



Bild 1: Die miprotek GmbH ist u. a. im Bereich der innerbetrieblichen Förder-technik tätig.  
Bild: miprotek GmbH

# Sichere Fernwartung von Maschinen und Anlagen

Die Maschinen und Anlagen der Kunden des Automatisierungsspezialisten miprotek werden international aufgestellt. Um den Kosten- und Zeitaufwand im Wartungs- oder Fehlerfall gering zu halten, setzt miprotek eine Fernwartungs-Lösung auf Basis der MGuard-Technologie von Phoenix Contact ein.

**D**ie miprotek GmbH, die derzeit rund 55 Mitarbeiter beschäftigt, wurde 1983 gegründet. Das in Buxtehude bei Hamburg ansässige Unternehmen entwickelt und vertreibt weltweit Automatisierungs-

lösungen und Produktions-Planungs-Systeme für industrielle Fertigungsprozesse. Sein Leistungsspektrum reicht von der Konzepterstellung und Konstruktion der Schaltanlagen über die Programmierung der Steuerungen

und Hochsprachen-Systeme bis zur Interaktion zwischen ERP-Lösungen, Anlagen und Maschinen über vielfältige vertikale Automationsstufen und Knotenrechner. miprotek ist im Wesentlichen in zwei Geschäftsfeldern

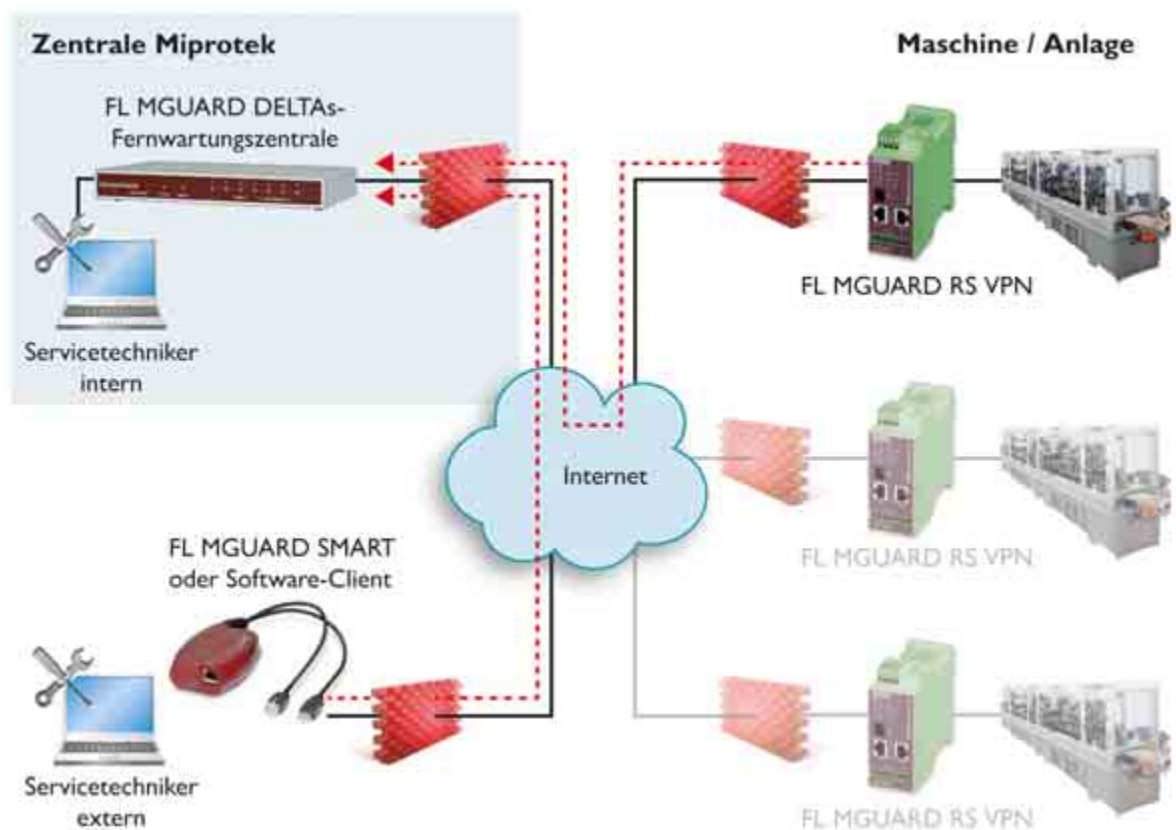


Bild 2: Fernwartung von Maschinen und Anlagen über die zentral installierte Security Appliance FL MGuard von intern und extern

tätig, die unabhängig voneinander agieren: der Asphaltindustrie und der innerbetrieblichen Fördertechnik sowie der Steuerungstechnik für Maschinen. Im letztgenannten Bereich werden Förderanlagen, Verpackungsstraßen und Abfüllanlagen für die chemische, Glas-, Nahrungsmittel- und Pharmaindustrie automatisiert. Steuerungssysteme zur Herstellung von Asphalt konzipieren die miprotek-Mitarbeiter seit 1983, wobei die

Plattform bereits mehr als 90% der Funktionalität abdeckt.

#### Aufbau der VPN-Verbindung nur durch den Anwender

Da die Fördertechnik und Asphaltmaschinen weltweit verwendet werden, nutzt das Buxtehuder Unternehmen Fernwartungs-Einrichtungen auf Basis der MGuard-Technologie und EDGE-Modems von Phoenix Contact, die sich mit der deutschen Zentrale verbinden. Hans Gerhard Schuran, Bereichsleiter SPS-Systeme bei miprotek, hat die Einführung und Umsetzung des breitbandigen Remote Service von Beginn an betreut. Bei der Auswahl der Geräte war ihm besonders wichtig, dass die VPN-Verbindung (Virtual Private Network) durch seine Kunden aufgebaut wird. Zu diesem Zweck verfügen die Mguard-Geräte über einen Schlüsselschalter, über den die Anwender die VPN-Verbindung ihrer Maschine oder Anlage nach Buxtehude bei Bedarf freischalten (Bild 1). Erst dann können die miprotek-Mitarbeiter die Wartungs- oder Umrüstarbeiten via

Internet über eine sichere Verbindung vornehmen. Hans Gerhard Schuran stellt fest: „Dass der VPN-Tunnel nur von ihnen selbst aktiviert werden kann, gibt unseren Kunden ein gutes Gefühl. Schließlich möchten sie verhindern, dass sich ein Externer unbefugt in ihrem Maschinen-, Produktions- und unter Umständen auch Unternehmensnetzwerk bewegen kann.“ Als Zentrale für alle von den Anwendern eingehenden VPN-Verbindungen fungiert das Security-Gerät FL MGuard Delta, das mit einem DSL-Anschluss und dem zentralen Backbone-Switch im Server-Raum in Buxtehude installiert ist. Sämtliche Maschinen und Anlagen, die miprotek mit einer Fernwartungs-Option ausliefert, laufen hier zusammen. Sollte es bei einer der Anwendungen zu einem Problem kommen, schaltet der jeweilige Kunde den eingerichteten VPN-Tunnel per Schlüsselschalter oder Befehl in seiner Visualisierungs-Oberfläche zur Zentrale frei. Parallel dazu können sich die Techniker von miprotek oder eines Partnerunternehmens mit der Fernwartungs-Zentrale verbind-



Bild 3: Der zentral installierte FL MGuard Delta (zweites Gerät von oben) nimmt sämtliche VPN-Verbindungen entgegen.

den. Dafür wird eine entsprechende Hardware wie der FL MGuard Smart oder ein IPsec-fähiger VPN-Software-Client eingesetzt. So erreichen die Service-Mitarbeiter die Kunden-Applikation weltweit ohne zusätzlichen Aufwand. Dabei spielt es keine Rolle, ob die Techniker im miprotek-Netzwerk angemeldet sind oder über einen anderen Netzwerkanschluss auf das Internet zugreifen.

### **Authentifizierung der Gegenstelle auf Basis von X.509-Zertifikaten**

Die sichere Kommunikation steht in jedem Fall im Vordergrund, weshalb die miprotek-Lösung ähnlich wie ein Service-Portal arbeitet. Das bedeutet, dass es sich bei allen Remote-Verbindungen aus Sicht der Internet-Verbindung um eine ausgehende Kommunikation handelt. Der Zugriff auf die Zentrale ist die einzige eingehende Verbindung – gleichgültig, ob er vom Endanwender, dem Lieferanten von Anbauteilen oder dem eigenen Mitarbeiter initiiert wird. Fordert der Kunde also einen Service, ein Firmware-Update oder eine Programmänderung an, kann das Wartungs-Team nur mit seiner Zustimmung die Gegenstelle kontaktieren. Im Vergleich zur Realisierung über ein Modem lassen sich auf diese Weise selbst komplexe Applikationen umsetzen. Aufgrund der Breitbandigkeit der Internet-Anwendung entspricht der Remote-Zugriff einer lokalen Vor-Ort-Vernetzung. Das macht sich bei der Inbetriebnahme bezahlt. Der Unternehmenssitz des miprotek-Kunden Gronemeyer Maschinenfabrik GmbH & Co. befindet sich beispielsweise im etwa 250 Kilometer entfernten Höxter. Dort ist ebenfalls MGuard-Technologie montiert, sodass beide Unternehmen sicher über das Internet Daten austauschen können. Die Remote-Zelle baut die Verbindung zur Zentrale über deren IP-Adresse auf. Die IP-Adressen der Remote-Stationen sind hier nicht von Bedeutung. Selbst wenn die Fernwar-

tungs-Hardware die IP-Adresse von einem DHCP-Server (Dynamic Host Configuration Protocol) erhält, ist die Adresse am zentralen Zielgerät ausschlaggebend. Der in der Zentrale installierte FL MGuard Delta überwacht die eingerichtete VPN-Verbindung, die erst nach erfolgreicher Prüfung der Authentifizierung mit Hilfe von X.509-Zertifikaten hergestellt wird. Eine Identitätskontrolle mithilfe von

PSK (Pre-Shared Keys) ist ebenfalls möglich, wobei sich die Verwendung von Zertifikaten bei einer VPN-Verbindung über das Internet als die sicherere Methode erweist. Durch diesen State-of-the-Art-Mechanismus wird dafür gesorgt, dass lediglich eine bekannte und im Vorfeld eingerichtete Gegenstelle Zugang zur miprotek-Zentrale bekommt. Dazu werden in der Gegenstelle zwei UDP-



Bild 4: Selbst komplexe Visualisierungsgrafiken werden unverzerrt sowie in Echtzeit dargestellt.

### Eindeutige Ansprache über 1:1-NAT

Über die NAT-Funktion (Network Address Translation) respektive das IP-Masquering werden den Teilnehmern an einem Router die angeforderten Pakete von dessen ARP Daemon folgerichtig zugeordnet. Eine spezielle Funktion ist das sogenannte 1:1-NAT, mit dem komplette Adress- oder Subnetzbereiche in eine neue IP-Umgebung gemappt werden können. Das 1:1-NAT erweist sich dann als wichtig, wenn Maschinen gleichen Typs identische IP-Adressen haben und in einem überlagerten Netzwerk zusammengeführt werden sollen. Beispielsweise gibt es in einer Anlage zehn Maschinen mit den Netzwerkbereichen 192.168.100.0/24. Jede Maschine wird per NAT mit einer neuen Adresse versehen. Maschine A erhält 172.16.101.0/16, Maschine B 172.16.102.0/16 und so fort. Die NAT-Funktion kann auch genutzt werden, um eine aus der Ferne zu wartende Maschine eindeutig zu bezeichnen. Bei miprotek wird jede Anlage unter einem festen IP-Adressbereich angesprochen. Dabei generiert der zentral installierte FL MGuard ein 1:1-NAT auf die Adressen, die von den Technikern angesprochen werden – und das unabhängig von der Remote-Adresse.

Ports nur für ausgehende IPsec-Verbindungen geöffnet, denn die Gegenstelle meldet sich bei der Zentrale.

### Verbindungen per vorkonfiguriertem EDGE-Modem

Für temporäre Verbindungen hat das miprotek-Team eine weitere interessante Variante entwickelt. Beispielsweise wird im Bereich der Asphaltindustrie oft eine VPN-Verbindung zur Ersteinrichtung einer Baustelle benötigt. In diesem Fall bietet sich ein bereits vorkonfiguriertes EDGE-Modem an, das im Anlagennetzwerk angeschlossen wird und die Kommunikation zur Zentrale aufbaut – im Bedarfsfall auch über einen sicheren Mechanismus. Die Aktivierung des VPN-Tunnels erfolgt mittels einer SMS oder eines Anrufs. Zu diesem Zweck werden im Vorfeld bis zu 20 Rufnummern im Modem hinterlegt, die eine Berechtigung zum Öffnen der Verbindung haben. miprotek schickt somit eine Art **Black Box** auf die Baustelle. Sofern notwendig, initiiert ein autorisierter Mitarbeiter den VPN-Tunnel von der Baustelle zur Zentrale, sodass der Service-Techniker von miprotek über ein breitbandiges Netzwerk auf die unterlagerten Komponenten zugreifen kann. Selbst

komplexe Visualisierungen oder Client/Server-Applikationen lassen sich problemlos übertragen.

### Fazit

Mit der Einführung von sicheren breitbandigen Fernwartungs-Verbindungen hat miprotek sein Dienstleistungs-Portfolio für die Kunden weiter ausgebaut. Bei einigen Projekten ist es sogar Voraussetzung, dass die Anlagen aus der Ferne überwacht und gewartet werden können. Dann wird das hutschienenmontable MGuard-Gerät mit VPN-Technologie in den Schaltschrank integriert. Der Anwender muss anschließend nur wenige Parameter setzen, damit die Kommunikation zur miprotek-Zentrale hergestellt werden kann. Hans Gerhard Schuran erläutert: „Zur Erstinbetriebnahme und Unterstützung unserer Mitarbeiter vor Ort lässt sich die VPN-Verbindung über das Mobilfunknetz aufbauen. Zur Einrichtung der Maschinen und Anlagen ist also kein DSL-Anschluss erforderlich, was sich insbesondere bei den Asphalt-Mischanlagen auszahlt. Obwohl sie irgendwo im Gelände stehen, können wir die Applikationen doch mit einer guten Performance erreichen. Das hilft bei der schnellen Unterstützung unserer Kunden im Bedarfsfall und verkürzt zudem den Zeitaufwand bei der Erstinbetriebnahme.“ ■

[www.phoenixcontact.de](http://www.phoenixcontact.de)



Autor: Alexander Bormann, Solution Partner Management, Phoenix Contact Electronics GmbH, Bad Pyrmont