

A&D[®] SELECT MARCH 2008



INNOMINATE SECURITY TECHNOLOGIES AG
Secure Remote Maintenance
via the Internet

Secure Remote Maintenance via the Internet

Remote Service gets more Secure, Economical, and Increases Plant Availability



Fast, high quality service for machinery and production equipment installed worldwide would be inconceivable without remote maintenance capabilities. Service costs can be significantly reduced, particularly during the warranty period. In the past, two hurdles existed: security concerns regarding unauthorized operators dialing into the network, and problems with antiquated modem connection technology. The Internet and VPN-based connections are increasingly replacing dial-up modems, and new industrial network security modules are providing tailored solutions efficiently and economically.

■ Torsten Rössel



Torsten Rössel
is the Director of Business Development for
Innominate Security Technologies AG in
Berlin.

The good news is that secure and economically scalable Internet-based remote service solutions are available today. This is critical because modern machinery and equipment is increasingly embedded with powerful software and firmware. The downside is that problems with software will be responsible

for most machine outages. Troubleshooting and software updates will therefore be central functions of a remote maintenance service. Previously used analog modem technology is no longer adequate.

The main reasons for the transition from modem to Internet-based remote services are simple. The keywords are cost,

availability, security, bandwidth and stability.

For international and long-distance service requirements, the costs of modem-based remote service connections are significant. The availability of analog telephone lines in the industrial environment is declining, and modems are increasingly incompatible with modern telecommunications facilities. In addition, there are growing concerns that modems can be utilized as “backdoors”, providing a security risk to networked systems. As a result of security policies, plant managers are increasingly banning modem technology from their networks. And finally, the very limited bandwidth and unsatisfactory stability of dial-in analog phone lines to distant regions of the world often prevents truly efficient customer support and no longer meets the requirements of an up-to-date remote services offering.

Increased Security Requirements

The growth in networking of complex industrial machinery, process equipment and high speed production lines has increased the requirements for the security and performance characteristics of Internet-based remote service solutions. All parties share the need for network security, and so it is important that access authentication, confidentiality and integrity be established by the use of Virtual Private Networks (VPNs). Ideally, these properties need to be established and ensured “end-to-end” between the Remote Service Center and the client equipment. Remote service providers want a single, scalable solution with central management capability, which can be retrofitted to systems already in the field, with no interference to the hardware or software of the plant equipment itself.

To connect many hundreds or even thousands of customer systems to a service center, it is necessary to consider and overcome potential IP address conflicts within private networks. Network managers place great value on the demonstration of a secure solution with minimal interference to their network and firewalls. They value remote service availability, but also value their control over the timing of remote service connectivity, on an “as required” basis. The successful proof of security is best achieved by the use of transparent, open standards such as the leading VPN stand-

ard, IPsec (Security Architecture for the Internet Protocol).

An Innovative Approach for Secure Remote Service via Internet

The majority of market solutions for Internet / VPN-based remote maintenance have proven technically and economically unscalable, because they conceptually continue to mimic the dial-up approach of the modem era. The key developers at Innominat Security Technologies decided to devise an innovative concept – providing IPsec VPN connections from the systems to the service center. The solution is provided by self-sufficient Innominat mGuard Industrial Security modules for each target system, as a carrier of the VPN and security functions. The devices can be installed in the field without interfering with the production machinery and equipment. They can be configured and administered from a central location using Innominat Device Manager software, including, amongst other features, the automated assignment of unique virtual addresses. An electrical switch or software button integrated with the production machine’s user interface allows the operator to enable and disable remote service connectivity on demand, providing the asset owner with the requested local control of the solution.

Because the solution is based on the IPsec open Internet standard, both Innominat products or IPsec standard compliant third-party equipment can be deployed as central VPN gateways. The mGuard devices also provide an additional security fea-



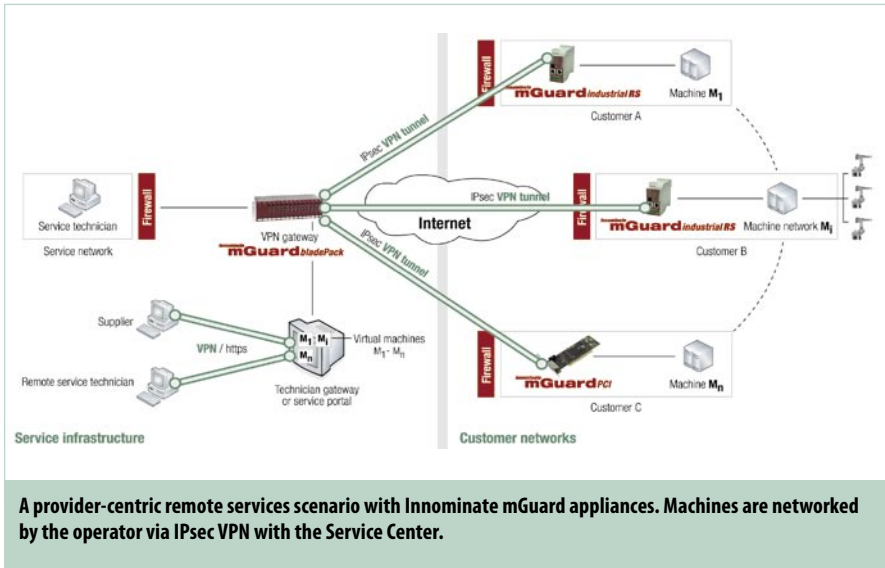
An mGuard Industrial RS: A Remote Services appliance for mounting on DIN rail with optional integrated Analog modem or ISDN terminal adapter. With this module, machinery and equipment can receive remote maintenance support at any time, optionally, by traditional dial-in modem, or via the Internet.

ture; you can control and restrict allowable communication through the VPN tunnels by firewall rules too.

This solution is interesting for manufacturers of production machinery, plant design and construction companies, their co-suppliers and service providers. It is also interesting to industrial manufacturers, automakers and infrastructure com- >



Innominat mGuard bladePack – protection of networked industrial systems and scalable central VPN gateway as a 19" rack blade solution.



panies. Both vendors and end-users benefit from the lower maintenance costs available through remote services. Extended with a VPN gateway for technicians or an optional service portal based on terminal server and/or virtualization software, the solution is suitable not only for employees in a stationary service center, but also for mobile personnel at any remote location where Internet access is available.

Flexible Secure Connectivity and Quality of Service

The connection of plant equipment is feasible in several variations.

When the necessary Internet access is provided via the asset operator's LAN, individual nodes such as control panels or HMI workstations can be connected to remote services with the mGuard module operating in "stealth mode". This uni-

que networking mode, patented by Innominat, is transparent to the equipment operator's network and therefore particularly suitable for retrofitting. Alternatively, whole machine networks or subnets can be connected through a single security appliance in router mode or even transparently in multi-stealth mode, which again greatly facilitates retrofitting. If Internet access is provided through a dedicated DSL line, the appliance acts as a DSL router providing secure VPN access to the machine network. Unauthenticated connections from the external network - as well as undesired infringements from the serviced machine into the operator's network - are reliably prevented by the mGuard firewall.

Innominat mGuard industrial modules are optionally fitted with an integrated analog modem or ISDN terminal adapter to provide for a transition phase over the next few years, for facilities where broadband Internet access is not yet available on the

factory floor. To assure the quality of data communications even further, the mGuard firmware also includes Quality of Service (QoS) functions. With these, the available bandwidth of remote service connections can be optimally utilized, and time-critical services such as desktop sharing applications or Voice over IP (VoIP) can be granted priority with a minimum data rate for a comfortable user experience.

About Innominat Security Technologies AG:

Innominat, a Phoenix Contact company, is a leading supplier of components and solutions for controlled and secured communication in industrial networks. The German company specializes in the protection of networked industrial systems and the secure remote diagnosis and maintenance of machinery and equipment over the Internet. With its mGuard product line of network security appliances, Innominat is offering router, firewall, VPN, QoS, and intrusion detection supporting functionalities, complemented with a highly scalable device management software. Innominat products are marketed worldwide under the mGuard brand through system integrators as well as through OEM partners. ■

Further information at www.AuD24.net

more @ click AD0389006



The mGuard PCI: A Network Security Appliance in integrated PCI card format for use in industrial PCs and PC-based controls

General Contact:

Innominat
Security Technologies

Innominat Security Technologies AG
Rudower Chaussee 13
12489 Berlin / Germany

T +49/30/921028-0
F +49/30/921028-020
E-Mail: contact@innominat.com
www.innominat.com