

## Damit nicht der Wurm im System steckt

In vielen Bereichen der industriellen Kommunikation haben in den letzten Jahren Netzwerkstandards aus dem Büroumfeld wie TCP/IP, Ethernet oder HTTP Einzug gehalten. Damit bietet sich das Internet als zentrales Medium für Fernwartung, -überwachung und -wirken auch im Umfeld der Automatisierungstechnik an. Firewall- und VPN-Systeme helfen, die Nutzung des Internets sicher zu gestalten und teure Punkt-zu-Punkt Verbindungen abzulösen. Sicherheitslösungen aus dem Bürobereich lassen sich dafür aber nur bedingt nutzen. Security Appliances für den industriellen Einsatz schließen nun diese Lücke und ermöglichen eine sichere Übertragung bis hin zum einzelnen Automatisierungsgerät. Der Schutz vor dem unbeabsichtigten Einschleppen von Viren und Würmern spielt dabei eine ebenso große Rolle.

Bei klassischen Automatisierungsanwendungen handelte es sich bisher vor allem um Inselösungen mit sehr speziellen Aufgaben und einem örtlich begrenzten Einsatzgebiet. In jüngerer Zeit werden aber die offenen Kommunikationsstandards Ethernet, TCP/IP und HTTP auch für industrielle Anwendungen relevant und ermöglichen die umfassende Vernetzung vieler Komponenten und Systeme. Proprietäre Kommunikationsmethoden wie Feldbussysteme und Remote-Access-Lösungen werden zunehmend durch die offenen Standards verdrängt. Die geringeren Kosten für Standardkomponenten und für den Datenaustausch über das Internet spielen eine wichtige Rolle für den Siegeszug von TCP/IP in der Automatisierung. Der Trend zu offenen Kommunikationsstandards wird durch die Verbreitung von Standard-Betriebssystemen wie Windows Embedded und Embedded Linux weiter befördert. Die zunehmende Vernetzung über TCP/IP erlaubt immer komplexere, stärker vernetzte und interaktivere Lösungen.

Der schon heute in der Automatisierung weit verbreitete Bedienungszugang für viele Geräte über Internet-Browser und HTTP/HTTPS wird erst durch die durchgängige Nutzung von TCP/IP möglich. Dies führt zunehmend zu Automationsanwendungen, deren einzelne Funktionen örtlich weit verteilt sein können. Ein Beispiel ist die örtliche Trennung der Über-

wachung und Steuerung insbesondere von kleineren Anlagen: Eine zentrale Steuerung ist dann für mehrere dezentrale Anlagen zuständig. Die steigende Komplexität industrieller Systeme und der hohe Wertschöpfungsgrad durch Software-Anwendungen erfordern die Möglichkeit des schnellen Zugriffs von außen, um beispielsweise Sicherheits-Patches einspielen zu können. Die Fernüberwachung industrieller Prozesse über das Inter-



**Das Internet wird auch zunehmend für die Fernwartung und -überwachung von Maschinen und Anlagen eingesetzt**

### PRAXIS PLUS

Mit dem Innominate mGuard industrial ist eine Sicherheits-Komplettlösung erhältlich, die speziell für den Einsatz im Produktionsumfeld konzipiert ist: Das Gerät ist eine professionelle Hardware-Firewall, die auf DIN-Hutschienen montiert werden kann. Es schützt Einzelsysteme oder funktionelle Gruppen im industriellen Ethernet vor Angriffen von außen und vor unberechtigten Zugriffen von innen. Zudem wird optional einen umfassender Virenschutz geboten.

net ist in vielen Bereichen schon heute Realität. Dies gilt auch für die Überwachung oder Ablesung örtlich entfernter Systeme mittels drahtloser Kommunikation über GPRS.

### Neue Möglichkeiten – neue Gefahren

Bei all diesen neuen Möglichkeiten kommt das Thema Sicherheit oft zu kurz. Industrielle Anwender ignorieren die Gefahren, die die durchgehende Vernetzung über das Internet mit sich bringt. Und dies, obwohl die Sicherheitsrisiken größtenteils wohlbekannt und in vielen Fällen offensichtlich sind: Der gezielte Angriff über das Internet und die Ausspähung vertraulicher Kommunikation bei der Nutzung öffentlicher Netze wie Internet beziehungsweise GPRS sind nur zwei Beispiele dafür.

Darüber hinaus spielt auch die Gefahr der Einschleppung von Würmern und Viren beispielsweise über eine Fernwartungsanwendung eine wichtige Rolle. Würmer haben bereits ganze Fertigungsstraßen lahm gelegt oder sogar die Notabschaltung von Kraftwerken blockiert, weil Schadprogramme die Grenze vom Büro- in das industrielle Netzwerk übersprungen haben. Die Tatsache, dass Windows Embedded mittlerweile einen immer größeren Marktanteil im Bereich der Automatisierungstechnik erringt, verschärft die Problematik zusätzlich. Für die Fernwartung bedarf es Mechanismen, die zwar berechtigten Personen Zugang zu einer Maschine gewähren, andererseits aber auch verhindern können, dass ein Servicetechniker von dieser Maschine aus auf



**mGuard  
bladepack zur  
Absicherung  
einer großen  
Zahl ver-  
schlüsselter  
Übertra-  
gungskanäle**



**Industrielle  
Security Ap-  
pliance er-  
möglicht si-  
chere Fern-  
wartung**

weitere Systeme in einem Automatisierungsnetz gelangt. Dabei geht es nicht nur darum, den absichtlichen Missbrauch zu unterbinden. Versehen oder Zahlendreher bei Netzwerkadressen haben bereits dazu geführt, dass ein Techniker einen ganz anderen Roboter bedient hat, als er dachte.

## Firewall und Virenschutz für industrielle Anwendungen

Mittlerweile gibt es einige industrielle Security Appliances, die den Datenverkehr auch in den geschilderten Situationen absichern. Die Appliance mGuard industrial von Innominate kombiniert umfassende Sicherheitstechnologien wie die Trennung von erwünschtem und nicht erwünschtem Datenverkehr (Firewall), die sichere und vertrauliche Kommunikation über Virtual Private Network-Verbindungen (VPN) und Virenschutz mit einer besonderen Tauglichkeit für industrielle Anwendungen, indem relevante Industriestandards, die Möglichkeit der Hutschienenmontage und eine einfache Bedienbarkeit geboten wird. Der mGuard industrial lässt sich durch den „Stealth Mode“ außerdem in ein vorhandenes Netzwerk einfügen, ohne dass die Netzwerkeinstellungen oder die Netzwerktopologie geändert werden müssen. Sind solche Sicherheitsstrukturen erst einmal installiert, können bedenkenlos einzelne Systeme über DSL direkt an Fernwartungs- und Fernwirkanwendungen angeschlossen, oder Automatisierungsgeräte in einem größeren Netz

durch einen sicheren Tunnel über das Intranet erreicht werden. Wartungstechniker können nun über das Internet die Fernwartung eines Systems bei einem Kunden durchführen, ohne dass die Gefahr der Ausspähung, des Angriffs oder des Missbrauchs durch den Wartungstechniker be-

steht. Die sichere Datenübertragung kann über die gebräuchlichen Standards IPsec oder über das speziell für die Fernwartung entwickelte Protokoll SSH realisiert werden.

Das GPRS-Modem Tainy Gmod-V2-IO von Dr. Neuhaus Telekommunikation kombiniert die Nutzung vom Paketdatenfunk mittels GPRS mit den Sicherheits-Funktionen von Innominate in einem industriellen Gerät für die Hutschiene. Damit lassen sich Telematik-Anwendungen über GPRS realisieren, ohne Kompromisse bei der Sicherheit machen zu müssen. Die gute Netzabdeckung und die günstigen Tarife ma-



**Hutschienen GPRS-Modem  
von Dr. Neuhaus in Koope-  
ration mit Innominate**

chen GPRS dabei nicht nur zum Ersatz für Punkt-zu-Punkt Verbindungen, sondern in vielen Fällen auch zu einer interessanten Alternative zu leitungsgebundener Kommunikation.

### **eA-INFO-TIPP**

*Aktuelle Warnungen und Hinweise zu Viren und Würmern sowie Internetsicherheit bietet die Website des Bundesamtes für Sicherheit in der Informationstechnik:*

· [www.bsi.de](http://www.bsi.de)

*Einen Überblick über die Produkte von Dr. Neuhaus finden Sie unter:*

· [www.neuhaus.de](http://www.neuhaus.de)