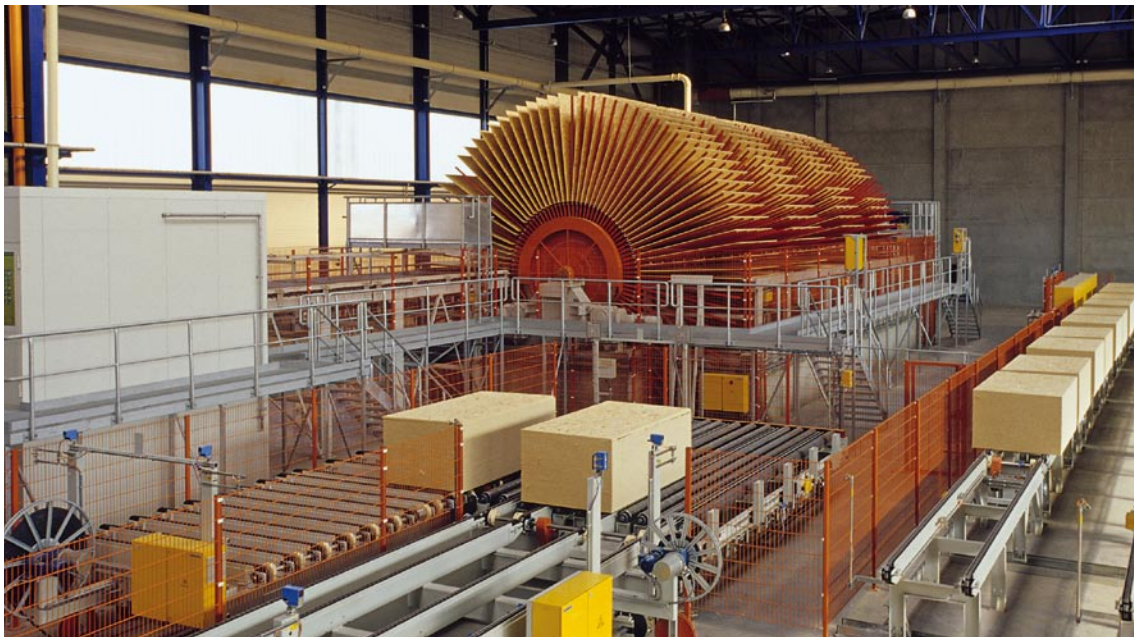


Foto: Dieffenbacher

Fertigungsanlagen werden heute flächendeckend vernetzt. Mit steigendem IT-Einsatz wächst aber auch die Bedeutung der Netzwerksicherheit und -administration.

Kommunizieren leicht gemacht oder versteckte Gefahr?

Auch Automatisierungsnetzwerke brauchen eine professionelle Administration

Ethernet, keine andere Kommunikationstechnik ist derart verbreitet. In den letzten Jahren findet sie zunehmend Verwendung in der Automatisierungstechnik. Mit steigendem IT-Einsatz erhöht sich aber auch die Abhängigkeit von diesen Systemen und das Risiko IT-bedingter Schäden. Umso wichtiger ist der Schutz des Fertigungsnetzes vor Systemausfällen.

Mit der großen Verbreitung von Ethernet sind alle Kommunikationskomponenten extrem preisgünstig geworden. Es gibt zahlreiche Programme, die eine Kopplung über Ethernet als integralen Bestandteil enthalten. Die hohe Datentransferrate garantiert recht kurze Reaktionszeiten und erlaubt die Übertragung größerer Datenmengen in einem kurzen Zeitraum.

Die Vorteile liegen auf der Hand: Es gibt nur noch eine Kommunikationstechnik, sie ist bewährt, verfügbar und preisgünstig. Zudem erleichtert sie den Durchgriff von den oberen Managementhierarchien bis zu den unteren Feldebenen.

Nachteile gab es zunächst keine. IT-Berater lobten den Wegfall von Schnittstellen und berechneten die Ersparnis durch weniger Administrationsaufwand. Man prophezeite den Niedergang der Feldbusvielfalt und pries die Web-Diagnose von Feldgeräten, womöglich über das Internet.

Vernetzen ist so einfach

Dem großen Vorteil einer hohen Geschwindigkeit, kombiniert mit einer einfachen Technologie, steht jedoch oft ein Nachteil gegenüber: Der einfache Aufbau verführt zum Anschluss ungeeigneter oder zu vieler Komponenten und Geräte. Und moderne Switches legen die Vermutung nahe, dass man über Bandbreiten und Kommunikationsressourcen nicht mehr nachdenken muss. Nicht selten werden immer mehr Netzwerkteilnehmer eingebunden oder Kommunikationsverbindungen erweitert, bis das gesamte Netzwerk versagt.

Schichten mit Charakter

Das Zusammenspiel von Geräten und Komponenten und der Fluss von Informationen kann in Form einer Kommunikationspyramide dargestellt werden. Die vertikale Hierarchie repräsentiert eine Funktionseinteilung, die bei der Planung und Konfiguration festgelegt wird.

Die Kommunikationspyramide spiegelt die sehr unterschiedlichen Charaktere der Datenverbindungen wider:

- In der untersten Schicht stellt sie eine hohe Anzahl von kleinen Datenpaketen und strengen zeitlichen Anforderungen dar,
- in der obersten Schicht eine geringere Anzahl von großen Datenpaketen, wobei Reaktionszeiten im Bereich von einigen hundert Millisekunden akzeptabel sind.

Über alle Ebenen hinweg

Wo früher für den jeweiligen Zweck geeignete Systeme eingesetzt wurden, findet man heute die flächendeckende Vernetzung mittels Ethernet. Das klassische Schichtenmodell, das eine Anlage sowohl technisch als auch organisatorisch prägte, ist eingeebnet worden. Der Zwang entfällt, die vertikale Kommunikation bewusst durch jede Schicht zu leiten.

Bekämpfung der Computerkriminalität

Bundestag und Bundesrat haben Mitte 2007 den umstrittenen Paragraphen § 202 c StGB entgegen dem Rat von IT-Experten verabschiedet. Der Paragraph macht den Besitz, die Herstellung und die Verbreitung von präventiven Werkzeugen, mit denen die Sicherheit von Computern geprüft werden kann, in Deutschland strafbar. Diese Werkzeuge sind jedoch wichtig, um die Sicherheit von Computersystemen zu gewährleisten. Auch der Betrieb eines Industrial Ethernet muss laufend abgesichert und überprüft werden. Dazu werden in aller Regel frei verfügbare Software-Werkzeuge eingesetzt, deren Besitz nun strafbar wird.

Kontakt:
Peter Früauf
FV Elektrische Automation
Telefon 0 69 / 66 03-16 44
peter.frueauf@vdma.org

Man wird leicht verführt, die Technik, die man vom heimischen DSL-Anschluss her kennt, quer durch alle Schichten einer Industrieautomatisierung anzuwenden. In den verschiedenen Schichten werden aber sehr unterschiedliche Anforderungen gestellt, beispielsweise an die Verfügbarkeit.

Ähnlich wie in einem modernen Flugzeug, in dem Passenger-Entertainment und Cockpitfunktionen verschiedene Leistungsmerkmale vom Netzwerk abfordern, so sind auch in einer Fertigungslinie Leit- und Prozessebene sehr differenziert zu betrachten.

Die einheitliche Vernetzung bietet große Vorteile, verlangt aber – entgegen dem vordergründigen Anschein – mehr denn je eine sorgfältige Projektierung und Pflege.

Globale und lokale Kommunikation

Ferndiagnose ist unumstritten eine nützliche Einrichtung, insbesondere für Firmen, die ihre Produkte oder Dienstleistungen exportieren. Mancher braucht auch die aktuellen Produktionszahlen auf seinem Blackberry. Beides wird durch Ethernet und IP-basierte Protokolle möglich.

Aber: Derart vernetzte Systeme führen dazu, dass unterschiedlichste Dienste über ein und dasselbe Netzwerk abgewickelt werden: Prozess-Datagramme, E-Mails, OPC-Verbindungen und Webseiten sind nicht mehr auf ihre Schicht begrenzt. Dazu kommen die Intra-Netzwerke großer Konzerne, die oftmals Kontinente verbinden. Es ist leicht einzusehen, dass solche Netzwerke einen Schutz nach außen brauchen: die Firewall zum Internet.

Für jeden Pförtner gibt es eine einfache Auflage: Der Chef darf immer ins Werk, Mitarbeiter haben einen Firmenausweis und Besucher werden angemeldet und abgeholt. Wie aber regelt eine Firewall den Datenverkehr?

Firewalls zum Internet, um beim Beispiel zu bleiben, lassen jeden hinaus und der darf dann andere mitbringen (Trust- versus Untrust-Policy). Bestimmte Personengruppen dürfen aber auch von außen hinein, wenn sie sich nur umsehen wollen (Web-Clients), oder sie haben einen passenden Ausweis bei sich (VPN-Tunnel).

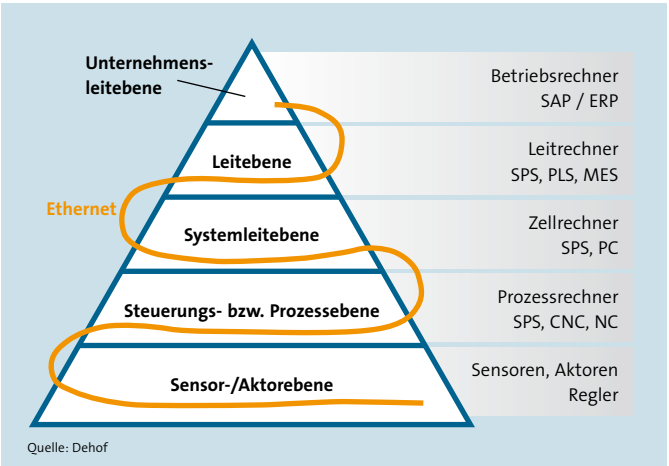
Diese Mechanismen scheinen selbstverständlich, finden aber im Netzwerk oft keine Entsprechung. Sei es aus Unwissenheit, finanziellen Gründen oder weil man das Risiko falsch einschätzt.

Anforderungen der Industrie

Der Betrieb eines „Industrial Ethernet“ muss anderen Anforderungen genügen als der eines Büronetzwerkes. Techniker und Ingenieure ersetzen planbare Systeme und Verbindungen durch ein scheinbar chaotisches Netzwerk – aus diesem Blickwinkel ist Ethernet mit einem latenten Risiko verbunden, irgendwann nicht zu funktionieren.

Auf einem Feldbuskabel existieren nur Feldbusdaten, die angeschlossenen Geräte verarbeiten auch nur diese, und wenn man etwas nicht richtig angeschlossen hat, funktioniert das System auch nicht. Im Umkehrschluss ist man versucht zu meinen, dass ein funktionierender Feldbus bedeutet, man hätte alles richtig gemacht. Es gibt Bandbreiten und Lastdaten, die sich bestimmen und kontrollieren lassen.

Ein Ethernet ist mit den Planungswerkzeugen, die heute vom Anlagenbau verwendet werden, eigentlich nicht zu konstruieren: Ein funktionierendes Ethernet bedeutet nämlich nicht, dass man alles richtig gemacht hat. Die Auslastung beziehungsweise verfügbaren ▶



Quelle: Dehof

Die Kommunikationspyramide spiegelt die sehr unterschiedlichen Charaktere der Datenverbindungen wider.

Reserven sind nur schwer zu bestimmen. Werkzeuge, die dem Produktionspersonal vertraut sind, bieten für Ethernet nur wenig Unterstützung, und der professionelle Umgang mit IT-Software ist weitgehend unbekannt.

Der sichere Betrieb eines „Industrial Ethernet“ stellt den Maschinenbau vor neue Aufgaben:

- Es werden einfache Werkzeuge benötigt, mit denen man bestehende Netze analysieren kann.
- Die Administration und der operative Betreiber müssen eng zusammenarbeiten.
- Hersteller müssen die Netzwerkeigenschaften ihrer Geräte offenlegen.
- Kommunikationsbeziehungen müssen dokumentiert und gesteuert werden.

Foto: Dieffenbacher

Wie sollte der Maschinenbauer mit seinem Anlagennetzwerk umgehen? Antworten dazu am 8. November im VDMA-Haus (siehe Kasten unten).

Lösungsansätze

Es gibt mittlerweile viele gute Ratschläge zum richtigen Aufbau eines Netzwerkes – diese funktionieren überwiegend bei komplett neuen Netzwerken oder bei abgeschlossenen Systemen. Die meisten Netzwerke sind aber gewachsen und unterliegen einem ständigen Wandel.

Die Infrastruktur eines Netzwerkes zu analysieren ist derzeit technisch nicht vollständig möglich. Warum unterstützen nicht einfach alle Industriegeräte LLDP – ein neutrales Protokoll, mit dem Geräte ihre Identität mitteilen? Das wäre oft sinnvoller als ein Webserver, den man erst dann verwenden kann, wenn man bereits weiß, dass es dieses Gerät gibt.

Das Outsourcen von IT-Administration führt in der Produktion oft dazu, dass Netzwerksicherheit nicht ausreichend existiert. Wenn hier Fachabteilungen eng zusammenarbeiten, entstehen meist technisch sinnvolle und kostengünstige Lösungen.

Ähnlich dem Typenschild eines Elektromotors sollten Hersteller von Netzwerkgeräten diese dokumentieren. Der Security and Administration in Industrial Ethernet e.V. (SecIE) schlägt beispielsweise ein neutrales „Security-Datenblatt“ vor, das relevante Informationen über das Produkt enthält und den Kunden in die Lage versetzt, entsprechend zu handeln.

› FuI-49

Dr. Peter Wratil
ist Geschäftsführer der innotec GmbH und Experte für Sicherheit in der Automation, Rosengarten.

Matthias Dehof
ist Vorstand des Security and Administration in Industrial Ethernet e.V. (SecIE), Magdeburg, und Geschäftsführer der DEHOF ingenieur+technik GbR, Mannheim.

Ulf Könekamp
ist Entwicklungsleiter Elektrik im Geschäftsbereich Holzplattentechnik der Dieffenbacher GmbH + Co. KG, Eppingen.

Ihr VDMA-Ansprechpartner zum Thema:
Birgit Sellmaier
FV Elektrische Automation
Telefon 0 69 / 66 03-16 70
birgit.sellmaier@vdma.org

3. VDMA-Technik-Benchmark Security

Sechs IT-Konzepte für Automatisierungsnetzwerke am 8. November 2007 im VDMA-Haus, Frankfurt am Main

Wie sollte der Maschinenbauer bei Engineering, Wartung und Umbau mit „seinem“ Anlagennetzwerk umgehen? Welche Regeln sollte er zum Betrieb und zur Pflege aufstellen? Das sind in der Praxis Graubereiche, zu denen der Maschinenbauer nur schwer echte Ansprechpartner findet.

Die Veranstaltung zeigt mehrere Lösungswege zu einer vorgegebenen Aufgabenstellung: Eine bestehende Dieffenbacher Spanplattenanlage soll erweitert werden. Hauptaspekte sind die IT-Administration und der Umgang mit dem „gewachsenen“ Netzwerk.

Dazu haben sechs Anbieter aus den Bereichen Steuerungstechnik, Visualisierung, ERP-Anbindung jeweils ein Konzept entwickelt und stellen es im VDMA zur Diskussion. Unabhängige Automatisierungsexperten werten und diskutieren mit den Teilnehmern die vorgestellten Lösungsansätze.

Teilnehmer
Die Veranstaltung richtet sich an Interessenten aus Planung, Projektierung, Inbetriebnahme oder Wartung von Automatisierungsnetzwerken im Maschinen- und Anlagenbau.

Teilnahmegebühr
VDMA-Mitglieder: 95,– € +19 % MwSt.
Nichtmitglieder: 190,– € +19 % MwSt.

Kontakt:
Birgit Sellmaier
FV Elektrische Automation
Telefon 0 69 / 66 03-16 70
birgit.sellmaier@vdma.org

www
Weitere Informationen unter:
www.vdma.org/ea