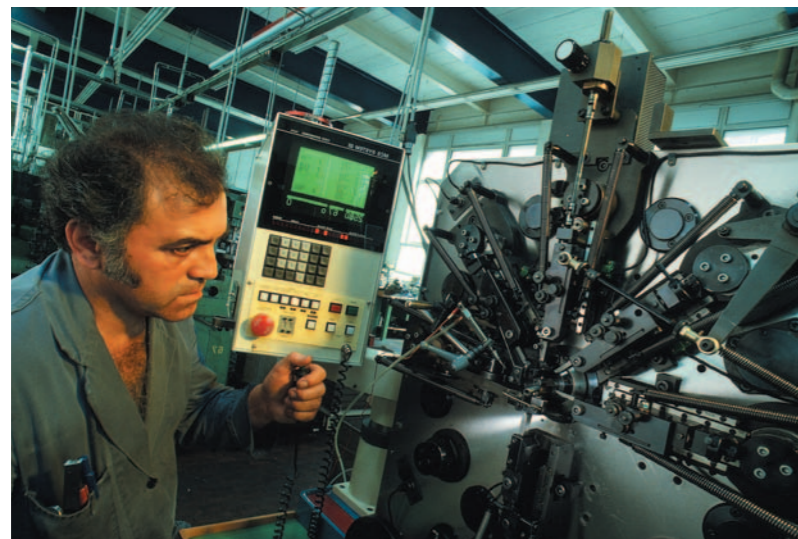


# Safeguarding the production and manufacturing environment

Network security has always been an important consideration in office environments – viruses and worms have been responsible for paralysing complete office networks. But with the expansion of industrial Ethernet, **Andreas Beierer**, director of marketing and alliances, Innominate, asks whether manufacturing and production industries are taking network security seriously enough?



The open standards Ethernet and TCP/IP are increasingly becoming relevant to all areas of industrial communication, and significantly lower costs for standard components have also contributed to the growing popularity of Ethernet in the world of automation. The IP protocols used in the factory network are effectively the same as the office network but extended by special Ethernet protocols such as EtherNet/IP, Modbus/TCP, Ethernet Powerlink, Ethercat and SerCos III – reflecting the real time

requirements of industrial control. technicians who have direct access to both networked and machine controls represent a risk to security and will ultimately make these open networks more susceptible to destructive programs and malicious attacks. In an industrial environment a virus can spell a disaster – with loss of production running into days.

#### Preventing viruses and hackers

Manufacturing and production industries are only just realising that there is an urgent need to find solutions against

*'Manufacturing and production industries are only just waking up and realising that there is an urgent need to find solutions against the encroachment of viruses and hackers – even though the consequences of a machine or production plant security breach could carry enormous costs'*

requirements of industrial control.

It is almost impossible, in fact, to imagine modern production networks without IP-based Ethernet LANs. The consolidation of the formerly insular production environment with other corporate divisions and the Internet have produced an enormous savings potential.

But, the increased use of Windows on the industrial floor and service

the encroachment of viruses and hackers – even though the consequences of a machine or production plant security breach could carry enormous costs with it. For example, a destructive program attacking a master computer through a massive overload of connection requests – so-called 'denial of service' attacks – can reduce network bandwidth for production controllers and robots enough to paralyse the

entire manufacturing line. This is far more serious than the temporary loss of a mail server, and there are several cases in which manufacturing firms have suffered this type of security incident. But, not surprisingly, these stories are not openly acknowledged.

This type of incident can also happen through human error or a lack of awareness of the risks involved. For example: while completing regular service work, a maintenance technician from an external company establishes a connection between his notebook and the controller of an industrial system. The technician has already inspected several systems on this particular day, and in between appointments he hasn't had enough time to thoroughly check his notebook and detect a hidden malign program. This destructive program now gains access to the unprotected industrial system, and once it has installed itself, its presence is quickly felt. One machine breaks down, a production line becomes paralysed or a robot runs riot. The damage is immense.

70-80% of all breakdowns are caused by unauthorised, negligent or simply careless access and activities to systems within a network. In the process, the central firewall is bypassed and becomes useless as a shield against this kind of attack from the inside. Safeguarding highly sensitive and expensive production systems requires more extensive measures.

Conventional security solutions suitable for the office environment can only be used effectively in manufacturing and production environments in a minority of cases. So what can be done? There are both software and hardware solutions which can be used to safeguard these networks. Software solutions are carried out using anti-virus programs that are installed in controllers, robots or industrial PCs – which are usually Windows-based. But hardware solutions in the form of 'all-in-one' security appliances are set to play an important role in the

&gt; 32

future of automation with the higher costs for appliances offset by lower running costs and the offer of a greater level of security.

At the very least, a security solution must include advanced firewall functionality and comprehensive virus protection. A protective shield is most effective if intruders from outside the system do not know that it exists. The Eagle mGuard firewalls from Innominate, for example, operate in the patented 'Stealth Mode'. In this mode, the device takes on the IP address of the system which it is protecting. As a result, they are able to operate fully transparently, relinquishing any 'identity' of their own which could be visible on the outside. The firewalls also operate 'invisibly' from the system itself. Eagle mGuard industrial features virus protection for DIN rails and is capable of recognising viruses in protocols such as HTTP, SMTP and FTP.

#### Protection

The increasing complexity of industrial systems necessitates external access to carry out remote monitoring or maintenance procedures. To ensure that systems are not put at risk, the firewall should support secure Virtual Private Networks (VPNs), which are protected individual connections between the individual systems and network areas.

In addition to firewall and VPN capabilities, high-performance virus protection is critical. With tried-and-tested technology from Kaspersky Lab, virus signatures can be updated instantly via the Internet or a special relay server in the production network. With the Software Development Kit, further communication protocols can be added which are also scanned for viruses.

With a range of further industry



features such as Din rail mounting, IP20 housing, electric signaling contact and 24V power supply, the Eagle mGuard devices have been developed specially to meet the needs of industrial applications.

Blade systems allow a number of machines to be protected by individual firewall blades that can also provide additional security through redundancy during running operation. In the case of failure, a standby firewall takes over the security and is automatically configured to provide the same level of protection.

System availability also means that the new security infrastructure is quickly operational. An innovative 'Autolearning Mode' ensures that all the data connections in the setup process are based on flexible rules so that the system can automatically and independently suggest security guidelines to the administrator. In this way, the most appropriate security policies are derived from the day-to-day running of network traffic – they simply need to be activated.

#### Medical industry

It is not just industry that can benefit from this new direct device-attached approach to security. The integration of information technology into medical systems is reaching increasingly complex levels with data exchange between medical systems and PCs within surgeries and clinics between general practitioners and specialists. Add to this the drive to make patient data more available and a high level of IT security is a prerequisite.

A wide range of options are becoming standard in medical diagnostics, from digital x-ray technology and full electronic analysis systems to high-tech computerised tomography. Computer controlled laser scalpels are among the latest innovative technological developments. Video recording and archiving and the new field of telemedicine – which encompasses video conferencing, i.e. between specialists located in different cities – are increasingly being used for difficult operations. Today, even routine operations require computer-controlled systems.

Computer-controlled medical technology systems are normally connected to the clinic network and therefore usually protected from external attacks through conventional gateway appliances. However, critical systems such as medical equipment actually require a much higher level of security. But whatever measures are used to protect a network from outside attack, the danger still exists from within. In the same way as in the industrial scenario, viruses can be unknowingly transmitted into medical systems by way of employee laptops.



Blade systems allow a number of machines to be protected by individual firewall blades

To make matters worse, an increasing number of these medical systems have been linked up in order to save time, increase efficiency and cut costs. This allows the complete range of patient data – from in-patient registration and laboratory results to OP reports – to be stored in a central location. In this way, any authorised user can access a complete range of data immediately. At the push of a button, the treating doctor is fully informed. The other main advantage is that the systems' availability can be monitored remotely. In the case of an emergency, maintenance work or software updates can also be undertaken remotely, without a service technician having to work on the system locally. This also saves time and money while ensuring that the system is always up for use.

But many medical computer systems are not adequately protected from attacks. Sometimes, this is due to the fact that they run on proprietary platforms so that conventional security solutions cannot be implemented, because software or hardware are not compatible.

With mGuard technology each computer-controlled medical system can be assigned its own independent security device either inserted between the medical system and the network cable or as a PCI card.

It doesn't matter which operating system or hardware platform the system runs with, for mGuard is compatible with all systems requiring no modifications to medical systems – either upon installation or afterwards. The systems run independently of processor technology and the operating system used, with the added benefit that they do not require regular software updates.

There is a long way to go before the shop floor or some front line medical systems catch up and take security as seriously as many commercial organisations. But, it is starting, and as production and healthcare IT managers look to add functions such as remote access and machine diagnostics and maintenance, the need for better protection will be further increased.

The eEagle mGuard range has been developed specifically for industrial applications

Innominate Security Technologies  
T: 49 30 6392 3688 . . ENTER 225