

Sichere Fernwartung über Internet

Teleservice wird sicherer, wirtschaftlicher und erhöht die Anlagenverfügbarkeit



Ein schneller und qualitativ hochwertiger Service für weltweit installierte Maschinen und Anlagen ist ohne Teleservice kaum noch denkbar. Besonders in der Gewährleistungsphase können Service-Kosten durch einen Fernzugriff erheblich gesenkt werden. Zwei wesentliche Hürden standen bisher dagegen: Sicherheitsbedenken der Betreiber gegen eine Einwahl in ihr Netz und Probleme mit der Verbindungstechnik über die Modemeinwahl. Jedoch ersetzen Internet- und VPN-basierte Lösungen immer häufiger die Modem-Wählverbindungen. Und durch den Einsatz industrietauglicher Network Security Appliances sind die Lösungen sicher, wirtschaftlich und maßgeschneidert einsetzbar.

■ Torsten Rössel



Torsten Rössel
ist Director Business Development
bei Innominat Security Technologies
in Berlin
T +49/30/6392-3300
troessel@innominate.com

Die gute Nachricht: sichere und wirtschaftlich skalierbare Internet-Teleservice-Lösungen sind heute verfügbar. Das ist auch notwendig, denn moderne Maschinen und Anlagen werden immer stärker mit leistungsfähiger Soft- und Firmware ausgestattet. Die Kehrseite: Probleme mit der Software werden künftig für die meisten Maschinenstillstände verantwortlich sein. Statusabfragen und Softwareupdates gehören deshalb zu den zentralen Funktionen des Teleservice. Die bisher genutzte analoge Modemtechnik reicht dafür allerdings nicht mehr aus.

Als wesentliche Motive für den Übergang von Modem- zu Internet-basierten Teleservice-Verbindungen sind die Stichworte Kosten, Verfügbarkeit, Sicherheit, Bandbreite und Stabilität zu nennen. Für meist internationale Fernverbindungen beim Modem-basierten Teleservice entstehen nicht unerhebliche Kosten; auch die Verfügbarkeit analoger Telefonleitungen im industriellen Umfeld ist rückläufig und Modems sind immer öfter inkompatibel mit modernen TK-Anlagen. Außerdem wachsen die Bedenken gegen Modems als Sicherheitsrisiko („Backdoors“) für vernetzte Systeme. Security Policies

der Betreiber von Maschinen und Anlagen verbannen deshalb die Modemtechnik zunehmend aus deren Netzen. Und schließlich klagen auch immer mehr Anbieter darüber, dass die äußerst beschränkte Bandbreite und unbefriedigende Stabilität von Wählverbindungen in weit entfernte Regionen der Welt den Ansprüchen an einen modernen Teleservice nicht mehr gerecht wird und kein effizientes Arbeiten erlaubt.

Die Anforderungen an die Sicherheit steigen

Mit der zunehmenden Vernetzung industrieller Maschinen und Anlagen steigen auch die Anforderungen an die Sicherheits- und Leistungsmerkmale von Internet-Teleservice-Lösungen. Allen Beteiligten gemeinsam ist das Bedürfnis nach Netzwerksicherheit, das heißt nach Authentisierung, Vertraulichkeit und Integrität der Teleservice-Verbindungen, wie sie durch den Einsatz von Virtual Private Networks (VPNs) erreicht werden. Idealerweise sollten diese Eigenschaften „End-to-End“, also vom Service Center bis zur Maschine gewährleistet werden. Teleservice-Anbieter suchen vor allem nach einer einheitlichen, skalierbaren Lösung mit zentralem Management, die auch bei bereits im

Feld befindlichen Systemen nachgerüstet werden kann und dabei möglichst keine Eingriffe in Hardware oder Software der Maschine oder Anlage erfordert.

Um viele Hunderte oder sogar Tausende von Kundensystemen an ein Service Center anbinden zu können, müssen ferner die absehbaren IP-Adresskonflikte zwischen den (privaten) Netzwerken der Betreiber überwunden werden. Die Betreiber ihrerseits legen größten Wert auf eine nachweislich sichere Lösung mit möglichst minimalen Eingriffen in ihre Netzwerke und Firewalls sowie eigene Kontrolle über die zeitliche Verfügbarkeit der Teleservice-Verbindung analog zum häufig praktizierten An- und Abstecken des Telefonkabels beim traditionellen Modem. Der Nachweis der Sicherheit gelingt am überzeugendsten durch Verwendung transparenter, offener Standards wie etwa dem führenden VPN-Standard IPsec (Sicherheits-Architektur für das Internet Protokoll).

Innovatives Konzept für sicheren Internet-Teleservice

Die Mehrzahl der auf dem Markt befindlichen Lösungen für die Internet/VPN-basierte Fernwartung haben sich als technisch und wirt- >



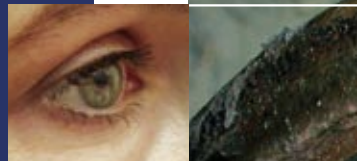
mGuard industrial RS: Remote Services Appliance zur Montage auf DIN-Hutschienen mit optional integriertem Analog-Modem oder ISDN Terminal-Adapter. Mit dieser Ausrüstung können Maschinen und Anlagen jederzeit einfach von traditioneller Fernwartung per Wählverbindung auf moderne Fernwartung über Internet umgestellt werden

TSA Transparente sichere Anlagenverfügbarkeit

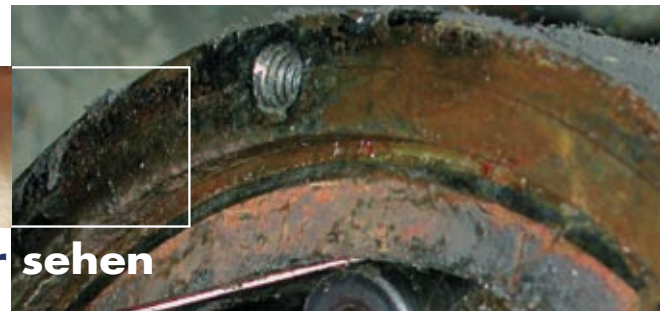
Mit unserer Messtechnik sehen, hören, fühlen und dokumentieren wir den Zustand Ihrer Maschinen und Komponenten. So werden notwendige Reparaturen planbar und die Anlagenverfügbarkeit erhöht. Mit unserem Dienstleistungssystem TSA nutzen Sie die Vorteile unseres qualitativ hochwertigen Sortimentes an C-Teilen. Darüber hinaus übernehmen wir das Ersatzteilmanagement Ihrer Sonderteile. Mit TSA bieten wir Ihnen eine vertrauensvolle Partnerschaft rund um die Optimierung Ihrer Produktionsanlage. Als Fachbetrieb für Antriebstechnik sind wir außerdem in der Lage, sämtliche Wartungs- und Reparaturarbeiten schnell und zuverlässig auszuführen.

UHLEN-BROCK Die ganze Welt der Antriebstechnik
1954

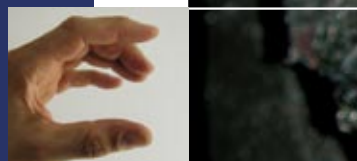
Siemensstr. 41 · 48565 Steinfurt
Tel. (+49) 2552 / 93 33 -0 · Fax 93 33 -61
www.uhlenbrock.org · info@uhlenbrock.org



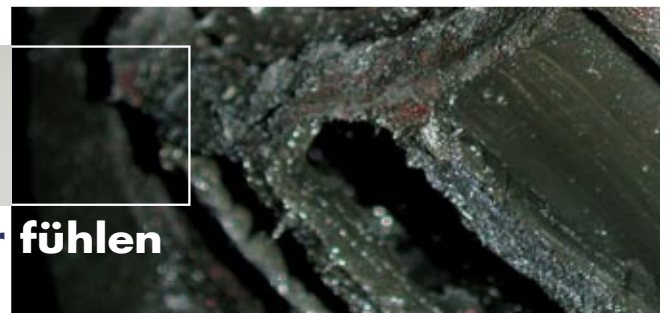
wir sehen

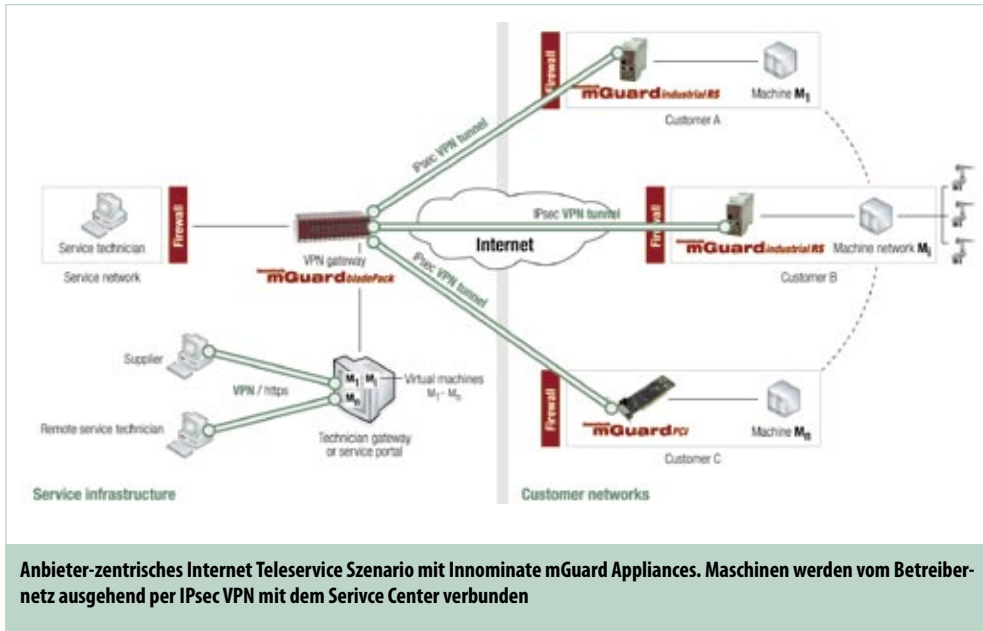


wir hören



wir fühlen





schaftlich nicht skalierbar erwiesen, weil sie konzeptionell weiterhin dem Einwahl-Ansatz aus der Modem-Ära verhaftet bleiben. Wesentlicher Eckpfeiler der von Innominate entwickelten Internet-Teleservice-Lösung war daher ein innovatives VPN-Konzept mit ausgehenden IPsec VPN-Verbindungen von den Systemen zum Service Center. Dabei fungieren autarke, industrietaugliche mGuard Security Appliances an jedem System als Träger der VPN- und Sicherheits-Funktionen. Die Geräte sind auch im Feld ohne Eingriff in Maschine oder Anlage einfach nachrüstbar und können samt der virtuellen Adressierung durch eine Device-Management-Software zentral und weitgehend automatisiert verwaltet werden. Sie gestatten dem Betreiber, die Teleservice-Verbindung nach Bedarf über einen in die Bedienoberfläche integrierten Software-Schalter oder einen elektrischen Schaltkontakt zu akti-

vieren bzw. deaktivieren, und geben ihm so die gewünschte Kontrolle.

Da die Lösung auf dem offenen Internet-Standard IPsec basiert, können neben Produkten von Innominate prinzipiell auch zu diesem Standard konforme Geräte anderer Hersteller als zentrale VPN-Gateways verwendet werden. Die mGuard Appliances bringen außerdem ein weiteres Sicherheitsmerkmal mit: Sie können die zulässige Kommunikation auch innerhalb der VPN-Tunnel durch Reglementierung der Firewall gezielt auf das gewünschte, notwendige Maß beschränken.

Die Lösung ist sowohl für Hersteller des Maschinen- und Anlagenbaus bzw. deren Zulieferer und Service-Dienstleister interessant (Anbieter-zentrisches Szenario) als auch für Industrie- und Infrastruktur-Unternehmen, die Teleservice für Maschinen und Anlagen verschiedener Anbieter nutzen wollen (Betrei-

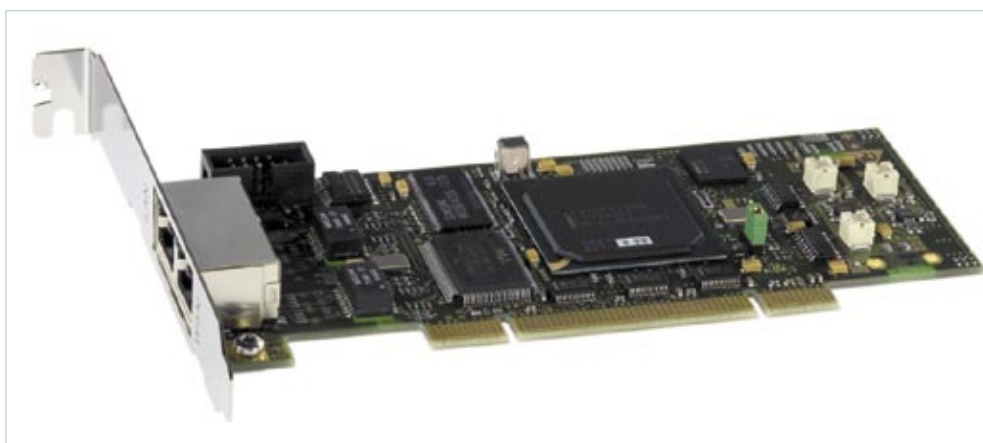
ber-zentrisches Szenario). Erweitert um ein VPN-Gateway für Techniker oder optional ein Service-Portal auf Basis von Terminal-Servern und/oder Virtualisierungssoftware eignet sie sich nicht nur für Mitarbeiter in einem stationären Service Center, sondern auch für mobiles Personal an beliebigen entfernten Standorten, sofern dort nur ein Internet-Zugang verfügbar ist.

Flexible sichere Anbindung und Quality of Service

Die Anbindung auf Maschinen- oder Anlagen-seite ist in mehreren Varianten möglich. Wird der notwendige Internet-Zugang über das Betreiber-LAN zur Verfügung gestellt, können einzelne Knoten wie etwa Leitstände oder Bedienrechner über eine mGuard Appliance im so genannten Stealth Modus als Fernwartungsziele angebunden werden. Dieser von Innominate patentierte, für das Betreiber-netz transparente Modus ist insbesondere für Nachrüstungen ideal geeignet. Alternativ können ganze Anlagen-netze oder Subnetze über eine einzelne Appliance im Router Modus und neuerdings sogar auch transparent im Multi-Stealth Modus angebunden werden, was wiederum die Nachrüstung sehr erleichtert. Wird der Internet-Zugang über eine dedizierte DSL-Leitung bereit gestellt, können die Appliances als DSL-Router für sicheren VPN-Zugang zum Anlagennetz sorgen. Nicht authentifizierte Verbindungen aus dem externen Netz hält die mGuard Firewall dabei der Anlage ebenso zuverlässig vom Leib, wie sie unerwünschte Übergriffe von dieser aus ins Betreiber-netz verhindern kann.

Für die Übergangsphase der nächsten Jahre, in denen Internet-Zugang noch nicht überall und für jede Anlage verfügbar sein wird, stehen Geräte mit integriertem Analog-Modem oder ISDN-Terminaladapter bereit. Um die Qualität der Datenkommunikation noch weitergehend abzusichern, bietet die mGuard Firmware auch noch „Quality of Service“ (QoS)-Funktionen an. Damit kann beispielsweise die verfügbare Bandbreite von Teleservice-Verbindungen optimal genutzt und für komfortables Arbeiten wichtigen oder zeitkritischen Diensten wie Desktop-Sharing-Applikationen oder Voice over IP Vorrang und eine garantierte Mindestdatenrate eingeräumt werden. ■

Dieser Beitrag als PDF und weiterführende Informationen (ähnliche Beiträge, technische Daten, Direktlinks zum Hersteller etc.) sind online verfügbar auf www.AuD24.net



mGuard PCI: Network Security Appliance im integrierbaren PCI Kartenformat für den Einsatz in Industrie-PCs und PC-basierten Steuerungen

more @ click AD0389006