

The Siemens logo is displayed in a white rectangular box in the upper left corner of the page. The background of the entire page is a photograph of an industrial factory floor with a production line of red car doors.

Fachartikel

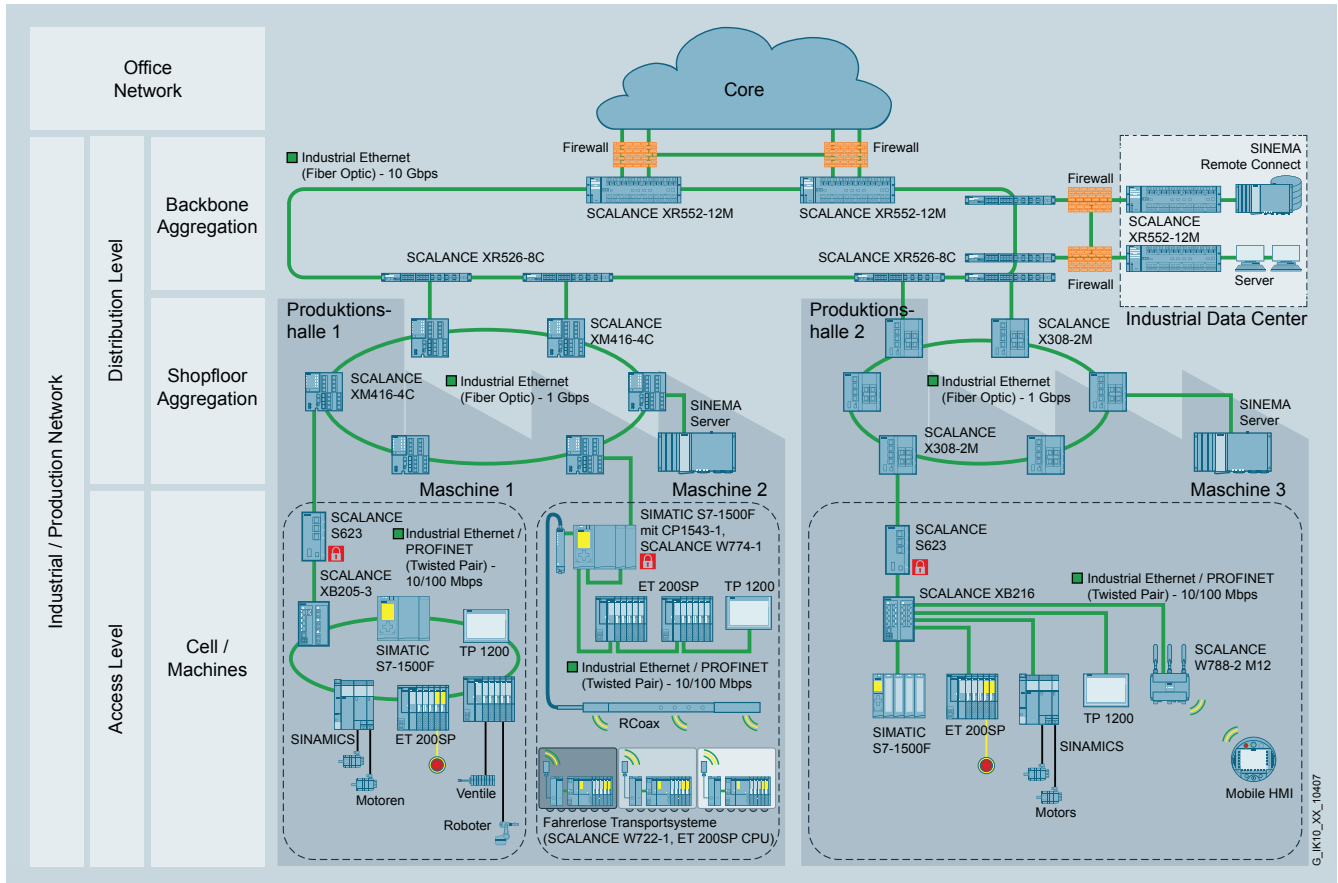
Die Grenzen der Konvergenz von Datennetzwerken

Industrielle Netzwerke als Teil der Automatisierung

Die geschickte Anbindung der Office- und Rechenzentren-Netzwerke an Automatisierungsnetzwerke ist für Unternehmen eine große Herausforderung – gerade im Hinblick auf die Aufgaben bei der Digitalisierung der Industrie, der damit einhergehenden, übergreifenden Vernetzung aller Unternehmensbereiche und des umfassenden Datenaustausches. Die Erfahrung zeigt, dass nicht jedes Netzwerk auf Ethernet-Basis – auf gleiche Weise geplant, realisiert und betrieben werden kann. Die falsche Herangehensweise im Hinblick auf eine vollständige Konvergenz der Netzwerke kann Kunden teuer zu stehen kommen.

Seit sich die Ethernet-basierte Kommunikation in industriellen Netzwerken mehr und mehr durchsetzt, haben sich spezielle Netzwerkdesigns – orientiert an den Anforderungen der Applikationen – in den unterschiedlichen Branchen, etabliert. Nun versuchen zahlreiche IT-Abteilungen, die geforderte Anbindung der Produktionsnetzwerke nach den bekannten Vorgehensweisen für das Design und den Betrieb von Office-Netzwerken zu realisieren, lösen bestehende industrielle Netzwerkstrukturen auf und binden die Automatisierungsgeräte in eine vorhandene IT-Infrastruktur ein. Die Risiken für die Unternehmen sind erheblich.

Hier ist zunächst festzustellen, dass erfahrene Anbieter industrieller Netzwerke dieses als Teil der Automatisierung verstehen und Greenfield- und Brownfield-Projekte unter anderen Voraussetzungen angehen als die Planung eines Office- und RZ-Netzwerkes. Es geht um das Ziel der Zusammenführung eines funktionalen Datenaustausches mit einer ausfallsicheren Automatisierung.



Beispielhafte schematische Darstellung einer industriellen Netzwerkinfrastruktur für ein produzierendes Unternehmen mit diskreter Fertigung, wie z. B. in der Automotive-Branche, mit Anbindung an die Office-IT.

Strukturelle und technische Besonderheiten eines industriellen Netzwerks

Industrielle Netzwerk-Infrastrukturen unterscheiden sich aufgrund der unterschiedlichen Anforderungen je nach Branche.

Bei produzierenden Unternehmen beispielsweise reichen die relevanten Netzwerkbereiche des industriellen Teils – je nach Netzwerkstruktur – vom Cell Level und Machine Level, auch Access Level genannt, über das Distribution Level mit den Zellenaggregationen wie der Shop Floor Aggregation, der Hallen- oder Stationsaggregation und der Anbindung eines möglichen Industrial Data Centers an die Backbone Aggregation. Letztere wiederum ist unter Beachtung der Security Policy über geeignete Schnittstellen an den Core-Bereich des Unternehmensnetzwerks mit der Rechenzentren-Netzwerkstruktur anzubinden.

Der Datenfluss

Der Datenfluss in industriellen Netzwerkinfrastrukturen ist geprägt von horizontaler und teilweise vertikaler Kommunikation. Somit besteht – anders als in der rein vertikalen Client-Server-Kommunikation in der Office-IT – häufig ein direkter Datenaustausch zwischen Devices (horizontale Kommunikation). Auch die vertikale Kommunikation unterscheidet sich teilweise, wenn sie beispielsweise zwischen Device und Controller erfolgt.

Um die Funktion der industriellen Steuerungskomponenten sicherzustellen, bedarf es nämlich einer zyklischen Kommunikation mit Deterministik, Taktsynchronität und sehr geringem Jitter¹⁾. Dies setzt eine dauerhaft aktive Kommunikationsverbindung voraus, die es bei der Client-Server-basierten Ethernet-Kommunikation – die nach dem „Best Effort-Prinzip“ funktioniert – innerhalb der sonstigen Unternehmens-IT nicht gibt. Eine industrielle Anlage muss in der Regel unterbrechungsfrei funktionieren, d. h. hochverfügbar sein und dies über einen langen Zeitraum, der nicht selten zehn und mehr Jahre beträgt. Die Auslegung des industriellen Netzwerkes mit robusten Komponenten und geeignete Redundanzverfahren, wie stoßfreie Redundanz für Motion-Applikationen oder Systemredundanz für Prozess-Applikationen, ist die Basis für eine erhöhte Verfügbarkeit der Produktionsanlage und kann den Betrieb auch in einem eventuellen Fehlerfall aufrechterhalten.

¹⁾ Unerwünschtes zeitliches Taktzittern bei der Übertragung von Digitalsignalen

Fehler- oder Servicefall

Tritt der Fehler- oder Servicefall dennoch ein, ist eine industrielle Anlage in der Regel über die IT-üblichen SLAs (Service Level Agreement) nicht ausreichend schnell wiederherzustellen. Selbst ein ständig verfügbarer Service kann unter Umständen nicht ausreichen, wenn die Reaktionszeit im SLA für zwei oder vier Stunden definiert ist. Letztendlich zählt nur die schnelle Wiederherstellzeit – also, wie lange es dauert, bis die Anlage wieder problemfrei läuft. Eine schnelle, einfache Fehlerlokalisierung ist gerade in komplexeren Netzwerkinfrastrukturen nur durch geeignete und integrierte Diagnose- und Monitoring-Tools möglich, die auch vom Automatisierungspersonal bedient werden können. Dabei sollte das Tool alle relevanten angebotenen Endgeräte, beispielsweise auch Steuerungs-, Antriebseinheiten und Peripherie überwachen und sich nicht auf Infrastrukturgeräte wie Server und Switches beschränken. Was ist der Vorteil?

Um schnellstmöglich defekte Komponenten austauschen und wieder in Betrieb nehmen zu können, ist es sinnvoll, auch die Aggregationsnetzwerke, wie den Industrial Backbone, direkt an der Anlage zu platzieren und so den Serviceweg und die Reaktionszeit gering zu halten. Die Umgebungsbedingungen in einer Fertigung, einer Verteilerstation oder an einer Ab- oder Umfüllanlage unterscheiden sich signifikant von den Klimabedingungen im Rechenzentrum oder Büro. Dass hierfür robuste Komponenten verwendet werden sollten, für die es auch nach Jahren noch Ersatz gibt, versteht sich ebenfalls von selbst.



Robuster Access Point, Variante für besondere Umwelthanforderungen und den Einsatz in Bus und Bahn

Zur Sicherung der Anlagenverfügbarkeit sollte eine Hotline jederzeit bereitstehen, die mit der Gesamtanlage vertraut ist. Hierfür hat sich gezeigt, dass ein homogenes Konzept und die Konzentration auf einen einzigen Automatisierungsherstellers die schnelle und effektive Lösungsfindung für Steuerungs- und Netzwerkkomponenten deutlich begünstigt.

Outsourcing und Personal

Outsourcing ist im Bereich der Office-IT für viele Firmen Alltag. Im Sinne der notwendigen Hochverfügbarkeit der industriellen Anlagen werden die zugehörigen Netzwerke selten fremdvergeben. Eigene Mitarbeiter tragen die Verantwortung und rüsten sich für Wartung und Störfälle. So werden für besonders kritische Bereiche Ersatzkomponenten vor Ort bereitgehalten.

Darüber hinaus ist bei der Planung und dem Betrieb einer industriellen Infrastruktur darauf Rücksicht zu nehmen, dass für den störungsfreien Betrieb ausreichend ausgebildetes Personal vor Ort ist. Nicht jede Firma ist in der Lage, IT-Fachleute stets verfügbar zu haben. So sind die Ansprechpartner typischerweise Automatisierer mit IT-Wissen und nicht IT-Spezialisten. Deshalb sollte die Netzwerktechnologie auch für weitergebildete Automatisierungstechniker beherrschbar sein, denn häufig müssen auch „Nicht-IT-Spezialisten“ einzelne Komponenten warten können.

In jedem Fall muss diese Rolle durch Fachkräfte besetzt sein, die eine Schnittstelle zwischen der Automatisierungstechnik und der IT bilden können und für beide Seiten als kompetenter Ansprechpartner dienen. In dieser Rolle ist neben der kabelgebundenen industriellen IT-Architektur auch die Verwaltung von Funkkanälen (WLAN, BT, Wireless HART, ...) im industriellen Umfeld anzusiedeln.

Safety and Security

Beim Thema Sicherheit unterscheidet man im industriellen Umfeld zwischen Safety, der funktionalen Sicherheit und Security, der Datensicherheit.

Unter dem Thema Safety versteht man die Funktionalitäten, die dem Schutz der Menschen, sowie der Maschinen und Anlagen dienen. Im Notfall muss es möglich sein, einzelne Maschinen, Anlagensegmente oder ganze Anlagenkomplexe in den sicheren Zustand zu überführen. Dazu ist eine unverzügliche und direkte Datenübertragung an die entscheidenden Steuerungselemente notwendig. Die Safety-Signale müssen medienunabhängig und zuverlässig mit höchster Priorität übertragen werden. Wenn Netzwerkabschnitte mit „Not-Halt“-Funktionalität realisiert werden, muss die entsprechende Netzwerkverbindung sichergestellt sein – und dies sowohl bei kabelgebundenen als auch in funkbasierten Netzwerkinfrastrukturen wie Wireless LAN. Um der Bedeutung der Anforderungen im Bereich der Security in industriellen Netzwerken gerecht zu werden, sind u. a. spezielle Zellschutz- und Firewall-Konzepte zu realisieren. Jeder Produktionsbereich muss hierdurch zwingend vor unautorisierten Zugriffen geschützt werden. Insbesondere für die sensiblen Fernzugriffe bedarf es professioneller Security-Konzepte, beispielsweise um Wartungsarbeiten an definierten Anlagenteilen klar geregelt zu gestatten. Aber auch die Versionsverwaltung unterscheidet sich zur typischen Office-IT. Bei industriellen Anlagen sind zur Patch-Einspielung fest geplante Zeitfenster für die Wartung zu nutzen, und Performance-Einbußen für Updates bei laufenden Anlagen sind nicht selten kritisch. So können ungeplante Netzwerk-Scans ganze Anlagen ungewollt zum Stillstand bringen.

Abschließend bleibt festzuhalten, dass für eine ausfallsichere industrielle Anlage ein durchgängiges Netzwerkkonzept auf der Basis einer physikalischen Netzwerktrennung mit einem Anbindungskonzept dringend zu empfehlen ist, das sowohl der Security- als auch der Performance-Anforderung entspricht. Konvergenz-Konzepte, die das industrielle Netzwerk lediglich wie ein weiteres, logisch zu separierendes behandeln oder gar ohne VLAN-Separierung „designed“ werden, sollten seitens der Anwender mit größter Sorge betrachtet werden. Wie in unzähligen industriellen Applikationen nachgewiesen, spielt das Netzwerk als Teil der Automatisierung eine entscheidende Rolle für störungsfreie Abläufe. Eine Planung und Umsetzung auf der Basis der entscheidenden Kriterien stellt den Erfolg der industriellen Unternehmen sicher.

Eigenschaften industrieller Netzwerkkomponenten

- **Erhöhte Anlagenflexibilität und Kosteneinsparung**
Klare Ring- und Liniennetzwerkstrukturen mit Kompaktgeräten an der Anlage schaffen hohe Flexibilität und reduzieren die Kosten für Wartung und Service.
- **Investitionsschutz bestehender Anlagen**
Langfristige Ersatzteilsicherheit, modular erweiterbare Aktivkomponenten sichern den dauerhaften Einsatz bestehender Anlagen.
- **Investitionsschutz zukünftiger Anlagen**
Zukunftssichere Technologien und kontinuierlicher Ausbau verfügbarer Produkte mit durchgängiger Kompatibilität.
- **Optimale Maschinen- und Anlagenverfügbarkeit**
Höchste Zuverlässigkeit der Produkte im Betrieb. Darüber hinaus Service und Support rund um die Uhr (24/7), weltweit.
- **Planungssicherheit und Know-how-Schutz**
Lange Produktlebenszeit und Verfügbarkeit sichern langfristig angelegte Anlagenkonzepte und die Nutzung des Know-hows der Mitarbeiter.
- **Kompatibilität**
Durchgängige Produkte und Zubehör sichern die Integration zusätzlicher Komponenten für Erweiterungen zur kompletten industriellen Infrastruktur.
- **Weltweiter Einsatz**
Industrielle Netzwerkgeräte mit Zulassungen für die Länder weltweit.
- **Entwickelt für unsere Kunden**
Die Entwicklungsprozesse der Komponenten und Services berücksichtigen schon bei der Planung spätere Anwendungen und Lösungen. Damit sind Leistungen stets leicht zu integrieren und umzusetzen, sowie auf die Bedürfnisse der Anwender und Endkunden zugeschnitten.

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

© Siemens AG 2016
Änderungen vorbehalten
PDF
Technischer Fachartikel
FAV-285-2016-PD-PA
BR 022017 De
Produced in Germany

Die Informationen in dieser Broschüre enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden. Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle Erzeugnisbezeichnungen können Marken oder Erzeugnisnamen der Siemens AG oder anderer, zuliefernder Unternehmen sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.