

# Remote maintenance service is safe and increases plant availability

By Torsten Rössel, Innominate

*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. Providing IPsec VPN connections from the systems to the service center solves this problem.*



Figure 1. An mGuard Industrial RS for mounting on DIN rail with optional integrated analog modem or ISDN terminal adapter

■ Fast, high quality service for machinery and production equipment installed worldwide would be inconceivable without remote maintenance service. 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.

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 are responsible for most machine outages. Service requests and software updates will therefore be central functions of the 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 so called 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.

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 and safety is best achieved by the use of transparent, open standards such as the leading VPN standard, IPsec (Security Architecture for the Internet Protocol).

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 Innominate 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 Innominate 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 pro-

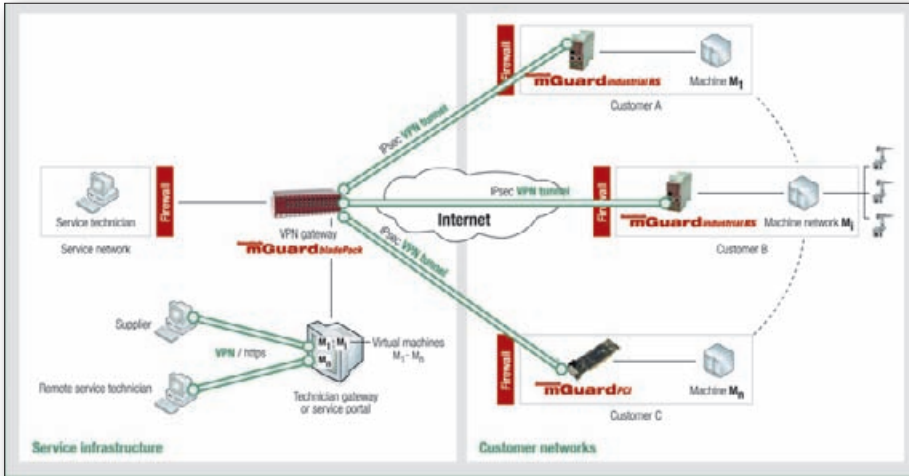


Figure 2. A provider-centric remote services scenario with mGuard appliances. Machines are networked by the operator via IPsec VPN with the service center.

duction machinery and equipment. They can be configured and administered from a central location using Innominate Device Manager software, including, amongst other features, the automated assignment of unique virtual addresses. An electrical switch or software button integrated with the user interface of the production machine 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 Innominate products or IPsec standard compliant third-party equipment can be deployed as central VPN gateways. The mGuard devices also provide an additional security feature; 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 companies. Both vendors and end-users benefit from the lower maintenance costs available through remote services. Extending availability 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 sta-

tionary service center, but also for mobile personnel at any remote location where Internet access is available. The connection of plant equipment is feasible in several variations. When the necessary internet access is provided via the LAN of the asset operator, individual nodes such as control panels or HMI workstations can be connected to remote services with the mGuard module operating in stealth mode. This unique patented networking mode is transparent to the equipment operator 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.

Innominate 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. ■



Figure 3. The mGuard PCI network security appliance in integrated PCI card format for use in industrial PCs and PC-based controls.