SIEMENS

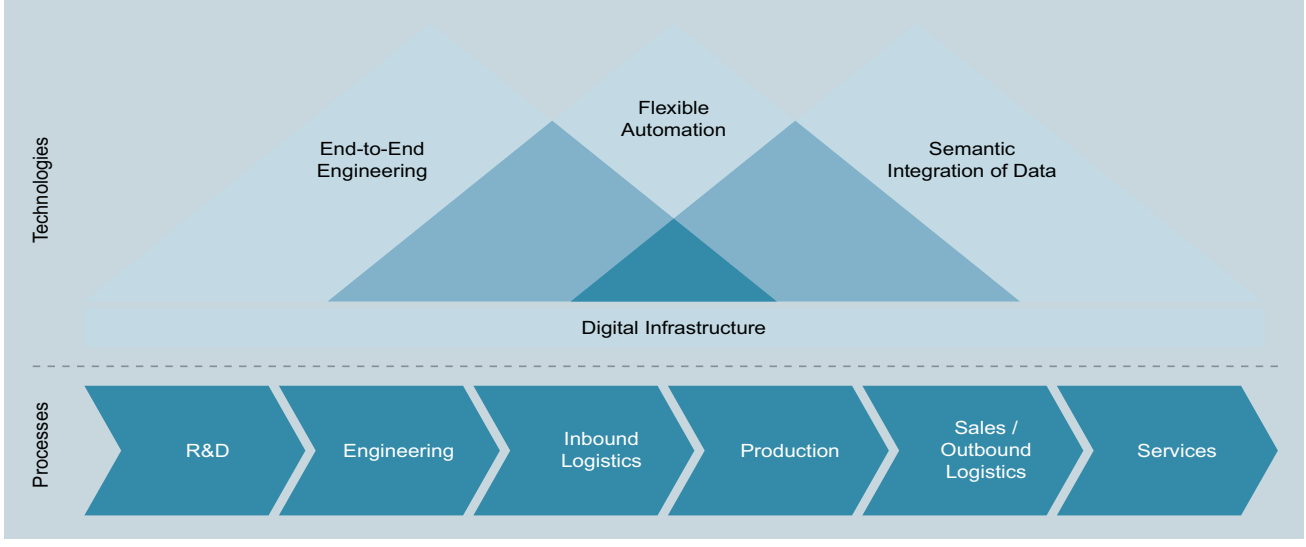
Fachartikel

Vom Sensor in die Cloud

OPC UA und industrielle Netzwerke als Infrastruktur der digitalen Fabrik

Die Integration unterschiedlicher Systeme in eine IT- oder Automatisierungsarchitektur ist kompliziert, weil es keine einheitlichen Schnittstellen und Protokolle gibt. Wie muss eine Kommunikationsarchitektur aussehen, die Zehntausende Geräte in der digitalen Fabrik vernetzt? Industrielle Netzwerke und OPC Unified Architecture gelten hier als Schlüssel der digitalen Infrastruktur.

Die Herausforderung wird deutlich, wenn man sich die Anwendungsszenarien in der digitalen Fabrik näher betrachtet. Diese lassen sich in drei Bereiche gliedern.



Die wesentlichen Technologie-Felder der digitalen Fabrik benötigten eine gemeinsame digitale Infrastruktur.

Erstens: Das End-to-End-Engineering bedeutet, dass die Daten aus dem Produktdesign für das Fertigungs-Engineering genutzt werden können, zum Beispiel zur Ableitung von Steuerungsprogrammen. Damit können unterschiedliche Perspektiven auf ein Erzeugnis in einem einheitlichen Datenmodell erfasst und entwickelt werden, was Änderungen vereinfacht, Fehler vermeiden hilft und die Engineering-Zeiten einschließlich der Fertigungseinführung deutlich reduziert.
Zweitens: Die flexible Automation will den (scheinbaren) Widerspruch zwischen Flexibilität und Automatisierung auflösen, um auf dem gleichen Anlagenpark unterschiedliche Produkte herstellen zu können. Kollaborative Roboter, die ihren menschlichen Kollegen assistieren, sind ein Beispiel, wie sich die gleich bleibende Leistungsfähigkeit und Präzision einer Maschine mit den menschlichen Möglichkeiten im Umgang mit komplexen, dynamischen Situationen optimal ergänzen. Neue Fertigungsverfahren wie der 3D-Druck zählen in diesen Bereich.
Drittens werden mit der Sammlung und Integration von Daten über den gesamten Maschinenlebenslauf neue Services möglich, zum Beispiel für die Wartung.

Vertikale und horizontale Integration

Heutige Lösungen folgen meist einer typischen „Automatisierungspyramide", das heißt die einzelnen Schichten von der Sensor- über die Controller- und HMI-Ebene bis zum MES- und ERP-System sind hierarchisch aufgebaut und erlauben oft keinen direkten Zugriff von den überlagerten Systemen auf weiter unten liegende Schichten – außer die Zwischenschichten haben ein explizites Routing dafür vorgesehen.

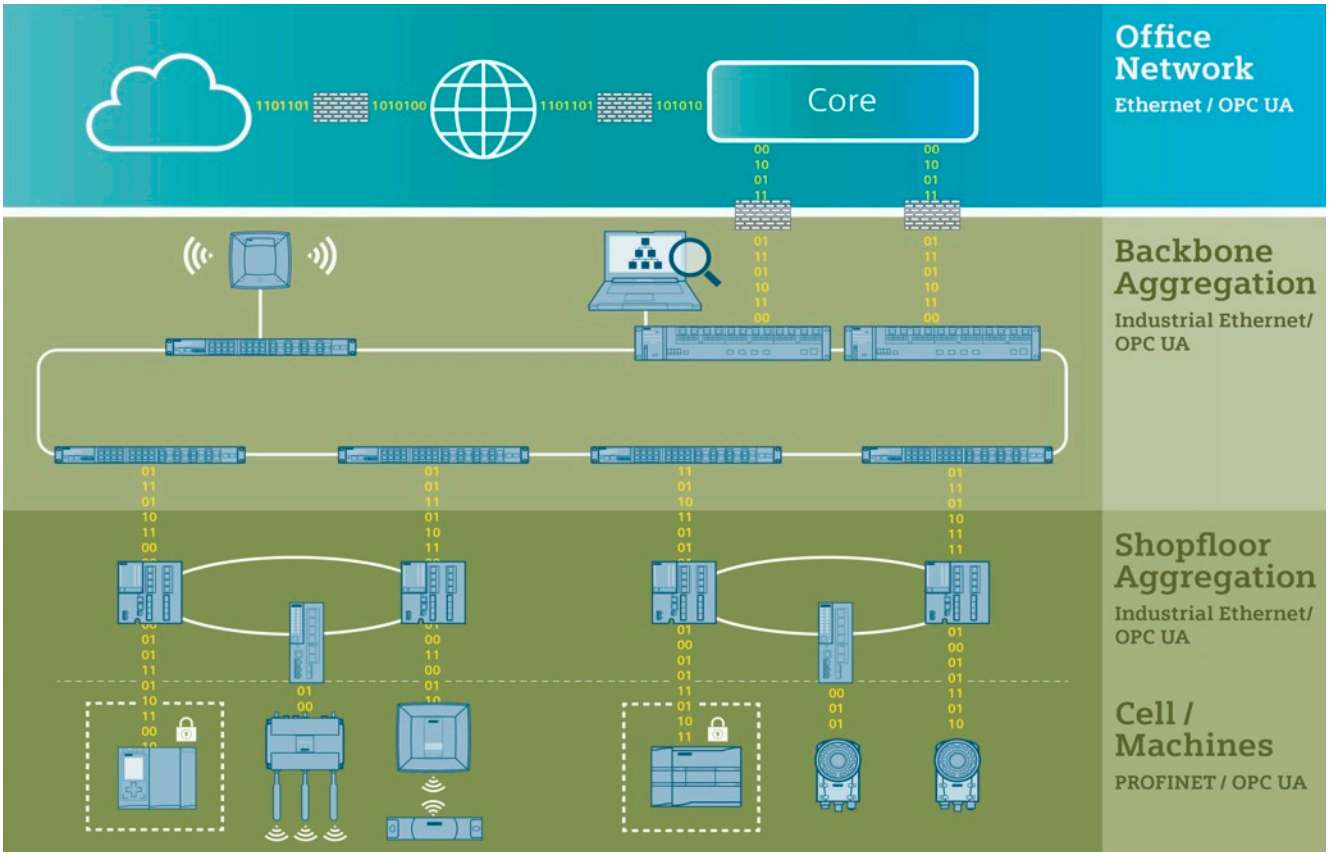
Die digitale Fabrik forciert hingegen die horizontale (also zwischen Komponenten auf der gleichen Ebene) und vertikale Integration (Kommunikation zwischen Schichten) der Kommunikationsebenen. So löst sich in der digitalen Fabrik einerseits die bisherige starre Zellenorganisation einer Fertigung auf (zum Beispiel durch frei bewegliche, autonome Roboter); die Maschinen brauchen deshalb eine Informationsinfrastruktur, die nicht mehr strikt hierarchisch organisiert ist, sondern der jeweiligen, sich dynamisch verändernden Umgebung Rechnung trägt.

Die Integration von Daten als Informationsquelle für analytische, datenbasierte Services führt andererseits zur Auflösung der horizontalen Schichten. Denn um zum Beispiel für vorausschauende Wartung (predictive maintenance) neue Erkenntnisse zu gewinnen, ist eine hohe Datendichte notwendig, von Design und Engineering angefangen über Qualitätsdaten in der Fertigung bis hin zu Sensoren, die bei der Verwendung einer Maschine ihre Messwerte in die IT-Systeme (Cloud) liefern. Diese Daten sind unter Umständen für die SPS, die die Fertigungsmaschine steuert, nicht relevant oder würden die Ressourcen des Controllers für reines Daten-Routing missbrauchen. Es ist deshalb sinnvoll, dass die Sensoren als Informationsquelle zwar einerseits die Steuerungsebene bedienen, andererseits aber ihre Ergebnisse in anderen Zyklen, Auflösungen oder mit unterschiedlichen Messwerten direkt in den Datenpool der Cloud liefern.

Schließlich darf man sich eine solche digitale Fabrik nicht als unveränderliches System vorstellen, sondern eher als einen Organismus, der sich (selbststeuernd oder durch Engineering) laufend den neuen Anforderungen anpasst. Dementsprechend muss eine solche Architektur flexibel und leicht wartbar sein, um die Komplexität intelligent beherrschen zu können.

Anforderungen an die Datennetzwerke

Die Kommunikationsinfrastruktur, die als Basis für die skizzierte Architektur notwendig ist, muss deshalb unterschiedlichen Anforderungen genügen. Einerseits sind Eigenschaften wie die Nutzung offener Standards, Verfügbarkeit, Quality of Service und vor allem Sicherheit gefordert, die ein Industrial-Ethernet-Netzwerk bereits heute auszeichnen. Da aber andererseits die Anbindung an IT-Systeme für datenbasierte Services und eine erhöhte Transparenz über alle Ebenen gefordert wird, ist eine Verknüpfung zwischen Office- und Produktionsnetzwerk notwendig, die zwar über Absicherungsmaßnahmen die Performance im Industrie-Netz sicherstellt, aber dennoch den Zugriff auf alle Schichten, Geräte und Komponenten erlaubt. Als Netzwerk-Topologie bieten sich deshalb verschiedene Aggregationsstufen sowie die Einführung eines Factory Backbones an, um einerseits die schnelle Kommunikation zwischen den Geräten in den einzelnen Zellen zu ermöglichen und um andererseits die leistungsfähige Verknüpfung von Office-Netzwerk und den verschiedenen Unterbereichen sicherzustellen.



Verschiedene Aggregationsebenen und ein Factory Backbone als Ring bilden die „Industrial Network Topology"

Um jedoch die Ziele und Anforderungen der digitalen Fabrik zu erfüllen, ist es mit einer durchgängigen Netzwerk-Topologie nicht getan. Benötigt wird ein Kommunikationsprotokoll, das offen und standardisiert ist, ausreichende semantische Informationen und Übersetzungsmöglichkeiten bereitstellt, einfach erweiter- und wartbar ist, ein Höchstmaß an Sicherheit in verschiedenen Ausprägungen bietet sowie einen so geringen Speicher- und Prozessorbedarf hat, dass es auf kleinen Geräten implementiert werden kann.

Kommunikationsarchitektur für die digitale Fabrik

Die Antwort auf diese Anforderungen ist das Unified-Architecture-Protokoll der Open Platform Communications Foundation (OPC UA). Das Wichtigste: Bei OPC UA handelt es sich nicht nur um ein Protokoll, sondern um eine vollständige Architektur, die zur Übertragungsdefinition geeignete Software-Stacks für Geräte- und Softwarehersteller sowie Engineering-Tools für die Systemintegratoren bereithält. Damit bietet OPC UA wichtige Vorteile. Zuerst ist durch das Information Model sichergestellt, dass alle Daten typsicher übertragen werden. Auch komplexe Datentypen (Strukturen) sind möglich. Außer den reinen Datenwerten transportiert OPC UA semantische Informationen zwischen den Kommunikationspartnern.

Da die Architektur objektorientiert funktioniert, ist die Semantik in einen Objektkontext eingewoben – sie besteht also aus mehr als nur einem „sprechenden" Bezeichner, sondern bezieht sich immer auf das gesamte Objekt mit seinen Eigenschaften und Methoden. Funktionsaufrufe über das Netzwerk erlauben eine gewisse Steuerung des Kommunikationspartners. Schließlich werden Events als Ad-hoc-Kommunikation oder Message Broker für die Anbindung an die Cloud unterstützt.

Die Fehlersicherheit bei der Implementierung wird durch Schnittstellen, die ihre Spezifikation in der Engineering-Umgebung einbringen (browseable interfaces), erhöht. Für jedes Gerät kann eine Beschreibungsdatei ins Engineering importiert oder aus dem online verfügbaren Gerät gelesen werden, die eine detaillierte Spezifikation der Schnittstelle bietet. Die korrekte Verwendung der Schnittstelle im Anwenderprogramm wird durch die Entwicklungswerkzeuge sichergestellt. Der Schutz vor unberechtigten Zugriffen ist ein weiterer, zentraler Punkt. OPC UA nutzt zur Abwehr zum Beispiel X.509-Zertifikate und entsprechende Sicherheitsprotokolle.

Für die konkrete Anwendung in unterschiedlichen Applikationen arbeiten Industrie-Verbände mit der OPC Foundation an sogenannten Companion Specifications, die die Standards von OPC UA für eine bestimmte Domain ergänzen. Ein Beispiel ist die Zusammenarbeit mit PLCopen, bei der gemeinsam Bausteine und Zugriffsverfahren für Daten in einer speicherprogrammierbaren Steuerung (PLC) definiert wurden. Hersteller wie Siemens integrieren diese Mechanismen, um eine auf OPC UA beruhende Integration der Steuerung zum Beispiel mit Geräten anderer Hersteller oder mit PC/IT-Systemen zu ermöglichen. So unterstützt der CP 443-1, der als Steckbaugruppe im System SIMATIC S7-400 eingesetzt wird, die Client- und die Server-Funktionalität von OPC UA. Damit können andere Systeme auf die zuvor im Engineering freigegebenen Datenbereiche der SIMATIC S7-400-CPU über die standardisierte Schnittstelle zugreifen. Durch diese Baugruppe können bestehende Anlagen mit OPC UA-Kommunikationsmöglichkeiten nachgerüstet werden.

Doch bis OPC UA als durchgängige Kommunikationsarchitektur eingesetzt werden kann, sind weitere Standardisierungsaufgaben zu erledigen, da manche Bereiche der industriellen Kommunikation nicht vollständig abgedeckt werden. So sind beispielsweise auf der Ebene der Sensoren erst einige Gerätefamilien oder Technologien wie RFID-Systeme (Radio Frequency Identification) für OPC UA spezifiziert. Zudem werden Definitionen auf höherer Ebene benötigt, wenn es nicht mehr um technische Parameter, wie zum Beispiel die Sendeleistung eines RFID-Readers, oder den Zugriff auf reine Prozessdaten gehen soll. Vielmehr wird es notwendig sein, funktionale Charakteristika je nach Branche und Anwendungsfall zu standardisieren, die mehr dem Engineering-Kontext des Anlagen-Ingenieurs und weniger dem des Software-Entwicklers entsprechen.

Doch abgesehen von diesen künftigen Aufgaben – OPC UA ist heute eine in ihrem Funktionsumfang einzigartige Kommunikationsarchitektur, die als Basis für die vertikale und horizontale Integration in der digitalen Fabrik unverzichtbar ist.

Security-Hinweise

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
www.siemens.com/industrialsecurity

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

PDF
Fachartikel
FAV-407-2016-PD-PA
BR 092016 De
Produced in Germany

siemens.de/industrielle-kommunikation