unterstützt) in den technischen Daten zu achten. Wenn hierzu zum Produkt keine Angaben vorliegen, muss davon ausgegangen werden, dass keine Performance Tests vom Hersteller gemacht wurden. Dies würde ein erhöhtes Risiko für der Umsetzung darstellen, welches im Vorfeld ausgeschlossen werden sollte.

5. **Sonstige Punkte:**
   a. Getrennte Netze
      Aus Sicherheitsgründen ist darauf zu achten, dass das Gateway in 2 komplett unterschiedlichen Subnetzen (1 x Cloud, 1x Automatisierungsnetz) arbeiten kann und auch ein entsprechendes Routing dazwischen ausgeschlossen ist.

   b. Unterstützung von digitalen oder analogen Inputs bzw. Outputs
      In Industrieanwendungen werden immer wieder IOs benötigt um den Prozess, wenn notwendig zu beeinflussen. Der einfachste Fall wäre zum Beispiel die Datenübertragung an die Cloud per Schalter hart zu beenden, weil ein Sicherheitsrisiko besteht.

   c. Einfacher Gerätetausch
      Ein schneller und einfacher Gerätetausch sollte möglich sein, um im Austauschfall den Produktionsprozess nicht unnötig aufzuhalten. Hierzu bietet sich die Übertragung der Gerätekonfiguration über USB Speicher in ein neues Gerät als sinnvolle Möglichkeit an, auf die geachtet werden sollte.

   d. Zeitsynchronisation
      Da alle Prozesswerte mit einem Zeitstempel versehen werden müssen (siehe: Das Problem der Semantik) muss das Gateway über eine Möglichkeit verfügen die Zeit von einem Server synchronisiert zu bekommen. Eine manuelle Zeiteinstellung am Gerät ist für die Inbetriebnahme zwar sinnvoll, jedoch für einen laufenden Prozess nicht ausreichend. Hier muss eine automatisierte Synchronisierung (zum Bsp. über NTP) angeboten werden, um im Falle einer Stromunterbrechung keine verfälschten Zeitwerte zu bekommen.

Siemens AG
Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

PDF
BR 1019 11 De
Produced in Germany

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter **https://www.siemens.com/industrialsecurity.**

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter **https://www.siemens.com/industrialsecurity.**