3 Industrielle Netzwerke – Datenautobahn in der digitalen Fabrik

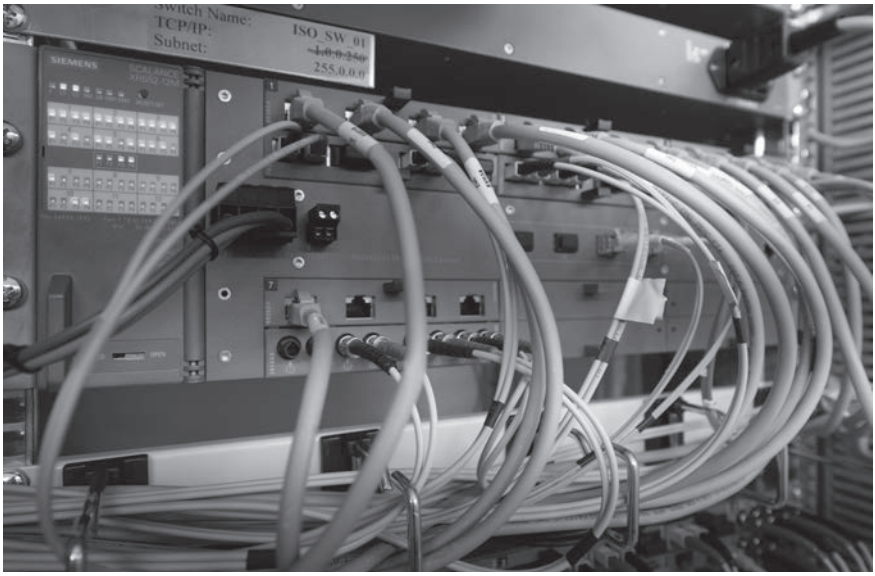
Manfred Wolf

Über den Autor

Manfred Wolf ist Marketing Manager für Industrial Network and Components, Hardware and Software bei der Siemens Division Process Industries and Drives und unter anderem für die Vermarktung industrieller Kommunikationsnetzwerke zuständig. Seine Expertise für das Thema Industrielle Kommunikation erlangte er als Produktmanager für IWLAN und strategisches Business Development für industrielle Kommunikation im Umfeld erneuerbarer Energien. Herr Wolf ist gelernter Energieelektroniker und studierte Elektrotechnik mit der Fachrichtung Automatisierungstechnik an der Technischen Hochschule Nürnberg Georg Simon Ohm.

Ziel der rasant fortschreitenden Digitalisierung der industriellen Welt ist es, sämtliche Prozesse entlang der Wertschöpfungskette transparenter und dadurch letztendlich effizienter zu gestalten. Dies führt zu einer ständig wachsenden Zahl „intelligenter", netzwerkfähiger Komponenten im Produktionsumfeld und zu steigenden Datenmengen. Dadurch wächst der Bedarf an leistungsfähiger, industrietauglicher Netzwerktechnik (Abbildung 14) für den koordinierten Transfer und die Verarbeitung all dieser Daten – vom einzelnen Sensor bis zur Cloud.

Die „digitale Fabrik" stellt deutlich höhere Anforderungen an Aufbau, Struktur, Hardware, Software und Verbindungen eines Netzwerks als dies im Bereich der klassischen Büro- und Unternehmens-IT der Fall ist. Einen viel höheren Stellenwert haben insbesondere die Themen Robustheit, Zuverlässigkeit und Sicherheit. Hinzu kommen die aus der klassischen Automatisierungstechnik bekannten Anforderungen hinsichtlich Verfügbarkeit, Deterministik und Flexibilität. Dabei müssen oft bestehende Lösungen integriert beziehungsweise migriert und erweitert werden. Das setzt geeignete Komponenten, individuell anpassbare Strukturen sowie applikations- und netzwerkspezifisches Know-how voraus. Nicht zu vernachlässigen ist der reibungslose und gesicherte Betrieb des industriellen Netzwerkes, um die Kommunikation an 365 Tagen rund um die Uhr am Laufen zu halten. Jeder Produktionsausfall kostet unter Umständen erhebliche Summen und mindert die Wettbewerbsfähigkeit des Unternehmens.



Quelle: Siemens AG

Abbildung 14: Die digitale Fabrik erfordert leistungsfähige Netzwerktechnik und gut strukturierte Netzwerke

Daher unterscheidet sich auch der Service und Support in der Produktion von dem in der Office-Welt. Industrielle Netzwerkkomponenten müssen einfach zu handhaben, schnell auszutauschen und von Fachpersonal ohne spezielle IT-Kenntnisse in Betrieb zu nehmen sein.

3.1 Spezielle Anforderungen im Industrieumfeld

Zahlreiche Unternehmen setzen heute auf standardisierte Kommunikationsmechanismen. Wurden bis vor ein paar Jahren Office- und Industriekommunikation strikt voneinander getrennt, verschwimmen die Grenzen zunehmend. Die Standards des Institute of Electrical and Electronic Engineers (IEEE) haben sich etabliert und die Industrie nutzt diese, um eine durchgängige Kommunikation von der Feldebene bis in die Cloud zu ermöglichen. Abgesehen von einheitlichen Netzwerkstandards für die Datenübertragung (z. B. Ethernet nach IEEE 802.3), unterscheiden sich industrielle Netzwerke in etlichen Punkten von klassischen Unternehmensnetzwerken. Das deutlich rauere Umfeld sowie sicherheitsrelevante und produktionstechnische Aspekte stellen einige besondere Anforderungen an die Netzwerkkomponenten.

3.1.1 Robustheit

Viele Industrieanlagen laufen rund um die Uhr. Niedrige oder hohe Temperaturen, Staub, Vibrations- und Schockbelastung, Luftfeuchtigkeit, aggressive Substanzen und insbesondere erhöhte elektromagnetische Strahlung, beispielsweise durch Umrichter oder (Schweiß)Transformatoren, erfordern eine entsprechend robuste Ausführung aller Komponenten, gerade auch der Netzwerktechnik. Ein hoher Schutz gegen Staub und Feuchtigkeit (Schutzart IP65/67) ist im schaltschranklosen Einsatz im Feld eine Voraussetzung für dauerhaft zuverlässigen Betrieb. Die Robustheit bezieht sich auch auf die genutzten Protokolle. Das Standard-Ethernet-Zugriffsverfahren „Carrier Sense Multiple Access with Collision Detection“ (CSMA/CD) ist für viele Automatisierungsaufgaben nicht zuverlässig genug, da es Kommunikationsunterbrechungen im zwei- bis dreistelligen Millisekundenbereich zulässt. Standardisierte industrielle Protokolle wie Profinet schließen diese Lücke und ermöglichen einen robusten Datenaustausch zwischen Sensoren, Aktoren, Maschinen und Leitsystemen.

3.1.2 Zuverlässigkeit

Eine entscheidende Rolle in der industriellen Kommunikation spielt die Übertragungszeit. Die typische zyklische Abarbeitung von Steuerungsprogrammen im Bereich weniger Millisekunden erfordert eine deterministische, mitunter auch taktsynchrone Übertragung mit garantierter Reaktionszeit. Nur dann lassen sich beispielsweise mehrere Antriebe einer Anwendung dynamisch und präzise zueinander synchronisieren. Am Beispiel einer Zeitungsdruckmaschine lässt sich das gut veranschaulichen: Im Sekundentakt werden viele Zeitungen gedruckt, in die beispielsweise zusätzliche Werbeprospekte hineingelegt werden. Sollte der Werbeeinleger leer sein oder es zu einem Papierstau kommen, muss sich die Anlage schnell und präzise auf die jeweilige Situation einstellen können.

Zuverlässig müssen die Komponenten untereinander zusammenspielen. Aufeinander abgestimmte und getestete industrielle Komponenten sind für ein zuverlässiges Industrienetzwerk entscheidend. Schnelle Meldungen über den physikalischen Zustand der Komponenten in überlagerte Netzwerkmanagementsysteme und Leitwarten sind wichtig, um schnellstmöglich Wartungs- und Servicezeiträume zu terminieren. So kann der Produktionsfluss aufrechterhalten und die Wettbewerbsfähigkeit gestärkt werden.

3.1.3 Sicherheit

Unter dem Begriff Sicherheit versteht man im Deutschen zwei Aspekte – zum einen den der Netzwerksicherheit (Security), zum anderen den der funktionalen Sicherheit (Safety).

Netzwerksicherheit – gesicherter Zugriff

Mit zunehmender Vernetzung wird das Thema Netzwerksicherheit im Produktionsumfeld immer bedeutender. So muss mit geeigneten Security-Konzepten und -Komponenten gewährleistet werden, dass nur autorisierte Personen Zugang zum Produktionsnetzwerk und zu „ihren“ Maschinen und Anlagen haben. Das gilt sowohl für die Nutzer vor Ort als auch für Maschinenhersteller oder Dienstleister, die aus der Ferne Service- und Wartungsarbeiten durchführen. Umgekehrt muss sichergestellt sein, dass aus dem Produktions- oder einem Zellennetzwerk keine Gefährdung des Unternehmensnetzwerks und der Integrität der Daten möglich ist.

Das Konzept „Defense in depth“ (Abbildung 15) zeigt, wie Produktionsnetzwerke gesichert werden können, um die Gefahren von Cyber-Angriffen auf Maschinen und Anlagen weitgehend auszuschließen. Es setzt auf Anlagensicherheit, Netzwerksicherheit und Systemintegrität nach den Empfehlungen der ISA 99/IEC 62443.

Anlagensicherheit beginnt beim physischen Zugang von Personen zu Gebäuden und reicht bis zur Sicherung sensibler Bereiche über Berechtigungsausweise.

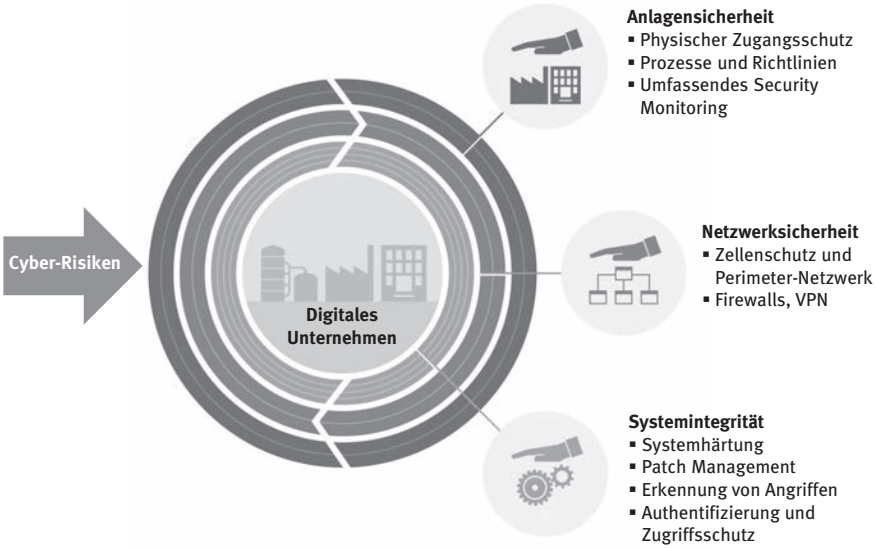


Abbildung 15: Defense-in-depth-Strategie für hohe Anlagen- und Netzwerksicherheit sowie Systemintegrität

Maßgeschneiderte Industrial Security-Services umfassen dazu Prozesse und Richtlinien für einen gesamtheitlichen Anlagenschutz. Von der Risikoanalyse über die Implementierung geeigneter Maßnahmen und deren Überwachung bis zu regelmäßigen Updates.

Produktionsnetzwerke vor unberechtigten Zugriffen zu schützen, ist heute insbesondere an den Verbindungsstellen zu anderen Netzwerken unabdingbar. Zusätzliche Sicherheit bietet die Segmentierung einzelner Teilnetzwerke über ein Zellenschutzkonzept mit Security-Moduln oder dezidierten Kommunikationsprozessoren der SPS. Die Datenübertragung kann zudem über Virtual Private Networks (VPN) geschützt werden, etwa für weltweite Fernzugriffe auf entlegene Anlagen über Internet oder Mobilfunknetze.

Die dritte tragende Säule ist die Sicherung der Systemintegrität. Dazu gehört, Feldgeräte, Steuerungen, SCADA- und HMI-Systeme gegen unbefugte Zugriffe abzusichern oder darin enthaltenes Know-how zu schützen. Weiterhin geht es um die Authentifizierung von Benutzern und deren Zugriffsrechte sowie um die Systemhärtung gegenüber Angriffen.

Funktionale Sicherheit – Safety

Spezifische Anforderungen stellt die Übertragung sicherheitsrelevanter Signale dar. Dabei muss unter allen Umständen gewährleistet sein, dass z. B. beim Betätigen eines Not-Halt-Tasters oder dem Auslösen einer anderen Sicherheitseinrichtung die erforderliche Reaktion unmittelbar und zwingend erfolgt. Nur dann lassen sich Mensch und Maschine vor Schäden schützen. Dafür gibt es zertifizierte Steuerungs- und Netzwerkkomponenten. Besondere Aufmerksamkeit erfordert in dieser Hinsicht die ständig wachsende Zahl mobiler Endgeräte in der Industrie. So müssen drahtlose Teilnehmer im Fehlerfall einen sicheren Zustand einnehmen, insbesondere bei Wartungs- und Serviceeinsätzen. Dabei ist zu beachten, dass funktionale Sicherheit nicht automatisch ein Abschalten der Anlage nach sich zieht. Beispielsweise wäre es fatal, wenn sich bei einem Kran mit Magneten der transportierte Gegenstand durch Abschalten der Anlage löst. In diesem Fall bedeutet der „Not-Halt“, dass der Magnet auch im Fehlerfall weiterhin seine Funktion beibehält.

3.1.4 Verfügbarkeit

Anders als im Büroumfeld können Ausfälle der Netzwerktechnik in der Produktion erhebliche Folgeschäden und -kosten nach sich ziehen, z. B. wenn Auftragsdaten von einem Leitstand nicht mehr zu den Maschinen übertragen werden können oder Maschinen einer Produktionslinie nicht mehr miteinander kommunizieren, weil ein Switch oder ein Kabel defekt ist. Entsprechend schnell

müssen fehlerhafte Komponenten jederzeit auch ohne IT-Spezialisten ausgetauscht werden können. In besonders sensiblen Anlagenteilen werden deshalb redundante Strukturen aufgebaut, die schnelles oder sogar stoßfreies Umschalten ohne Datenverlust ermöglichen.

Verfügbarkeit bezieht sich auch auf Geräte, Ersatzteile und geeignetes Personal. Für industrielle Anwendungen generell wichtig ist die Verfügbarkeit von Komponenten über einen langen Zeitraum, um die Funktionalität und die Investition abzusichern. Weltweiter Support und regional stationiertes, kompetentes Fachpersonal tragen dazu bei, lange Stillstandszeiten in der Produktion zu reduzieren und die Verfügbarkeit zu erhöhen.

3.1.5 Flexibilität

Sind in der Produktion Umstrukturierungen, Veränderungen oder Erweiterungen der Vernetzung erforderlich, z. B. durch Produktinnovationen, müssen Teilnehmer einfach unterschiedlichen Netzwerksegmenten/-domänen zugeordnet werden können und über verschiedene Medien (elektrisch/optisch) anzubinden sein. Weil viele Produktions- und Prozessanlagen oft sehr lange Laufzeiten haben, müssen auch ältere Kommunikationseinheiten in neue Strukturen integrierbar sein, um einerseits die Kosten, aber auch die Stillstandszeiten bei einer Modernisierung zu minimieren. Netzwerkgeräte für die Hutschiene im Schaltschrank, das klassische 19-Zoll-Rack oder die Wandmontage unterstützen diese Flexibilität. Bestimmte Anwendungen wie fahrerlose Transportsysteme, Einschienenhängebahnen, Krane, Stapler oder Handscanner erfordern Bewegungsfreiheit und müssen drahtlos mit überlagerten Steuerungen kommunizieren, wobei auch alle oben genannten Anforderungen gelten.

3.2 Aufbau und Struktur industrieller Netzwerke

Um den erhöhten Anforderungen industrieller Anwendungen zu genügen, empfiehlt sich eine Netzwerk-Architektur in mehreren Schichten und Segmenten (Abbildung 16).

In der Maschinen- oder Zellenebene, dem sogenannten Access Layer, sind Netzwerkteilnehmer (Steuerungen, dezentrale Peripheriebaugruppen, Umrichter, Bediengeräte) der Maschinen oder Anlagenteile meist über Kupferleitungen miteinander verbunden. Auf dieser untersten Ebene überwiegt die horizontale Kommunikation, der Austausch kleiner Datenpakete innerhalb beziehungsweise zwischen Maschinen (Machine-to-Machine, M2M) und Zellen, die Übertragungsdistanzen sind eher kurz (bis zu 100 Meter). Die Kommunikation muss mitunter zugleich deterministisch, fehlersicher, hoch verfügbar und zugriffsicher sein.