SIEMENS

Fachartikel

Automatisierungsdaten für die Cloud

Kommunikationsarchitekturen im Industrial Internet of Things

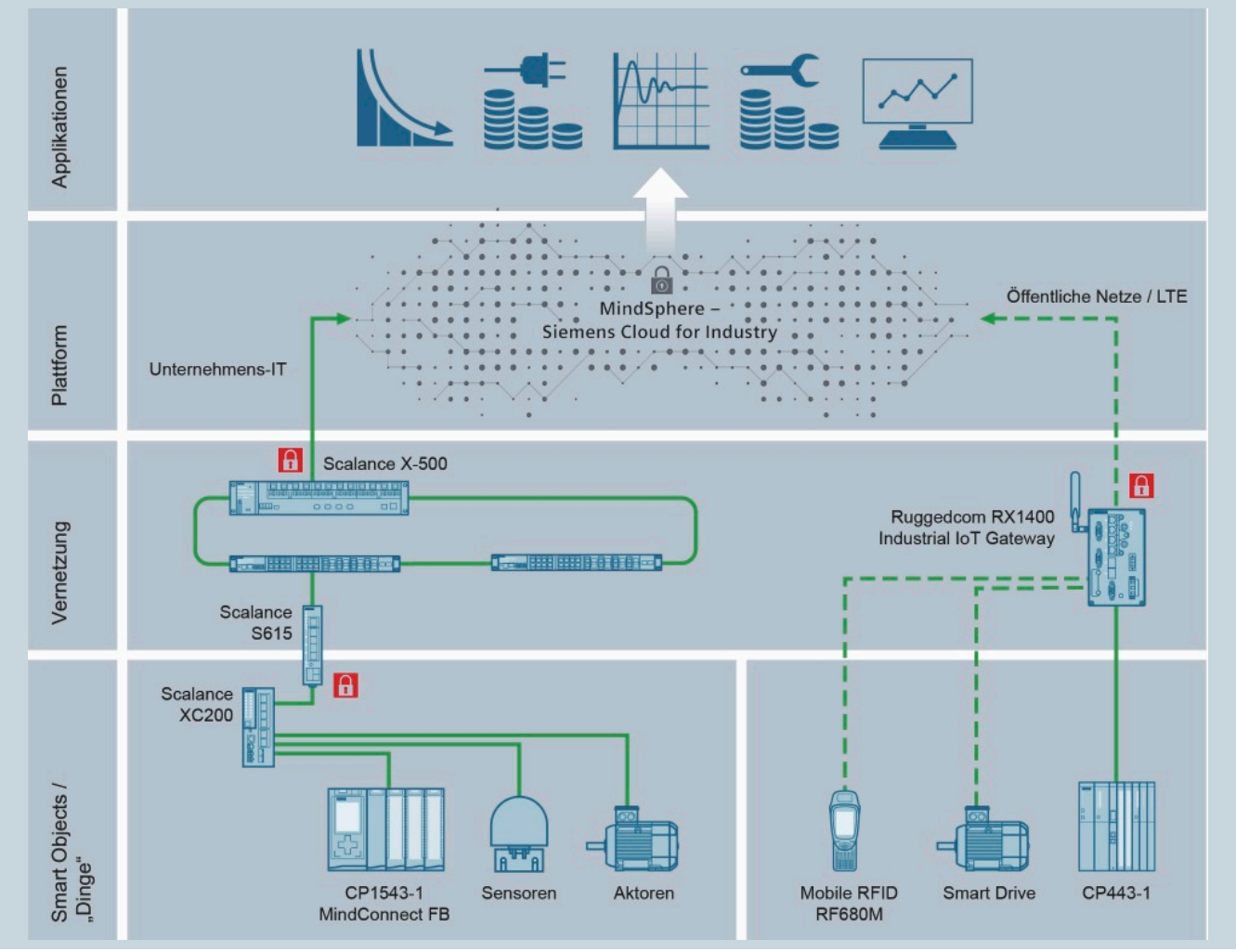
Cloud-Computing und das Internet der Dinge versprechen interessante Möglichkeiten – von der Prozessgestaltung bis zu neuen Geschäftsmodellen – auch für Industrieunternehmen. Voraussetzung ist eine ausreichend breite Datenbasis, die aus der Feldebene in die Cloud übertragen wird. Doch hierfür braucht es eine leistungsfähige, sichere und flexible Kommunikations-Architektur.

Die Idee ist also, die Sensoren der Feldebene, die zum Beispiel Temperaturverläufe, Vibrationen und Stromaufnahme einer Maschine überwachen, als Grundlage für Big-Data-Algorithmen an die virtuelle Auswerteplattform – die Cloud – zu übertragen. Doch eine direkte Konnektivität der Sensoren über Intra- und Internet an die Cloud erscheint in der Praxis eher schwierig. Viele Sensoren sind heute noch nicht einmal ethernetfähig, sondern transportieren die Messwerte über eine Stromschnittstelle (4...20 mA) an eine speicherprogrammierbare Steuerung (SPS). Moderne Sensoren bieten zum Beispiel eine IO-Link-Schnittstelle, die aber auch nicht cloudfähig ist, sondern erst durch ein Master-Modul und ein Gateway in die entsprechenden Protokolle inklusive der Routing-Fähigkeit übersetzt werden muss. Selbst wenn die Sensorik die benötigten Ethernet-Schnittstellen und -Protokolle mitbrächte, so wären tausende von Internet-Verbindungen aus dem Feld in die Cloud für die IT-Administratoren kaum zu kontrollieren – ganz zu schweigen von den Unmengen an Daten, die ohne klaren Business Case in der Cloud verarbeitet werden müssten.

Sinnvoller ist es deshalb, eine Aggregationseinheit in der Control-Ebene vorzusehen, die zum einen eine Verdichtung von Daten vornimmt, zum anderen die Informationen einer Vielzahl von Sensoren bündelt. Aus Automatisierungssicht kann diese Aufgabe ideal die SPS vornehmen, da dort die meisten Sensordaten sowieso auflaufen, zum Beispiel zur Maschinenüberwachung. Zudem führt die SPS bereits eigene Verdichtungen durch, zum Beispiel durch die logische oder rechnerische Verknüpfung der Daten.

Um die Kommunikation von der SPS zur Cloud zu realisieren, gibt es im Prinzip zwei Ansätze mit spezifischen Vorteilen. Zum einen können IoT-Gateways eingesetzt werden. Diese Geräte verfügen über zwei logische Einheiten zur Datenakquisition und zur Kommunikation in die Cloud. Der Akquisitionsteil dient zur zyklischen Abfrage der zu übertragenden Daten aus der Feldebene, vor allem aus der SPS. Dazu bietet das Industrial IoT Gateway Ruggedcom RX1400 von Siemens zum Beispiel das Simatic-S7-Protokoll an, das die Abfrage von Daten ohne vorhergehende Anpassung des Automatisierungsprogramms ermöglicht – die ideale Lösung für Bestandsanlagen. Für andere Gerätetypen unterstützt RX1400 auch OPC UA in der Feldebene; neben Ethernet können die Daten auch über WLAN transportiert werden. Zur Übertragung in die Cloud unterstützen die Gateways die unterschiedlichen Kommunikationsprotokolle, zum Beispiel zur Anbindung an MindSphere. Zudem sind Gateways mit Blick auf die Sicherheit der Kommunikationsnetze sinnvoll, da die Cloud-Anbindung über einen separaten Netzwerkpfad erfolgen kann.

Als Alternative können Steuerungen auch eine intrinsische Cloud-Konnektivität anbieten. Zwar muss dabei das Automatisierungsprojekt angepasst werden, doch die Möglichkeiten sind deutlich vielfältiger. So sind in der SPS auch Informationen zum Kontext der Cloud-Daten vorhanden, zum Beispiel ob eine Maschine im Anlauf, im normalen Betrieb oder im Standby arbeitet. Abgeleitet davon können dann unterschiedliche Daten übertragen werden, oder die Zykluszeit für die Übertragung wird dynamisch angepasst – enge Zeitraster beim Hochlauf, eine eher sporadische Statusmeldung im Standby-Betrieb. Dies hilft, die Kommunikationslast zu reduzieren und überschwemmt die Cloud nicht mit

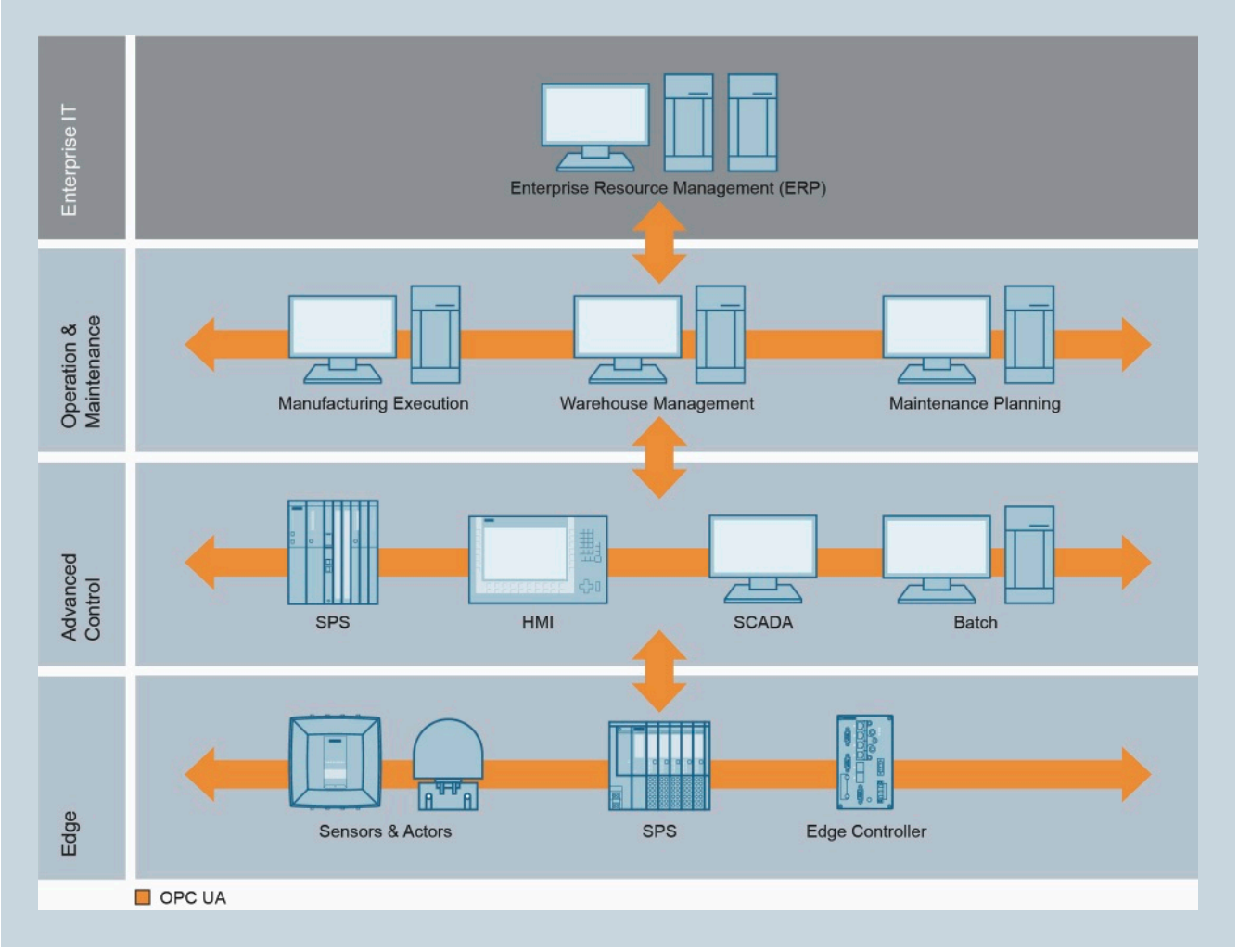


Mögliche Varianten zur Cloud-Anbindung: Mit MindConnect FB und CP1543-1 (links) oder einem Industrial IoT Gateway wie RX1400 (rechts)

irrelevantem Informationsrauschen. Aus diesen Gründen gibt es mit MindConnect FB die entsprechenden Kommunikationsbausteine zum Beispiel für die Steuerung Simatic S7-1500 und das Betriebssystem MindSphere, die im TIA-Portal projektiert und programmiert werden. Damit sind auch die Engineering-Daten für die Cloud-Anbindung automatisch in der Projektsicherung enthalten und können zum Beispiel auf weitere Steuerungen dupliziert werden – ein wichtiger Vorteil für Hersteller von Serienmaschinen.

Doch auch bei der intrinsischen Kommunikation ist die Sicherheit gegen Angriffe von höchster Bedeutung. Zwar bietet die Bibliothek MindConnect FB bereits eine verschlüsselte Übertragung der Daten. Doch für maximale Sicherheit empfiehlt sich der Einsatz eines getrennten Kommunikationsmoduls, wie dem CP 1543-1. Dieses Steckmodul für die Simatic S7-1500 koppelt die Cloud-Kommunikation vom Automatisierungsnetzwerk ab, da es eine separate Ethernet-Schnittstelle bereithält. Um Angriffe auf den CP abzuwehren ist eine Firewall in das Modul integriert. So können zum Beispiel Denial-of-Service-Attacken (DoS-Attacken) auf das Automatisierungsnetz abgewehrt werden.

Neben der reinen Kommunikationsarchitektur ist auch das Informationsdesign zu beachten, das heißt vereinfacht, die Protokolle in die Cloud. Aus der Perspektive eines Datenanalysten müssen geräte- oder herstellerabhängige Datenformate unbedingt verhindert werden, um aufwändige Normalisierungen in der Cloud zu vermeiden. Zudem ist es wichtig, auch den semantischen Kontext der SPS-Daten in die Cloud zu transportieren, das heißt den Bezeichner, den Datentyp und die Verortung im Objektmodell – nur so kann die Anbindung aufwandsarm und fehlersicher erfolgen. Dazu benötigt es aber eine gemeinsame Sprache im IIoT, die möglichst von allen Geräten in gleicher Weise unterstützt wird. Die Unified Architecture der OPC Foundation (OPC UA) bietet die besten Voraussetzungen hierfür.



OPC UA kann als gemeinsame Sprache alle Ebenen des IIoT integrieren.

OPC UA ist herstellerneutral, kann auf unterschiedlichen Hardware-Plattformen und Betriebssystemen implementiert werden, bietet umfangreiche Dienste – von der dynamischen Exploration der Schnittstelle eines Gerätes bis zu leistungsfähigen Sicherheitsfunktionen – und wird vor allem von einer breiten Allianz von Herstellern unterstützt.

Für den Erfolg von OPC UA entscheidend sind jedoch die branchen- und applikationsspezifischen Ergänzungsstandards, sogenannte Companion Specifications. Hier werden von Herstellerkonsortien oder Industrieverbänden gemeinsam mit der OPC Foundation spezifische Ausprägungen von OPC UA formuliert, um die unterschiedlichen Geräte bzw. Applikationen tatsächlich interoperabel zu gestalten. Beispiel: Der Hersteller eines Temperaturfühlers kann natürlich ein eigenes Objektmodell in den Sensor integrieren. Aber wie lautet der symbolische Name – „Temp“, „Temperature“, oder nur „t“? Wird der Wert in Grad Celsius, Grad Fahrenheit oder Kelvin ausgegeben? Handelt es sich um eine Ganzzahl oder um eine Fließkommazahl? Festlegungen dieser Art treffen die Companion Specifications, die OPC UA erst richtig IoT-fähig machen.

Ein Beispiel ist die Companion Specification für AutoID-Geräte (RFID oder optische Codes), die von Herstellern wie Siemens und Harting mit der OPC Foundation entwickelt wurde. Auf der Hannover-Messe 2017 konnte die OPC Foundation eindrücklich die Interoperabilität zwischen dem RFID-Leser Simatic RF600 von Siemens und dem Gerät eines anderen Herstellers nachweisen. Doch ist die Erarbeitung dieser ergänzenden Spezifikationen vergleichsweise aufwändig und braucht eine Gruppe von Herstellern, die gemeinsam die Arbeiten vorantreiben. Bis zu einer umfassenden OPC-UA-Modellierung für alle Geräte und Objekte einer Fabrik wird deshalb noch einige Zeit vergehen.

Securityhinweise

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 nur einen Bestandteil eines solchen Konzepts. Weitergehende Informationen über Industrial Security finden Sie unter **http://www.siemens.com/industrialsecurity**

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Deutschland

PDF
Fachartikel
FAV-295-2017-PD-PA-V01
BR 1017 / 4 De
Produced in Germany

siemens.de/industrielle-netzwerke