

VPN and Internet provide secure remote maintenance connections

Fast, high quality service for machinery and production equipment installed worldwide would be inconceivable without remote maintenance services. Service costs can be significantly reduced, particularly during the warranty period. Nice idea but the reality can be held back by antiquated data connections and unauthorised access concerns. Internet and VPN-based connections have come to the rescue bringing tailored remote maintenance solutions where ever they are needed says Torsten Rössel

MODERN MACHINERY and equipment is increasingly embedded with powerful software and firmware. This carries a burden of potential software problems which are often responsible for machine outage, mostly in the form of software glitches. Service requests and software updates are therefore central functions of the remote maintenance service.

Previously used analogue modem technology is no longer adequate for the job. The main reasons for the transition to Internet-based remote services are simple; cost, availability, bandwidth, stability and security now largely determine the process.



PHOTO: INNOMINATE

Stealth mode: The hardware security module invisibly adopts the MAC and IP address of the protected equipment but blocks and discards unauthorised data

For international and long-distance service requirements, the line usage costs of modem-based telecommunications are high, and data throughput rates are slow compared to an Internet connection. Maintenance services over the Internet reduces both the telecommunication expense and the on-site maintenance required to resolve time-consuming problems. This approach has been demonstrated to reduce the cost of maintenance operations by as much as 50%.

Another problem is that many Asian and African countries have few phone lines available. The diversity of different modem generations and signalling schemes further complicates the situation. An Internet connection poses much less hassle.

Remote services via the Internet offer high speed connectivity, the ability to share the machine operator's actual display, see visual machine elements via webcam, and speak to the machine operator using VoIP, greatly reducing the barriers to productivity. The maintenance service provider is thus able to offer additional profitable services – monthly diagnostics and

predictive maintenance are real-world examples.

And finally, there are growing concerns that modems can be used as open and unsecured backdoors, providing a security risk to networked systems.

Internet connectivity features firewall protection at the entry points of the corporate network, and layers of firewalls between departments, or between the front office and the production area. This provides a highly desirable defence-in-depth.

Security requirements

With Internet-based remote service solutions, the risk exists that viruses and malware could infiltrate a Windows-based operating system on a production console via the network, a technician's laptop, or from a remote service partner. In addition, production managers prefer to control the timing of remote diagnostics or software patches and upgrades so as not to interrupt a running system.

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). Remote service providers usually request a single, scalable solution with central management capability that can be retrofitted to systems already in the field, without interference to the hardware or software of the plant equipment itself.

To connect many hundreds of customer systems to a service centre, it is necessary to consider potential IP address conflicts within private networks. Network managers place great value on minimal interference to their network and firewalls. It is also a matter of remote service availability and 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 IPsec (Internet Protocol Security architecture).

Most VPN-based remote maintenance solutions do not scale particularly well because they continue to mimic conceptually the modem dial-up approach. Innominate as a company proposes that the way forward is to provide IPsec VPN connections from the systems to the service centre. The method devised by Innominate involves provision of an individual security

module for each target system, as a carrier for the VPN and security functions.

Device attached security provides free-standing protection; it can be installed in the field without interfering with the production machinery and systems. The concept is operating system-independent and can be configured and administered centrally. It can also restrict allowable communication through the VPN tunnels by firewall rules.

Connectivity and QoS

The connection of plant equipment is feasible in several variations. When the necessary Internet access is provided via the equipment operator's LAN, individual nodes such as control panels or HMI workstations can be connected to remote services with the VPN/security module operating in stealth mode: The hardware security module invisibly adopts the MAC and IP address of the protected equipment but blocks and discards unauthorised communications. This networking mode is transparent to the equipment operator's network, and therefore suitable for retrofitting.

Whole machine networks or subnets can be connected through a single security appliance in router mode, or transparently in multi-stealth mode. 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 corporation network – are prevented by the appliance's stateful packet inspection firewall. It blocks undesired traffic from the inside as well as from the outside. This may also be seen as an inter-departmental firewall to restrict production machine access, perhaps only to the engineering department for example.

Manufacturers should be aware that security breaches and malware incidents can occur over the Internet, internally behind firewalls or from laptops, and from business partner connections to production equipment or the company network. These risks to critical production equipment can be mitigated by defence in depth protection.

Torsten Rössel is director of business development at Innominate Security Technologies AG

FOR MORE INFORMATION CIRCLE 38