



Foto: Koerbig & Bauer

Kostspielige Service-Einsätze vor Ort können durch einen leistungsfähigen Teleservice minimiert und optimal vorbereitet werden.

Reif für den Abschied von der Insel

Sicherheit und Effizienz bei Vernetzung und Teleservice von Maschinen und Anlagen

Die einsame Insel war gestern: Heute sieht sich der Maschinen- und Anlagenbau regelmäßig mit der Anforderung konfrontiert, seine Produkte in Netzwerke seiner Kunden zu integrieren. Eine durchgängige Daten- und Prozessintegration auf Basis von Ethernet und TCP/IP soll den nächsten Produktivitätsschub bringen. Aber bitte mit Sicherheit, versteht sich.

Bei der Integration von Maschinen in ein BetreiberNetz spielen verschiedene Aspekte eine Rolle: Soll die Einbindung flach und direkt oder mit Netzsegmentierung und Routing erfolgen? Sollen Kommunikationsverbindungen nur vom Maschinennetz ins BetreiberNetz aufgebaut werden oder auch umgekehrt? Und vor allem der Umfang des Maschinennetzes: Ist es nur ein einzelner IP-Knoten, zum Beispiel Bedienrechner oder Steuerung eines kleineren Systems, fällt die Adressanpassung an das Kundennetz leicht. Nutzt die Maschine hingegen ein ganzes IP-Subnetz für ihre interne Kommunikationsstruktur, sind Anpassungen der IP-Adressstruktur meist aufwendig und möglichst zu vermeiden. Ein häufiger Spezialfall ist die Aufgabe, mehrere solcher Maschinen mit herstellereitig identischem internem Netz in dasselbe BetreiberNetz zu integrieren.

Wer hat Angst vor wem und wovor?

Spätestens auf den zweiten Blick wird aber klar, dass einer unmittelbaren Anbindung von Maschinen an ein BetreiberNetz selbst in Fällen, wo dies IP-technisch einfach möglich wäre, berechtigte Bedenken aller Beteiligten entgegenstehen. Sorgen sich sowohl der Hersteller, dass schädliche Einflüsse aus dem BetreiberNetz den störungsfreien Betrieb seiner Maschine, den er gewährleisten muss, als auch umgekehrt der Betreiber, dass das Verhalten der Maschine andere Systeme in seinem Netz beeinträchtigen könnte. Und ist auch noch eine Teleservice-Verbindung im Spiel: Wie stellt man dann eigentlich sicher, dass der Zugriff darüber auf das definierte Zielsystem beschränkt bleibt und keinen weiteren Durchgriff ins BetreiberNetz erlaubt?

Die relevanten Bedrohungen gehen dabei nicht von spektakulären Hacker-

Angriffen aus, sondern sind meist banaler, alltäglicher Natur: Die Ausbreitung von Schadsoftware, unbefugte Zugriffe, Fehlkonfigurationen und die Überlastung von Netz oder Komponenten zählen zu den üblichen Verdächtigen.

Lösung: Network Security Appliances

Wirksamste Abhilfe ist die Beschränkung der zulässigen Kommunikation mit kritischen Maschinen- oder Anlagen-Teilen (Zellen) auf das operativ erforderliche Maß. Möglich ist dies durch den Einsatz dezentraler Firewalls mit geeignetem Regelwerk, das entweder aus der System-Dokumentation abgeleitet oder aus einer Lernphase direkt am Netz gewonnen werden kann. Oberste Maxime: Was nicht explizit erlaubt ist, ist verboten!

Leistungsfähige industrielle Network Security Appliances verbinden die flexible Einbindung von Maschinen und Anlagen in ein BetreiberNetz mit der Lösung der genannten Sicherheits- und Firewall-Aufgaben in einem autonomen, vom zu schützenden System unabhängigen Gerät. Sie unterstützen dabei sowohl eine IP-technisch transparente flache Einbindung (in sogenannten Stealth Modes) als auch die Netzwerksegmentierung per Firewall Router mit NAT oder 1:1 NAT-Funktionalität (Network Address Translation). Letztere löst ebenso effizient wie elegant durch Abbildung auf eindeutige virtuelle Netze auch den genannten Spezialfall der Einbindung mehrerer Systeme mit identischem internem Netz.

Teleservice unter Quarantäne

Interessanterweise können die gleichen Appliances auch noch dafür genutzt werden, sichere, vom Betreiber kontrollierbare Teleservice-Verbindungen zu etablieren. Dabei werden VPN-(Virtual-Private-Network-)Verbindungen von den Maschinen zum jeweiligen Service Center, also aus dem BetreiberNetz ausgehend aufgebaut, was diese einfach und dennoch sicher administrierbar macht. Gleichzeitig sorgt die integrierte Firewall dafür, dass der Teleservice keinen Durchgriff über das Maschinennetz ins BetreiberNetz erhält. Werden dann noch zentral betriebene



Im Profil

Innominate Security Technologies AG, Berlin

Der deutsche Security-Spezialist stellt Embedded-Network-Security-Lösungen für industrielle Anwendungen her und ist in den Geschäftsfeldern „Industrial Ethernet Security“ und „Secure Remote Maintenance“ für Maschinen und Anlagen tätig. Innominate-Hardware bietet Firewall-, VPN- und Virenschutz-Funktionalitäten. mGuard-Lösungen werden über OEM-(Original-Equipment-Manufacturer)-Partner wie Phoenix Contact GmbH & Co. KG, Blomberg, und über ein internationales Netzwerk von Distributoren (in Deutschland: TLK) und Resellern vertrieben.

www.innominate.de

und sauber gepflegte Virtuelle Maschinen (VM) als Service-Arbeitsplätze eingesetzt und so direkte IP-Verbindungen zwischen Techniker-PC und Maschinen vermieden, findet Fernwartung wie unter Quarantäne-Bedingungen statt – Infektion auch jenseits der einsamen Insel ausgeschlossen.

Erfahrungen aus Druck und Papier

Die Koenig & Bauer AG (KBA), Würzburg, einer der weltweit größten Hersteller von Druckanlagen, hat das Potenzial gesicherter Internet-Fernwartung frühzeitig erkannt. In Technologie-Kooperation mit der Innominate Security Technologies AG, Berlin, wurden von KBA seit Anfang 2007 circa 100 Druckmaschinen in allen Regionen der Welt mit der „mGuard Security Appliances“ ausgerüstet und über diese an das KBA Teleservice Center angebunden. Da-

bei weiß man inzwischen sowohl die Stabilität und Verlässlichkeit der VPN-Verbindungen als auch die Effizienz bei Roll-out und Administration der Geräte durch den zentralen Innominate Device Manager zu schätzen. Ein weiterer führender Anbieter der Branche, die Winkler+Dünnebieber AG, wird auf der Drupa im Mai 2008 seine neue mGuard-basierte Lösung für Netzwerk-Integration und Internet-Teleservice von Papier verarbeitenden Maschinen präsentieren. Die mGuard-Technologie selbst ist dabei völlig branchenneutral und wird auch bereits von Kunden aus etlichen anderen Zweigen des Maschinenbaus erfolgreich eingesetzt. > Bp-39

Autor:

Torsten Rössel

ist Director Business Development der Innominate Security Technologies AG, Berlin.

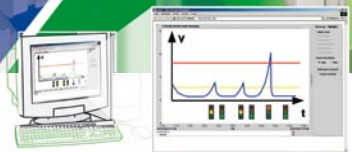
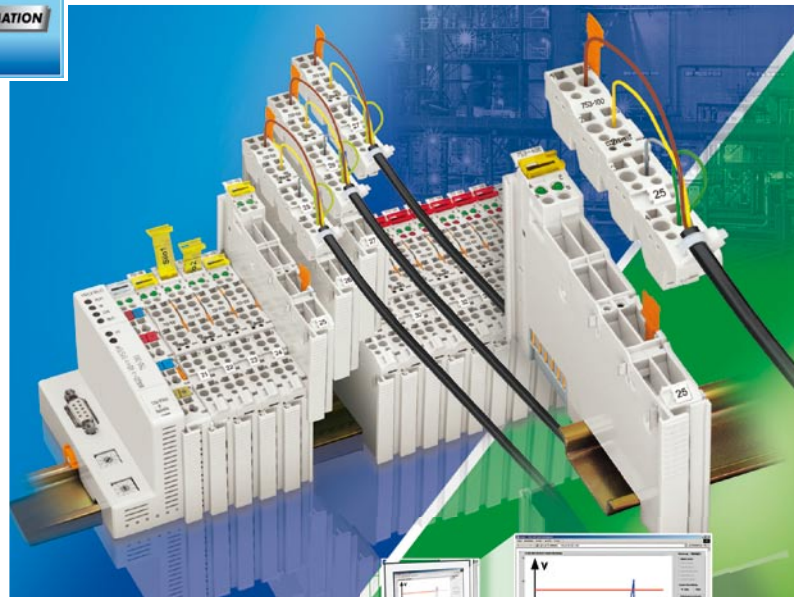
Anzeige

„Maschinengesundheit“ einfach überwachen – feldbusunabhängig!

Condition Monitoring mit WAGO: Schwingungs-, Strom- und Temperaturmessklemmen

- Schwinggeschwindigkeitsmessung (RMS) nach ISO 10816-3
- Stoßimpulsmessung (SPM) zur Wälzlagerüberwachung
- Vorverarbeitung in der Klemme
- Konfigurierbare Alarm- und Warnschwellen
- Direkte Ansteuerung der Alarmausgänge
- Tandem Piezo Sensoren
- Strommessklemmen 0-1/5A, 0/4-20mA
- 3-Phasenmessklemmen
- Temperaturmessklemmen (RTD, Thermoelemente)

www.wago.com



WAGO[®]
INNOVATIVE CONNECTIONS