

# Decentralised solutions preferred

## Industrial Ethernet – chances and risks

*Networking production systems through open interfaces and protocols has increased substantially over the years. Today, Ethernet and TCP/IP have entered the production halls that were previously dominated by bus systems; as a result, the communication borders between office and production networks are being blurred.*

Andreas Beierer and  
Torsten Rössel

■ Synergies and improved access possibilities to production systems are the desired effects – a uniform security policy is the resulting obligation. The merging of these network environments involves many risks, mainly due to the infiltration of malicious programmes as well as faulty operations from within the company. In this report, suitable security concepts for production lines will be examined.

### Perimeter security vs. endpoint security

It is not from outside the company network – here a company firewall usually protects the system

at the Internet access point – but it is from within the company network that most malicious programmes arise, the kind that can paralyse industrial automation. The average level of damage caused by viruses or worms lies at approximately 1.5 million Euros per incident. This figure was revealed by the management, system and technology consultants of the PA Consulting Group in a current report.

The threats are real and must be reflected in the security strategies of production enterprises. In addition, breakdowns and safety gaps registered by the CERT (Computer Emergency Response Team) Coordination Center have increased significantly – by approx. 50-100% per year since 2000. What's more, the consequences of breakdowns in the industrial sector are much more substantial than disturbances in the office network. Should a production line fail for hours, it can potentially result in a much higher cost to the company than when a PC crashes in the office.

Intelligent “intruders” can bypass the security systems which protect entire company networks. Moreover, external service technicians regularly work with their own laptops within these networks, and like all internal employees, are thus already behind central enterprise firewalls. So-called “perimeter security”, the technique of securing a network by controlling access to all of its entry and exit points, is therefore not enough to sufficiently protect production cells. Decentralised concepts, also known as “defence-in-depth” and “endpoint

security”, and appropriate systems for end device security, are required. In general, architectures with larger centralised or smaller distributed security systems can be used in this area.

### Security appliances for industrial networks

To guarantee the individualised protection of production cells, Innominates' mGuard industry firewalls support a decentrally distributed architecture. mGuard security appliances have been specifically conceived for use in industrial environments. They combine the characteristics of a stateful inspection firewall, which monitors incoming and outgoing data packets based on pre-defined rules, with options for encrypted and authenticated communication via virtual private network connections (VPNs, of particular interest for secure remote maintenance via Internet) and high availability through router redundancy.

Their suitability to industrial applications can be seen in their fulfilment of relevant industry standards and their integration capacity for industrial control and service systems (controllers, IPCs, panel PCs), as well as machine and plant network systems.

The mGuard industry firewall can be integrated as an independent system into the network in order to protect a subnetwork, production cell or individual automation device. The crucial advantage of this concept is the complete absence of any retroactive effects caused by the firewall to the protected system itself. This principle has been patented by Innominate and is known as the “Stealth Mode” firewall. It shows



Andreas Beierer,  
Director Marketing &  
Alliances at  
Innominate Security  
Technologies AG

[www.innominate.com](http://www.innominate.com)



Torsten Rössel,  
Director Business  
Development at  
Innominate Security  
Technologies AG



*The Innominate mGuard bladePack for space-saving, individual protection of up to 12 production cells in a 19" casing*

its true effects in that it doesn't interfere with the protected system – even in the case of updates. For this reason, the expansion of existing systems can also be undertaken without any problems. In another typical scenario, with the so-called NAT function (Network Address Translation) in Router Mode, the devices can be used to securely connect numerous production cells with identical internal address spaces to an overall network.

### Product examples of firewalls in industrial environments

mGuard bladePack is an industrial security solution for installation in 19" cabinets. The system has been modularly designed and can be equipped with up to twelve mGuard blade plug-in modules. In order to guarantee the highest possible availability, the mGuard bladeBase comes standard-equipped with a redundant power supply, which is controlled by a monitoring unit. Should any problems occur, a notification is immediately sent out via SNMP traps to the administrator. Additionally, each plugged in mGuard blade module is recognised and monitored.

mGuard PCI offers integrable firewall protection, e.g. for industrial PCs and robots, the control units of which are frequently based on standard PC systems. This compact firewall appliance has been designed in the PCI card format and is powered via the PCI bus of the host system. Like all mGuard systems, the mGuard PCI works without a driver (no data communication via the PCI bus), is completely transparent and will not have

any repercussions on the system. Alternatively, the mGuard PCI can function with a driver as a network interface card and firewall in one.

### Distributed security architecture advantageous

A study conducted in 2006 by the industrial network planner Roewaplan AG (Germany) compared the overall costs of distributed and centralised security architectures with one another. The centralised approach requires a high level of investment capital, since in this case production systems are connected in a star-structure. With a centralised solution, the level of concentration of data terminals per surface area in the production hall is usually low, meaning that the working load of

the switch/router modules is not high enough to enable a cost-effective application.

The following example shows a typical production scenario consisting of 44 production systems (data terminals) set up to cover a surface area of approx. 30,000 m<sup>2</sup>. The costs for acquisition and operation over 3 or 5 years are 50-60% less with Innominate's decentralised security architecture than with the use of a centralised network and security components.

### Conclusion

Industrial Ethernet enables machines and production systems to be linked with the external world. However, standard network inter-

faces and access points to company networks and the Internet leaves them open to attack. Only decentralised protective devices with a distributed architecture can offer an economical solution for adequate security. To ensure that the expanded security infrastructure does not involve larger administration expenses, easy-to-use, central management systems for administration and the assignment of user rights are also necessary. Specialists such as Innominate offer solutions which meet these new framework requirements. A production infrastructure protected by mGuard ensures that companies can fully exploit the potential of networked infrastructures in a highly secure manner.

### ABOUT US

Innominate Security Technologies AG is the market and technology leader for embedded security used in industrial applications. The German security specialist has two strategic business fields: "Industrial Ethernet Security" and "Secure Remote Maintenance" for machines and industrial plants. With its mGuard product family, supplemented by a device management software, Innominate offers hardware firewall, VPN and virus protection functions. mGuard solutions are sold and distributed via OEM (Original Equipment Manufacturer) partners and a network of national and international partners.



*The Innominate mGuard PCI security appliance enables the integrable and secure networking of IPCs, panel PCs and industrial systems*