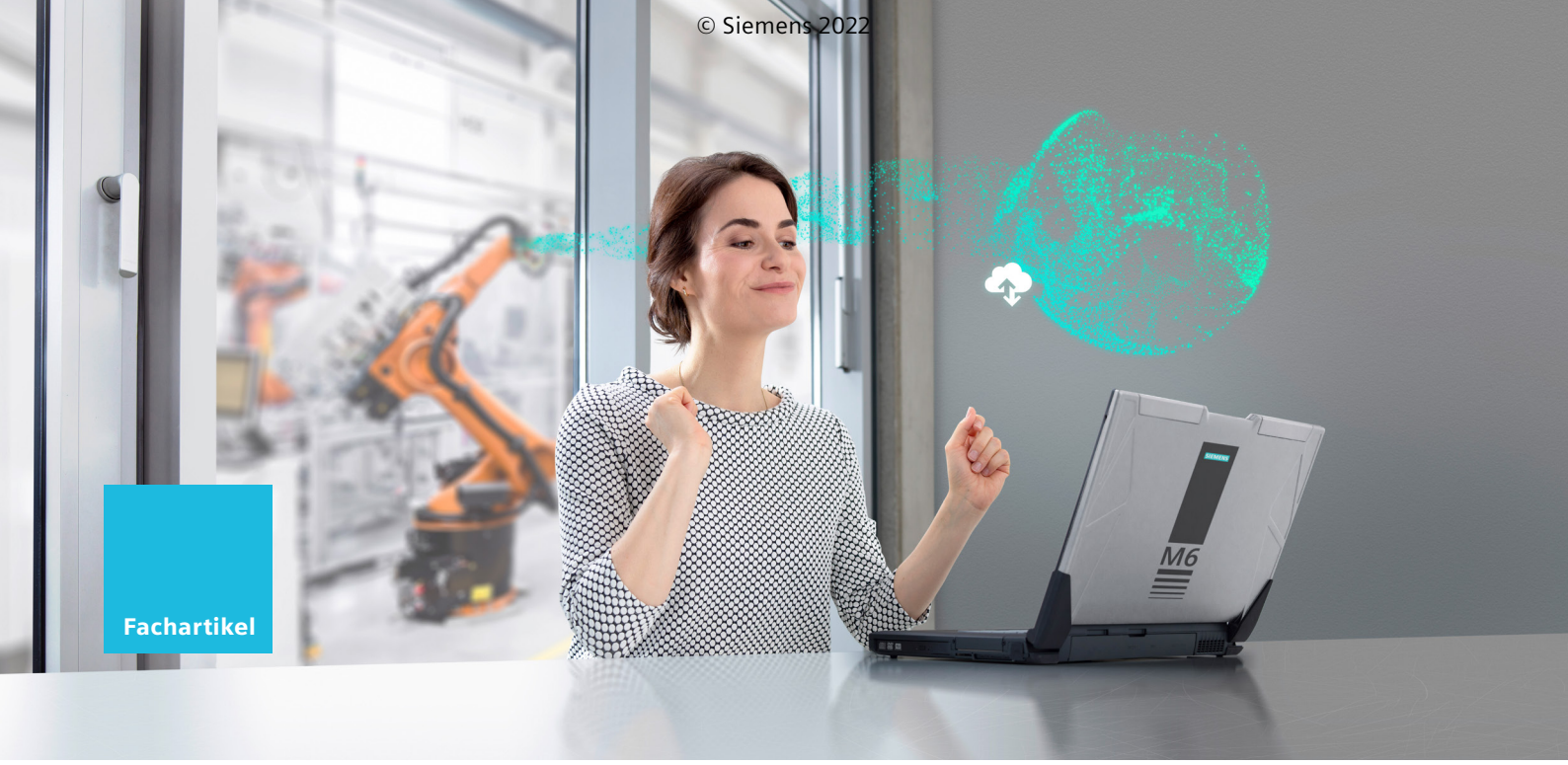


Fachartikel

Viele Wege führen zur Cloud

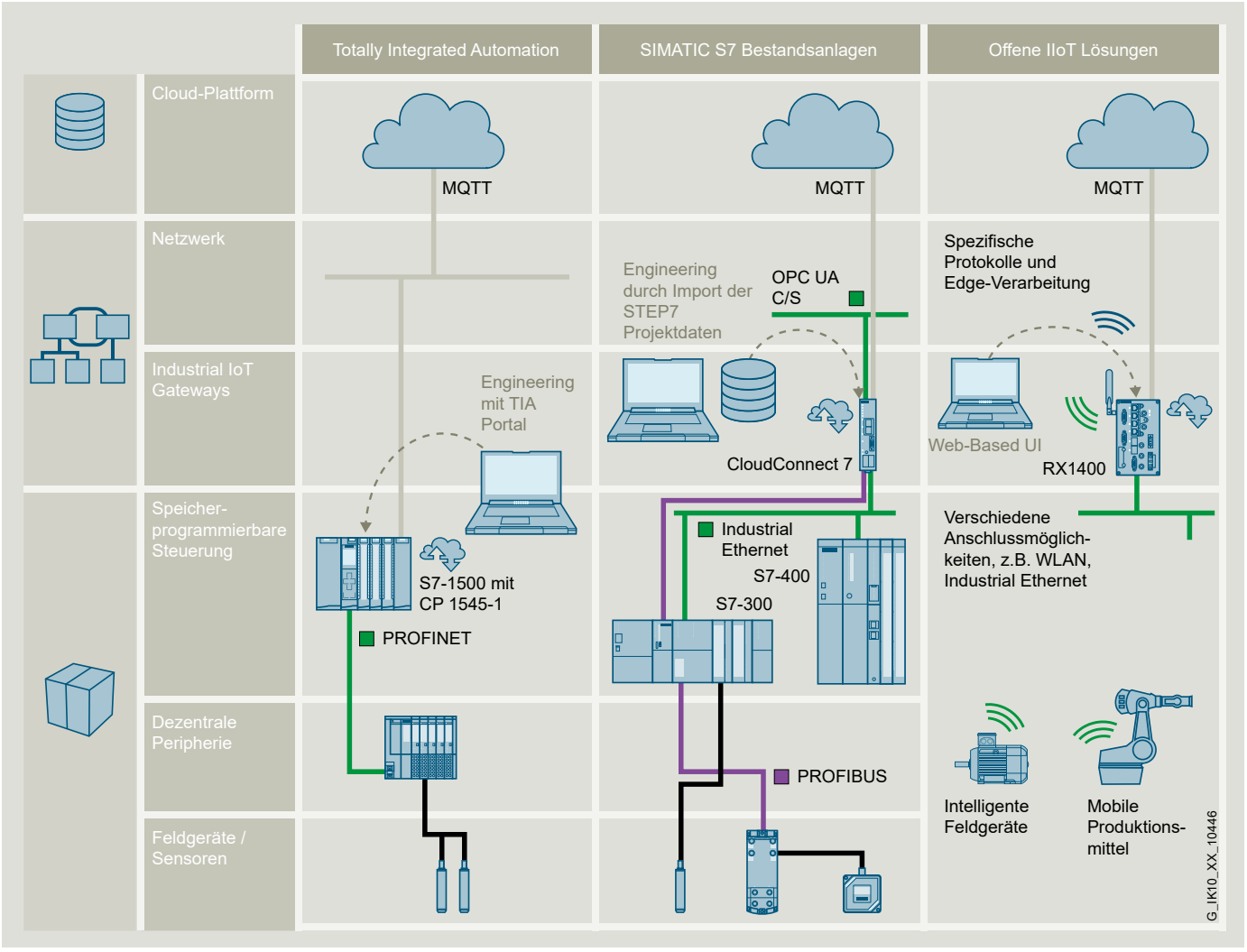
Sprichwörtlich führen viele Wege nach Rom. Ähnlich verhält es sich mit dem Datentransfer in Cloud-Lösungen. Um einen Mehrwert aus Daten generieren zu können, müssen diese zunächst gesammelt und transferiert werden. Die möglichen Lösungen dafür sind so vielfältig wie die Anforderungen der verschiedenen Automatisierungssysteme. Datensicherheit spielt dabei immer eine zentrale Rolle.

IIoT und die Cloud

Zwei wesentliche Merkmale der Digitalisierung sind ein steigender Vernetzungsgrad von Industrieanlagen sowie eine Erhöhung dezentraler Intelligenz: In einer industriellen Anlage sind mehr Geräte in der Lage, Daten abseits ihres eigentlichen Einsatzzweckes zu liefern. Gleichzeitig kann dieses Mehr an Daten besser abtransportiert werden.

Um diese im „Industrial Internet of Things“ (IIoT) generierten Daten nutzbar zu machen, also aus Daten Wissen und wirtschaftlichen Nutzen zu generieren, braucht es flexible und skalierbare Speicher- und Rechenkapazitäten. Diese Eigenschaften bringen cloudbasierte Systeme, wie das cloudbasierte, offene IoT-Betriebssystem MindSphere von Siemens, mit.

Sollten alle verfügbaren Informationen direkt in die Cloud übertragen werden? Das ist nur bedingt zu empfehlen. Während es bisher hieß: „Woher überhaupt die Daten nehmen?“, muss man sich heute zunehmend die Frage stellen: „Wo ist eine Vorverdichtung der Daten sinnvoll?“ Der Grund: Obwohl die von der Infrastruktur zur Verfügung gestellte Bandbreite oft zunimmt, wächst sie nicht notwendigerweise so stark wie die Datenmenge. Vorausschauende Planung kann helfen, zukünftige Engpässe zu vermeiden. In dieser Hinsicht bietet eine in die Anlagensteuerung integrierte Lösung eine Reihe von Vorteilen. Zum Beispiel können hier Daten bereits vorverarbeitet werden – die Steuerung fungiert dabei als Datenkonzentrator und hilft dadurch, unnötige Netzwerklasten zu vermeiden. Darüber hinaus kann ein Kommunikationsprozessor mit Sicherheitsfunktionen das Konzept ergänzen, wie nachfolgend beschrieben. Andererseits kann oder soll in manchen Fällen – zumeist bei Bestandsanlagen – das eigentliche Steuerungsprogramm nicht verändert werden. In diesem Fall kann ein separates Gerät die benötigten Konnektivitätsoptionen bieten, während das Engineering-System unangetastet bleibt. Es werden also Daten generiert und eine Plattform zur Auswertung, z. B. die MindSphere, wird identifiziert. Wie aber erfolgt der eigentliche, sichere Datentransfer in die Cloud? Allgemein lassen sich zwei Methoden der Cloud-Anbindung unterscheiden: entweder über externe Hardware oder als integrierte Lösung, zum Beispiel in Form eines Kommunikationsprozessors für die Steuerung. Gehen wir ins Detail ...



Verschiedene Wege zur einfachen Cloud-Anbindung – je nach installierten Geräten und tatsächlichem Anwendungsfall

Werten Sie Ihre Steuerung mit Cloud-Anbindung auf

Eine integrierte Lösung wie der neue Kommunikationsprozessor SIMATIC CP 1545-1 erweitert zum Beispiel eine vorhandene Anlagensteuerung SIMATIC S7-1500 um die Möglichkeit, Daten sicher zur Cloud zu senden. Dieser Ansatz bietet mehrere Vorteile: Einerseits kann die Steuerung als bereits vorhandener Datenaggregator für die weiter oben erwähnte Vorverarbeitung verwendet werden. Die Anlagenhersteller besitzen bereits das hierfür erforderliche prozessbezogene Know-how. Der Aspekt der Cloud-Anbindung kann somit bei der Erzeugung des Steuerungsprogramms unmittelbar mit einbezogen werden. Andererseits kann bereits vorhandene oder ohnehin erforderliche Hardware zum Berechnen von Werten genutzt werden, während der Kommunikationsprozessor die benötigten Cloud-Protokolle wie Message Queuing Telemetry Transport (MQTT) zur Verfügung stellt.

Schlussendlich sollte noch beachtet werden, dass nicht in jedem Fall auf alle in einer Anlage verfügbaren Messwerte direkt zugegriffen werden kann. Zwar steigen der Vernetzungsgrad und vor allem die Ausbreitung der Ethernet-Infrastruktur weiter, jedoch ist es nicht immer sinnvoll diese Vernetzung bis in die unterste Sensorebene zu führen. Vor allem aus ökonomischen Gründen ist beispielsweise die Sensorebene oft noch über Bus-Systeme oder analoge Signale angebunden. Die Informationen so angebundener Sensoren stehen auf der Anlagensteuerung jedoch zur Verfügung und können durch eine integrierte Cloud-Anbindung für übergeordnete Auswertungen genutzt werden.

Anwenderfreundliche Cloud-Anbindung für Bestandsanlagen

Bei der externen Variante werden Informationen aus der Anlage von einem separaten Gerät gesammelt und dann gesichert an die Cloud gesendet. Eine solche Lösung ist immer dann ratsam, wenn die eigentliche Maschine oder Anlagensteuerung unangetastet bleiben soll und die Automatisierungsseite nicht von Sicherheitsaktualisierungen betroffen sein darf.

Neben dem bereits verfügbaren RUGGEDCOM RX1400 gibt es zwei weitere Wege, bestehende Systeme mit der Cloud zu verbinden: über das Industrial IoT Gateway SIMATIC CloudConnect.

SIMATIC CC712 erleichtert die Anbindung einer SIMATIC S7-300 oder S7-400 über Industrial Ethernet mit dem S7-Protokoll. Mit SIMATIC CC716 können dagegen bis zu sieben Steuerungen des Typs SIMATIC S7 über Schnittstellen wie Industrial Ethernet oder Profibus/MPI angebunden werden.

Mit dem neuen SIMATIC CP 1545-1 lässt sich die Steuerung SIMATIC S7-1500 auf einfache Weise mit Fähigkeiten zur Cloud-Kommunikation versehen.

SIMATIC CloudConnect 7 bietet eine einfache Möglichkeit zur Anbindung von Bestandsanlagen.

Bei dieser Lösung braucht das bestehende Automatisierungsprogramm nicht geändert werden, um die wesentlichen Informationen auszuwählen und weiterzuleiten. Darüber hinaus können die von CloudConnect 7 aus den SIMATIC S7-Stationen der unteren Ebene gelesenen Daten als OPC UA-Variablen (Server) bereitgestellt werden. Dies ermöglicht einen standardisierten Datenaustausch, zum Beispiel mit MES-Systemen oder Bedienoberflächen und Steuerungen von Fremdanbietern.

In allen Fällen wird das offene Cloud-Protokoll Message Queuing Telemetry Transport (MQTT) verwendet. Dieser etablierte Standard ermöglicht auch die Übertragung von Daten an MindSphere, das IoT-Betriebssystem von Siemens. Auch Direktverbindungen mit Plattformen wie Microsoft Azure, IBM Cloud oder Amazon Web Services (AWS) sind damit implementierbar.

Security als elementarer Bestandteil

Immer wenn von cloudbasierten Systemen die Rede ist, werden Daten in unternehmenseigenen oder sogar öffentlichen Netzen übertragen. Daher sollte Datensicherheit (Security) immer Bestandteil des Gesamtkonzeptes sein. Die Datenübertragung in die MindSphere ist daher immer zertifikatsbasiert verschlüsselt.

Besondere Aufmerksamkeit sollte jedoch der eigentlichen Anbindung der Automatisierungszelle oder Anlage gewidmet werden. Da für den Cloud-Betrieb eine Verbindung mit dem übergeordneten Netzwerk notwendig ist, gibt es immer einen potentiellen Zugangspunkt für Angreifer. Die Schwere der potentiellen Bedrohung hängt vom übergeordneten Netzwerk und seinen Schutzmaßnahmen ab. In vielen Fällen ist allerdings ein zusätzlicher Schutzmechanismus in der Zelle sinnvoll, auch weil dann die Zugriffsberechtigung unabhängig von übergeordneten Mechanismen kontrolliert werden kann.

Zwei unterschiedliche Schutzkonzepte bieten sich an: entweder eines mit separater Hardware wie die Industrial Security Appliance SCALANCE SC632-2C für die Anbindung über das vorhandene Unternehmensnetzwerk oder aber ein WAN-Router für die leitungsgebundene oder drahtlose Kommunikation über Mobilfunknetze (z. B. ein SCALANCE M874-4 über LTE).

In jedem Fall fungiert das SCALANCE-Gerät unter anderem als konfigurierbare Firewall. Bei entsprechender Einrichtung kann auf alle Geräte im untergeordneten Netzwerk IP-basiert zugegriffen werden.

Weitere Informationen

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 **siemens.de/industrialsecurity**

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

PDF
Fachartikel
PD-PA-18/19-6
PDF 0522 5 De
Produced in Germany

Bei der integrierten Lösung mit SIMATIC S7-1500 bietet der Kommunikationsprozessor SIMATIC CP 1545-1 nicht nur eine separate Netzwerkverbindung, sondern auch eine eingebaute Firewall. Der Betriebsstatus des Kommunikationsprozessors hat keine Auswirkung auf die eigentliche Steuerung. Selbst im Fall einer von außen geführten Attacke mit der Absicht, den Dienst zu blockieren (Denial of Service), die die Funktion des Kommunikationsprozessors beeinträchtigt, kann die eigentliche Steuerung ungestört weiterarbeiten. Bei dieser Lösung ist stets eine Netztrennung realisiert: Die Steuerung ist vom übergeordneten Netzwerk aus erreichbar, aber der Zugriff auf untergeordnete Geräte ist gesperrt, weil kein IP-Routing stattfindet.

Kurz gesagt: Mit dem Kommunikationsprozessor CP 1545-1 kann eine für die individuellen Anforderungen der Anlage maßgeschneiderte Cloud-Anbindung implementiert werden. Für die Verarbeitung der Daten sind alle von der SIMATIC S7-1500 vertrauten Programmierungsmöglichkeiten verfügbar. Ein individueller Schutz der Steuerung oder des Automatisierungssystems ist sinnvoll und wird bereits vom Kommunikationsprozessor gewährleistet. Für externe Geräte wie CloudConnect 7 stehen zusätzliche Sicherheitsoptionen zur Verfügung.

siemens.de/cloudconnect