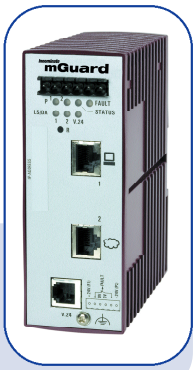
Network security: the next generation



As industrial networks expand and communicate with the world outside the production plant, they become vulnerable to attack from viruses or hackers, with potentially dangerous and costly results. Here IEN editor, Amy Barker discusses the latest security challenges with Innominate, a vendor for security appliances aiming at the machine to machine market.

No man is an island, or should that be no machine is an island: in today's production environment industrial networks and machine-to-machine communications play a vital role in plant performance, from process control to maintenance and condition monitoring.

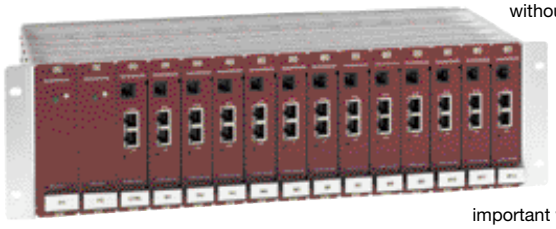
As these previously isolated and relatively secure industrial networks begin to communicate with the world outside and indeed to merge with office infrastructure, they become vulnerable to attacks from viruses or hackers, just like the office PC, but with more costly and potentially damaging consequences.

CEO of Innominate, Olaf Siemens, explained: "Many machines in the production environment are running a Windows derivative operating system, which means they can be affected by worms and Trojans, just like the office or home PC. However, if a manufacturing system goes down due to a virus, the resulting downtime can be very costly. Moreover it could also be dangerous, causing a serious malfunction of automated production equipment such as a robot. This could damage the kit itself and more worryingly could compromise the safety of operators or engineers in the vicinity."

Traditionally network security has been the preserve of the corporate IT department as they install and run the office-based infrastructure. When it comes to industrial networks however, production staff need to be involved in the commissioning process. It is important to share responsibility to create a system that is efficient and secure.

The problem is exacerbated because, unlike office networks, where all traffic in and out of the system is known, networks in the manufacturing environment need to be open to professionals from outside the corporate arena. Whether it's a service engineer, a representative from the equipment vendor, or a remote maintenance engineer dialling into the system over the Internet, access needs to be available, yet secure.

Olaf continued: "With the growth in outsourcing service and maintenance, large plants can have upwards of 100 service technicians or engineers requesting access to the network. Having just one firewall as a gateway to the entire production network is insufficient protection. That's why we have introduced the mGuard Industrial, a multi-function firewall, designed to protect individual automation systems and functional groups on the network, regardless of the operating system.



"As a first step we would simply observe what's happening on the network and the kind of traffic required. Then without removing or replacing the existing firewall, we could install the mGuard to secure individual production cells or specific items of critical machinery."

Designed to offer encryption, anti-virus and virtual private network functionality, the mGuard Industrial is a device attached tool for industrial Ethernet networks. It features a Stealth Mode, making it undetectable to attackers, while the device attached security approach avoids potential problems when installing security patches or upgrades.

Olaf added: "Stealth mode has two main benefits. Firstly it makes the security protection invisible to hackers. It is much harder for worms and viruses to attack the system if they can't see it. Secondly Stealth Mode allows existing industrial Ethernet users to deploy the mGuard Industrial without changing the topology of the network system. Engineers can plug the hardware into an Ethernet network without changing any IP addresses, for example."

This is particularly important with the growth of remote real-time monitoring, maintenance and process control, which can save time and cut costs because engineers are not required to physically be on-site. In order to send data via the Internet in this way, engineers locate, interrogate and control equipment via a unique IP address issued to that piece of equipment.

In addition to the Din Rail mountable mGuard, Innominate has also introduced the rack mount mGuard bladePack, designed to provide up to 12 mGuard blade security appliances with redundancy, audit and centralised management functions. Once again, this allows those responsible for production security to implement smaller sub-networks, perhaps restricting incoming service engineers to one specific area of the network.

Innominate 303