

**Translated by
Innominate**

Firewall security for automation: development status and trends

Today, it is impossible to imagine 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. However, without taking the necessary security precautions, standardized networking harbors high risks. If such risks aren't seriously considered and neutralized, destructive programs could lead to production losses or malfunction and even outfall of production processes. Only by implementing an efficient security strategy which is suitable for production networks can companies be assured that their industrial networks are maintained at the highest levels of system availability.

A major nightmare for any systems director would certainly be the following scenario: 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. In between appointments, he hasn't had enough time to thoroughly check his notebook – and a hidden malign program has remained undetected. This destructive program now gains access to the unprotected industry system. Once it has installed itself there, its presence is quickly felt. Suddenly one machine breaks down, a production line becomes paralyzed or a robot runs riot. The damage is correspondingly immense. 70-80% of all breakdowns are caused by unauthorized, 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.

Security planning

When planning and budgeting a new network infrastructure – or for the migration of existing systems to new standards such as Ethernet – the subject of protection must be considered from the very beginning. Instead of placing the safeguarding of production networks exclusively in the hands of the central IT department, a suitable security solution should be planned early in close consultation with a full range of company divisions. One thing is certain: security solutions from the office environment are not automatically suitable for production areas. The Stateful Inspection Firewall – well known from the office area – represents state-of-the-art technology. This type of firewall scans both incoming and outgoing data packets according to pre-defined rules. Only authorized connections are accepted.

Alternatives to software firewall/virus protection solutions include segmented and system-autonomous hardware-based firewall solutions. A hardware-based firewall is connected directly ahead of the system to be protected and therefore does not influence or affect the system software. This "device attached security" is particularly advantageous in a production environment.

Central software firewalls are often more economical than the individualized safeguarding of systems. But this is only true up to a point: namely, until a virus or a

worm succeeds in cracking the relatively lax software firewall. And if a production line fails for hours, this is bound to cost more than a computer crash in the office. For this reason, production networks require specialized security solutions.

Checklist – basis planning for a security system
<ul style="list-style-type: none"> ▪ Which central firewalls/routers already exist?
<ul style="list-style-type: none"> ▪ List all the critical production systems that must be individually safeguarded
<ul style="list-style-type: none"> ▪ List all the less critical systems that can be safeguarded on a segmented basis
<ul style="list-style-type: none"> ▪ Define the security levels: are secure outward connections necessary? Are internal service interfaces available?
<ul style="list-style-type: none"> ▪ Determine the security policies: have rules already been defined for access rights? If not, a step-by-step release of rights.

Industry firewalls – specializing in production

Both IT and security conditions in production are different than those for office environments, and for this reason, the requirements placed on security solutions are much different. For example, the operational availability of the system plays a much greater role – downtime is unacceptable. In production, one often finds various versions of older operating systems. For this reason, a centralized security software already represents a problem. Hardware industry solutions must be robust and easy to use. It is a well known fact that firewall appliances provide both security and system availability.

Stealth Mode – firewall with an “invisible cloak”

At its basis, a security solution must feature the most modern firewall functionality and virus protection. A protective shield is most effective if invaders from outside the system do not know that it exists. The 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.

What does "device attached security" stand for?
<ul style="list-style-type: none"> ▪ Direct allocation to the system being protected
<ul style="list-style-type: none"> ▪ Protects a system or a segment in production
<ul style="list-style-type: none"> ▪ Prevents effective attacks or faulty operations from inside
<ul style="list-style-type: none"> ▪ Encrypts user access for secure remote maintenance

The increasing complexity of industrial systems has made it indispensable that external access is possible – e.g. to carry out remote monitoring or maintenance procedures. To ensure that systems are not endangered by such access, the firewall should support secure Virtual Private Networks (VPNs), which are protected individual connections between the individual systems and network areas. In addition to the hardware firewalls, a security policy management which is both intuitive and simple to administer must be

on hand. This allows administrators to control access rights via a graphical user interface. Only then can a comprehensible and seamless security structure be guaranteed.

Operational availability

Machines in production downtime cost money. For this reason, security systems must fulfill their safeguarding function without endangering the running systems. After all, such endangerment is known to have happened in the past. For example, a renowned American company involved in process automation had installed anti-virus software in the control system of an industrial PC. Due to a software malfunction, the emergency shutdown for an important boiler system was prevented from functioning. This example shows that it makes sense to separate the software of individual systems from the software for the assigned firewalls. This separation offers another advantage, namely that systems subject to mandatory certification, i.e. those used in the pharmaceuticals industry, no longer need to be revalidated after each security update. If, on the other hand, the industry system is protected with security software, it would be necessary to cease operation each time a new security patch is uploaded – until the system receives a new certification.



Caption: The Innominate mGuard bladePack safeguards a large number of encrypted transmission channels

In addition, since November 2005, Innominate's mGuard bladePacks offer the opportunity of exchanging individual firewall blades during running operation. The blades are used to safeguard the back-office area between office and production. This feature is also offered by the mGuard industrial, which has been specially designed for use on DIN rails. In both units, a redundant firewall takes over the security in the case of failure of a primary unit, transferring the defined configurations within the shortest of time periods to the standby device.



Caption: Industrial security appliance for DIN rails: the Innominate mGuard industrial

System availability also means that the new security infrastructure is quickly operational. In November Innominate presented a new feature which it has named "Autolearning Mode". With this innovative mode, all the data connections in the setup process are protocolled so that the system can automatically and independently suggest security rules to the administrator. In this way, the most appropriate security policies are derived from the running network traffic. Following approval by the safety officer or the management, they simply need to be activated.

Conclusion

With the augmented use of company-wide networking, production and manufacturing areas are increasingly facing the dangers which have long been recognized and dreaded in office environments. Yet established office security measures cannot simply be transcribed to automation environments. Different laws apply in industry. Only the most perceptive security providers have really understood this problem and now offer specialized solutions to cover industry requirements.

About Innominate Security Technologies AG

Innominate Security Technologies AG is a specialist for security appliances used in industrial communication environments (M2M) and for safeguarding individual IT systems. With its mGuard product line, the company, founded in 2001, offers firewall, VPN and virus protection functionality.

mGuard appliances are sold in a range of types, from dongle to PCI card, blade server or DIN rail devices.



*Author: Andreas Beierer, Director Marketing & Alliances,
Innominate Security Technologies AG*