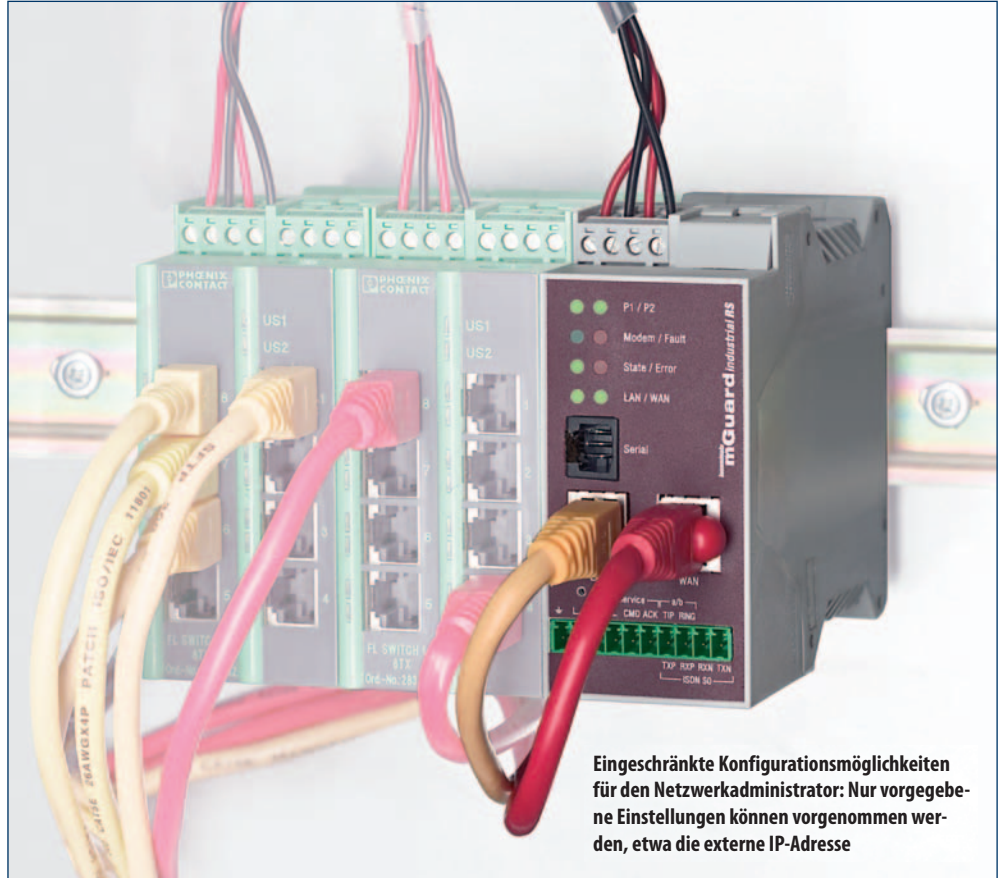


# Rechtmanagement

Integration von Security-Appliances durch gezielte Konfiguration „vor Ort“

Zugänge für Teleservice erfolgen zunehmend über VPN-Appliances, Zugänge zu Maschinen und Fertigungszellen werden durch Firewalls abgesichert. Der Maschinen- oder Anlagenbauer muss dabei die Appliance bereitstellen, gleichzeitig muss der Betreiber die Anbindung an sein Werksnetz konfigurieren. Durch ein flexibles Rechtmanagement auf der Appliance werden dabei Sicherheits- und Zuverlässigkeitsaspekte berücksichtigt. ■ Lutz Jänicke



Eingeschränkte Konfigurationsmöglichkeiten für den Netzwerkadministrator: Nur vorgegebene Einstellungen können vorgenommen werden, etwa die externe IP-Adresse

**M**it der Vernetzung von Maschinen sind Schutzmaßnahmen gegen versehentliche Fehlbedienung, Ausbreitung von Würmern, Trojanern und Viren erforderlich, ebenso gegen Industriespionage und Sabotage. Während die Office-IT weitgehend aus einer Hand kommt, sind in der Fabrikhalle meist verschiedene Parteien beteiligt: Die Fertigungs-IT, die Automatisierungstechnik und die Zulieferer. Die Umsetzung einer IT-Security-Policy muss daher einen kooperativen Ansatz verfolgen.

Die Vernetzung ist kein Selbstzweck, sondern dient der vertikalen Integration: Die Fertigung soll überwacht- und steuerbar sein. Die Kommunikationswege reichen aus der zentralen IT bis hinunter an einzelne Fertigungssysteme und greifen durch viele Verantwortungsbereiche hindurch. Zentrale Systeme wie ERP laufen im Rechenzentrum eines Unternehmens und sind damit in der Verantwortung der IT angesiedelt. Von der Klimatisierung bis zur Security-Policy ist hier alles geplant und in der Praxis erprobt. Das Zusammenspiel mit der Office-Umgebung

ist ebenso ausgereift. Dabei gilt das Prinzip der Homogenität, bei dem gleiche Konfigurationen auf möglichst identischer Hardware laufen.

In der Fertigung dient die Vernetzung der Bereitstellung von Kommunikationsverbindungen. Zumeist sind es Verbindungen zur Archivierung von Produktionsdaten, für Backups oder zur Fertigungssteuerung. Ziel der Fertigungs-IT ist die Bereitstellung der notwendigen Infrastruktur. Typischerweise ist die IT-Landschaft in der Fertigung durch Inhomogenität geprägt, in der Office-IT etablierte Prozesse greifen nicht: In der Fertigung ist es notwendig, Servicetechnikern von Maschinen- und Anlagenbauern Netzwerkzugang zu gewähren, um bei Problemen Diagnosemöglichkeiten zu haben. An der Schnittstelle zur zentralen IT sind die Zuständigkeiten nicht immer eindeutig geregelt. Die für den Fertigungsschritt notwendigen Kommunikationsbeziehungen sind meist intern und unterliegen zum Teil besonderen Echtzeitanforderungen. Eine Fertigungszelle oder Maschine ist daher



**Dr. Lutz Jänicke**  
Chief Technology Officer (CTO) bei der Innominat  
Security Technologies AG in Berlin  
T +49/30/6392-3300  
ljaenicke@innominate.com

als in sich geschlossenes Gebilde zu verstehen, zu der nur genau spezifizierte Zugänge erlaubt sein sollten. Am Übergang zwischen Zelle und Fertigungsnetz besteht auch ein Übergang in der Verantwortung für die IT.

Die Übergabe der Verantwortung lässt sich mit einer Security-Appliance abbilden, die differenzierte Administrationsrechte in einem Rollenmodell bietet: Der Verantwortliche für die Fertigungszelle hat die Hauptrechte für die Administration. Er kann die Policies konfigurieren und nur den notwendigen Zugriff in die Zelle freigeben. Andererseits kann er nicht alle Spezifika der jeweiligen Installation kennen. Diese Einstellungen, etwa IP-Adressen, lässt er offen und erlaubt dem Netzwerkadministrator die Konfiguration. Der hat die Kontrolle über die Zugriffsrechte: Er gibt die Zugänge für Netzwerkadministrator und Auditor frei und entscheidet, welche Einstellungen der Netzwerkadministrator vornehmen darf. Der Netzwerkadministrator ist eine Rolle der Fertigungs-IT. Er kann nur diejenigen Einstellungen ändern, die vom Administrator dafür freigegeben wurden. Dies könnten eventuell nur wenige IP-Adresseinstellungen sein, möglicherweise aber auch zusätzliche Firewallregeln. Der Auditor hat vollen lesenden Zugriff auf die Appliance und kann alle Einstellungen mit Ausnahme privater Daten überprüfen

und die Übereinstimmung mit der Security-Policy bestätigen.

Fernwartungszugänge sind ein leistungsfähiges Mittel zur Reduktion von Ausfallzeiten und Servicekosten. Gleichzeitig gestatten sie Zugriff auf Systeme im abgeschotteten Fertigungsnetz. Dabei sind nicht nur Zugriffe auf das eigentliche Zielsystem, sondern weitergehende Verbindungen vom Zielsystem auf das restliche Fertigungsnetz möglich. Klassische Fernwartungsansätze über Modem bieten hier keine Lösung. Die Modems sind typischerweise mit dem Steuerungsrechner einer Zelle verbunden, der selbst am Fertigungsnetz angekoppelt ist. Oft wird die Fernwartungs-Security daher über die Telefonsteckdose realisiert: Nur im Fernwartungsfall wird das Modemkabel eingesteckt.

Neue Internet-Fernwartungslösungen setzen auf Virtual Private Networks (VPN) mit starker Authentifizierung und abhörsichere, verschlüsselte Verbindungen. Je nach Modell sind VPN-Tunnel zwecks Zustandsüberwachung ständig aktiv oder werden nur bei Bedarf im Servicefall aufgebaut. Bei der Fernwartung über IP kann wiederum die Verwendung einer Security-Appliance mit Rollenmodell das Vertrauensverhältnis zwischen Betreiber und Anlagenbauer unterstützen. Mehr noch als bei einer reinen Security-Anwendung sind auf der Appliance schützenswer-

te Informationen gespeichert. Der Aufbau eines VPN-Tunnels zum Gateway des Anlagenbauers erfordert eine starke Authentifizierung unter Verwendung privater Schlüssel. Diese werden vom Anlagenbauer bei der Auslieferung oder Inbetriebnahme aufgebracht und müssen vor fremdem Zugriff geschützt werden. Nur der Administrator auf Seiten des Anlagenbauers darf daher diese Schlüssel aufbringen und abrufen können. Er konfiguriert die VPN-Tunnel entsprechend des Service-Konzepts. Der Netzwerkadministrator sollte grundsätzlich auf die Einstellungen zur Authentifizierung keinen Einfluss nehmen dürfen, private Schlüssel dürfen für ihn nicht einsehbar sein. Im Rahmen der Funktionsüberwachung darf der Netzwerkadministrator aber die Tunnelstatus abfragen. Der Auditor darf alle Daten mit Ausnahme der privaten Schlüsselinformationen einsehen. Er kann so auch die Einstellungen des VPN-Zugangs bewerten.

Die Umsetzung einer Security-Policy auch an den Übergabepunkten zwischen den Verantwortungsbereichen erfordert eine technische Lösung, die den unterschiedlichen Verantwortungen durch ein geeignetes Rollenmodell gerecht wird. ■

Weiterführende Infos auf [AuD24.net](http://AuD24.net):

**more @ click** AD029303

## SERIAL CONNECTIVITY

## INDUSTRIAL ETHERNET

## EMBEDDED COMPUTING

## WIRELESS & CELLULAR

# INNOVATION

## Active Ethernet I/O – die Komplettlösung von der Alarm- bis zur Kommunikationsebene.

Mit **Active Ethernet I/O** ermöglicht Moxas **ioLogik Serie** die ereignisgetriebene Abfrage und Überwachung für:

- Intelligente Transportsysteme (Schienenverkehr, Verkehrsleitsysteme)
- Sicherheits- und Überwachungssysteme (Alarmanlagen, Einbruchserkennung)
- Energiewirtschaft (Umweltüberwachungssysteme)
- Fabrikautomation (Durchflusskontrolle, Füllstandsanzeige)



**ioLogik E2262:**  
Active Ethernet I/O mit 8 Thermoelement-Inputs und 4 DOs  
Direkter Thermoelemente-Input mit 16-Bit Digitalwert für  
J, K, T, E, R, S, B, N und mV Sensoren.

## MOXA. INDUSTRIAL NETWORKING SOLUTIONS.