

## Virus catcher for the top hat rail Added security through virus protection in automation

**Translated by  
Innominate**

With the progressive expansion of industrial Ethernet into the area of automation technology, network security is also beginning to take on a high significance. Conventional security solutions from office environments can only be transcribed for the world of automation in a minority of cases. After initial manufacturers have taken up the subjects of access protection (firewall) and encryption (VPN) for industrial applications, the rapid spread of Windows in the world of automation is calling for solutions against the encroachment of viruses.



Picture 1: Innominate mGuard industrial is the first firewall for automation available with integrated virus protection.

With the high pace of innovation in information technology, the open standards Ethernet und TCP/IP are increasingly becoming relevant to all areas of industrial communication, up to field level. Significantly lower costs for standard components have also contributed to the popularity of Ethernet in the world of automation. Operational access via Internet browsers, which is widely used for many automation units, for example, has only been made possible through the widespread use of TCP/IP. The integration

of Ethernet as "industrial Ethernet" with its varieties such as Profinet, Ethernet Powerlink and Ethernet/IP (unfortunately these are not 100% compatible), will also gain prevalence during the coming years for hard realtime applications. It is already anticipated that increasing standardization and networking in the field of automation will lead to a greater susceptibility of these networks for destructive programs.

### What automation can learn from IT

The subject of network security has long been an important consideration in office environments – too often in the past, viruses and worms have been responsible for paralyzing complete office networks. But the situation looks much different in the world of automated production. Only now are many companies becoming conscious of this serious problem – even though the outfall of a machine or production plant could carry enormous costs with it. For example, if a destructive program attacks a master computer through a massive overload of connection requests (so-called "denial of service" attacks) and reduces bandwidth in the direction of subordinate controllers and production robots, then a disruption is likely to occur, paralyzing the entire production line. In the networked office world, while such an attack would prove to be annoying, it would not carry with it such serious consequences in terms of damage and costs.

A disabled production line is the source of much higher costs than the temporary loss of a mail server, for example. In hushed tones, one has heard several cases in which manufacturing firms have already been targeted by more security incidents in the production environment than is

openly acknowledged. Cases in which production has been halted for more than a day have had the effect of raising public consciousness as to the importance of security. In particular, the “Sasser” worm, a destructive program that spread like wildfire last year, left some major damages to industrial applications in its wake.

### **Security solutions for industrial use**

In order to meet the network security requirements in the area of production automation, firewall systems are increasingly being implemented that have been tailored for use in industrial environments. Stateful Inspection Firewalls, which are now standard in office environments, represent state-of-the-art technology. These firewalls scan incoming and outgoing data packets, based on predefined security rules. This assures that only authorized connections can take place, enabling a network to be safeguarded against harmful network traffic. The industry firewall is integrated into the network as an independent system, protecting a sub-network, production cell or individual automated unit. Through the use of bridging or stealth technologies, such a device can be introduced without modifications to the network topology. The security appliance is simply “merged” into the existing data stream of the machine which requires protection. In addition to the security offered by firewall functionality, it also makes sense to establish Virtual Private Networks (VPNs) for encrypted and secure data communication. In this process, data is not just encrypted for transfer via open networks (such as during remote maintenance via the Internet). Increasingly, VPNs are also being used to protect data communication carried out within the system, i.e. inside the production network. The fact that both communication partners need to identify themselves to one another (known as

“strong authentication”) can lead to a significant increase in the security of production networks. In this area as well, industrial firewall/VPN appliances are available that meld both functions. Examples of such security solutions are Scalance S by Siemens and Eagle by Hirschmann. Both of these solutions offer firewall and VPN functionality for access protection and the encryption of data in production networks.

### **Worms and viruses in automation**

Worms and viruses which have already paralyzed office networks for days are increasingly becoming a threat to automation networks as well. In hushed tones, talk is beginning to circulate about how viruses or worms that have surpassed the “species barrier”, so to speak, have been the cause of major damage to production processes. In addition, service technicians who have access to networked controls and machines represent a risk to network security. One key reason for the increasing spread of viruses: with the same pace that Ethernet and TCP / IP have made an entrance into automation, Windows Embedded has also imposed itself as the leading platform for the development of control units, robots, etc. Increasing standardization, simple training procedures and a powerful functional basis have all had a hand in contributing to its widespread acceptance. At the same time, this has intensified the problem of viruses and worms in industrial automation. Although firewalls and VPNs offer basic security functions, these factors alone cannot offer truly comprehensive protection against viruses.

### **Software or hardware?**

In principle, the safeguarding of production networks against viruses can take place – similar to the office world – either through

software of hardware solutions (so-called appliances). Software solutions are carried out using anti-virus programs that are installed in controllers, robots or industrial PCs – which are usually Windows-based. Due to the wide heterogeneity and the danger of repercussions to the system which is being protected, hardware solutions in the form of “all-in-one” security appliances will play a very important role in automation in the future. The higher costs for such appliances is mainly offset by lower running costs and the higher degree of security offered. A well-known American company which uses process automation can be used to illustrate the problematic. A malfunction in the anti-virus software installed on an industrial PC used in control technology prevented the emergency shutdown of an important boiler system from functioning. The damage was correspondingly large. Likewise, a manufacturer of anti-virus software recently entered the headlines, because a defective virus update that it had issued made thousands of PCs which had been installed with the virus protection unbootable. A similar incident occurring in a production environment would have led to extremely serious financial consequences.

### **The first virus protection for DIN rails**

The Berlin-based Innominate Security Technologies AG has recognized this gap in the market. With its new product

mGuard industrial, it offers the world’s first security appliance featuring virus protection for DIN rails. mGuard is capable of recognizing viruses in protocols such as HTTP, SMTP and FTP. This function expands the firewall and VPN capabilities of the Innominate product through a fast, high-performance virus scanner, based on tried-and-tested technology from Kaspersky Lab. Virus signatures can be updated 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. A range of further industry features (e.g. IP20 housing, electric signaling contact, 24V power supply) make the mGuard industrial a universal security solution for industrial applications.



*Author: Olaf Siemens is CEO of Innominate Security Technologies AG, Berlin.*

## Glossary

**TCP/IP:** Transfer Control Protocol / Internet Protocol = most common communication protocol in data transmission

**VPN:** Virtual Private Network = method of encryption and clear identification in data transmission

**DoS:** Denial of Service = attacks, in which IT systems are invaded through a massive overload of session information

**Stealth:** method in which security functions are performed invisibly for potential attackers as well as the system being protected

**HTTP:** Hypertext Transfer Protocol = the transmission protocol upon which the WWW is based

**FTP:** File Transfer Protocol = the most common protocol for file transfer in the Internet

**Firewall:** device or software which controls the admissible data connections

**SMTP:** Simple Mail Transfer Protocol = the most common protocol for transmitting e-mails

**Worm:** a destructive program similar to a computer virus, but which, unlike a virus, does not wait for the user to spread it but spreads itself (examples: Sasser, MyDoom)

**Appliance:** a combination of hardware and software which fulfills a single task (in this case, IT security)

**Stateful Inspection:** de-facto standard for firewalls, in which ingoing and outgoing data packets are assigned to a logical data stream

### Further information:

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