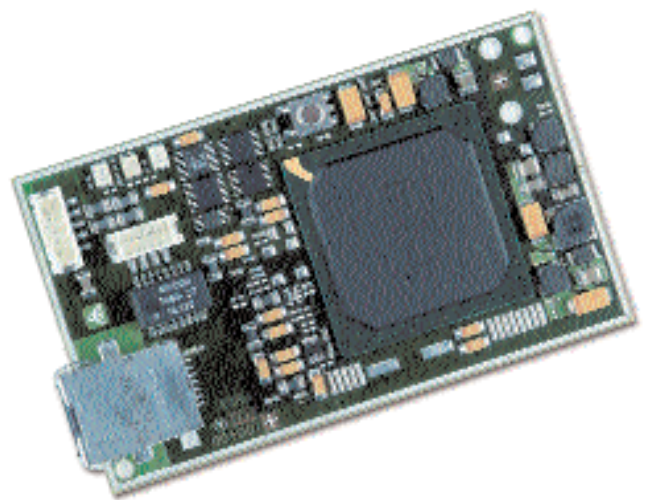


# Security: Firewall- und VPN für Industrial Ethernet



*Bild 1: Auf einer Platine liegt das gesamte Know-how für die Installation von Security-Applikationen im Umfeld von Industrial Ethernet.*



*Halle 6, Stand 255*

**Wer Ethernetnetzwerke bis auf die Feldebene in seinem Betrieb installiert, muss damit rechnen, dass die neuen Kommunikationsmöglichkeiten auch neue Gefahren mit sich bringen, etwa der Angriff von Viren und Würmern aus der Internetwelt. Inzwischen gibt es eine Lösung, mit der man klassische Sicherheitsanwendungen auch bei der industriellen Kommunikation installieren kann.**

**D**ie Standards Ethernet und TCP/IP, die sich in der Büro-Kommunikationswelt bewährt und etabliert haben, halten zunehmend Einzug im industriellen Umfeld und in der industriellen Automatisierungslandschaft. Sie werden immer häufiger als Ersatz oder als Ergänzung zu etablierten Feldbussystemen eingesetzt. Mit dieser Verbreitung von TCP/IP und Ethernet im Bereich der Automatisierung werden die industriellen Anwender mit den Sicherheitsproblemen konfrontiert, denen sich Büroan-

wender schon lange ausgesetzt sahen. Durch das Verschmelzen der Office- und Produktionsnetze muss eine Sicherheitslösung Anforderungen aus beiden Netzwerkwelten erfüllen. Die Innominate Security Technologies AG bietet basierend auf dem Security Modul Innominate mGuard OEM-Lösungen für den Schutz vor Gefahren, Angriffen und Fehlbedienungen aus dem Inter- und Intranet an, um so Schaden durch Viren und Würmer für Maschinen und Produktionszellen zu vermeiden. Der mGuard ist geeignet, um als Sicherheitschnittstelle zwischen der Produktion und dem Office-Netz betrieben zu werden. Das Security Modul mGuard ist mit 20x56x95 Millimetern eine kleine Security Appliance und basiert auf der Kommunikationsprozessorfamilie IXP42x von Intel, die aufgrund ihrer Eigenschaften für Embedded Security und Kommunikationsaufgaben geeignet sind. Der mGuard kommt ohne Lüfter oder andere bewegliche Teile aus, woraus eine hohe Mean Time Before Failure (MTBF) resultiert. Die auf Linux basierende Software bietet außer Firewall- und VPN-Funktionalität mit hardwareunterstützter Verschlüsselung auch optionalen Virenschutz sowie Serverdienste, wie DHCP und DNS. Durch Nutzung dieser offenen Standards kann die Software an verschiedene projekt- und branchenspezifische Anforderungen angepasst werden.

## Sicherheit als Prozess

Eine reale Bedrohung für den Betrieb eines IP-basierenden Produktionsnetzes stellen Viren und Würmer dar. Diese Bedrohung besteht neben den bekannten Schadenswirkungen auf vorhandenen Daten und Programmen vor allem auch darin, dass zusätzliche Verkehrslasten erzeugt werden, die durch das Automatisierungssystem verarbeitet werden müssen und die im ungünstigsten Fall das Echtzeitverhalten eines Systems verändern. Der Innominate mGuard kann so konfiguriert werden, dass nur autorisierte Verbindungen entgegengenommen werden. So entsteht ein Schutz vor schädlichem Netzwerkverkehr. Die freikonfigurierbare Stateful Inspection Firewall mit der neuesten Stealth-Technologie eignet sich für den Schutz einzelner Maschinen oder Produktionszellen, lässt sich aber auch in Industrieprodukte und Geräte der Automatisierungstechnik einbauen. Die Konfiguration ist einfach gehalten. Absender- und Empfängeradressen, Netze und IP-Adressen lassen sich einfach angeben. Der mGuard unterstützt hierbei unter anderem

die Protokolle UDP, TCP und ICMP. Durch Network Address Translation (NAT) kann man verschiedenste Maschinen hinter einer einzigen IP-Adresse anbinden.

## Betriebsmodi

Der mGuard kann in den zwei Betriebsmodi Stealth- und Router-Modus arbeiten: Der "Stealth-Mode" ermöglicht die Integration in bestehende Netzwerkstrukturen ohne Konfigurationsänderungen an dahinterliegenden Maschinen vorzunehmen. Der mGuard wird einfach in den bestehenden Datenstrom der zu schützenden Maschine geschaltet. Eingehende Verbindungen können gesperrt und nur autorisierte, ausgehende Verbindungen sind erlaubt. Teile dieser Lösung, wie z.B. die Möglichkeit aus dem Stealth-Mode heraus transparent einen VPN Tunnel aufzubauen, sind von Innominate patentiert. Im Router-Modus stellt sich der mGuard als Standard-Gateway zum unsicheren Netzwerk dar und erlaubt den Anschluss einzelner Maschinen oder grosser Produktionszellen. Die Hardware unterstützt Verschlüsselung mit 3DES und AES mit bis zu 75MBit/s Datendurchsatz. Dies wird über IPSec mittels X.509 Zertifikate oder Pre-Shared Secrets realisiert.

## Konfiguration

Konfiguriert wird der mGuard durch eine sichere SSL-Verbindung via Internet-Browser lokal aber auch remote über eine einfache Administrationsoberfläche. Hier lässt sich u.a. die Versionsnummer von jedem einzelnen Software-Programmpaket abfragen. Dies vereinfacht das Identifizieren von Sicherheitslücken im Softwarebestand. Log-Dateien sind einzusehen und auch ein Temperatursensor im Gerät zeigt den Zustand der lüfterlosen Hardware an. Darüber hinaus kann eine Einbindung in bestehende Netzwerkmanagementinfrastrukturen über SNMPv3 erfolgen. ■

**18389**

**[www.innominate.com](http://www.innominate.com)**

*Autor: Robert Zilliger ist Vertriebsleiter bei der Innominate Security Technologies AG, Berlin.*