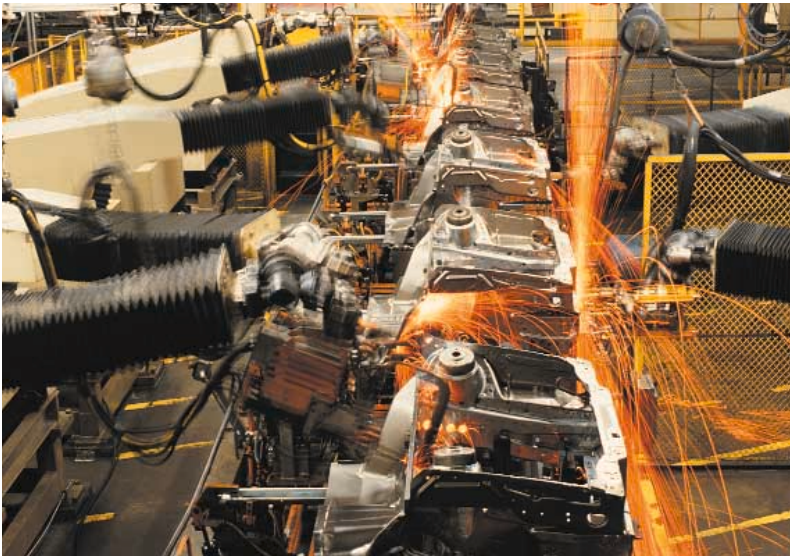


Innominate

mGuard

The innovative solution for security in industrial environments

Production environments and office environments are increasingly becoming networked, resulting in greater efficiency in business processes. For this reason, heads of production and IT departments are required to guarantee the security and availability of their systems in equal measure. Industrial computers that control production robot programs, for instance, must be protected from viruses, worms and other attacks from the network – a highly explosive subject.



In the process, they often overlook the fact that dangers from outside the system are just as large as those from inside. During the maintenance of industry robots, for example, central industry computers are often unwittingly infected with “malicious codes” from service technicians’ laptops. The resulting damages can be immense.

“Never touch a running system”

In no other sector is this old bit of IT wisdom followed so consistently as in industrial manufacturing environments. This is because every update, upgrade or patch influences the function of a computer and can often lead to unexpected – and annoying – surprises. For this reason, a comprehensive series of tests must first be carried out in test environments before the software for robots, control computers and especially central computers is modified. This represents a complex, time-consuming and very expensive process which, whenever possible, is avoided. Yet with the increase of company-wide networking, very serious security considerations need to be taken into account.

An additional problem is caused by what are known as validated systems. In this area, modifications to hardware and software can only be undertaken when taking strict rules into account. Such systems are commonly used in the pharmaceutical industry, for instance. It is nearly impossible to close security holes in this area using soft- or hardware updates. Nevertheless, making such systems reliable – and above all, protecting them in an economical way – remain enormous challenges.



Proprietary or standard: explosive security problems

Many industrial computers operate with proprietary operating systems, especially those that are somewhat older. These are judged to be secure, because operators believe that hackers would not be interested in transmitting "malicious codes" into these few systems. For this reason, the security holes in the system are often unknown. Moreover, little thought has been given as to how to block attacks. No one knows how such specialized operating systems would react to the thousands of viruses, worms or Trojan horses that are currently in circulation. And with increasing company-wide networking, it is these systems in particular that are at risk.

There are still numerous industry systems that employ older processor technology (e.g. Intel 386 or 486) as well as older versions of operating systems. This does offer some advantages – such as operation without fans and a compact form, as well as robustness and the high reliability of the system. But some serious disadvantages are also involved – not the least of which is the reduced performance caused by upgrades and software-based security solutions.

Newer manufacturing machines often run with standards such as Windows, Ethernet, TCP/IP and HTTP. But for exactly these reasons, such systems are increasingly exposed to security risks from the network.

The security holes in Windows programs are already well documented. The numerous patches that have been issued by Microsoft, even for its latest operating system, Windows XP, show that security holes and high risks are involved. Furthermore, lest we forget: "Never touch a running system". The result: what were assumed to be advantages by using standards actually turn out to be serious disadvantages. This is because the implementation of patches in an industrial environment is a complex and intricate process. Moreover, older running systems such as Windows 95, Windows 98 or Windows NT4 are no longer even supported by Microsoft.

Why conventional security technology is of little use

There are various forms of security technology that can be used in conjunction with industrial computers. But nearly all of these – regardless of whether hardware or software-based – have the same drawback: to be implemented, they require modifications to the system. And this is exactly what should be avoided at all costs in an industrial environment!

Hardware-based systems (routers, bridges) have the drawback that they can always be identified in the network based on their IP – and are therefore highly susceptible to attack. Particularly due to the fact that in many systems, standard ports are left open in order to make data transfer more unproblematic.

Unfortunately, software-based solutions (personal firewalls, anti-virus software) have other limitations: namely, they cannot run on some proprietary operating systems, due to lack of compatibility. Moreover, they often can't be integrated into systems using older processor technology – because these lack the necessary performance. Blocking a virus attack would demand so much of the processor's performance that the whole system would be paralyzed. Not to mention the fact that software constantly requires updates – otherwise viruses can easily attack the operating system time and again through newly detected security holes. Yet such updates are complex, requiring extensive resources in manpower and capital.

mGuard protects industrial computers without interfering with the system

All the drawbacks of other forms of security technology, which require modifications to the industrial system, are solved with Innominate's mGuard products in a simple, reliable and economical manner. For mGuard components are always compatible. They require neither modification to the computer configuration nor regular software updates. And they run independently of the processor technology and operating system used.



Highest security level, network-independent

Regardless of which components are used to protect a network from attack from "outside", there are enough potential dangers within the company itself. These span the spectrum from viruses which are unwittingly infiltrated by employees, all the way up to deliberate espionage and sabotage attempts. While a mail server breakdown caused by a virus is usually quite fatal, the attack on a central computer can be catastrophic. In this instance, the control computer and production robots can be restricted to such an extent that the entire production is crippled.

With mGuard technology, you can assign every industry system, whether central computer, control computer or production robot, its own security components – with individual levels of security, specifically configured access rights and numerous other unique advantages, simply and centrally administered with the Innominate Security Configuration Manager.

Effortless integration, quick installation

The mGuard platform is an independent system, which is either directly integrated into the industrial computer at the network cable and then connected to the computer or if desired, integrated as a PCI card. For industry computers that are combined into 19-inch rack systems, Innominate offers the mGuard bladePack with redundant power supply. With the mGuard bladePack, up to twelve computers can be protected individually or up to six computers protected in hot standby mode. In addition, Innominate offers the mGuard industrial, which has been especially designed for use in industrial environments based on top hat rail mounting. The implementation of both systems is equally fast and simple and the functions and operating performance of both are absolutely identical.

Regardless of which mGuard system you choose, the computer system does not have to be reconfigured, nor do driver units or other software have to be loaded. What's more, the operating system never has to be updated again using security patches. This saves time and money while offering the highest level of permanent security.

Primary functions of mGuard

mGuard, the "device attached security" solution from Innominate, unites all functions, reliably protecting IP connections, e.g. for remote administration of the system:

- VPN for secure data transmission using public networks (hardware-based DES, 3DES and AES encryption, IPsec protocol).
- Configurable firewall protects the system from unauthorized access from the "outside". The packet filter filters data packets based on the originating and target address and also blocks undesired traffic coming from the "inside".
- Integrated optional Kaspersky virus protection supports the protocols HTTP, SMTP and POP3 (recommended exclusively for the versions enterprise and enterprise XL). Virus protection already takes place on the mGuard – assuring increased security and high performance for the secured system.



Unassailable with the Innominate Stealth Mode

mGuard, the “device attached security” system from Innominate, features the one-of-a-kind Innominate Stealth Mode. This allows the device to work absolutely transparently, requiring no IP address of its own. mGuard uses the same IP as the computer it is protecting and therefore cannot be recognized by invaders, making it unassailable to attack. A further advantage: mGuard is implemented based on the automatic identification of the computer IP, which lasts just seconds. This is a decisive argument – particularly in industry environments, where production cannot stop for even a minute.

Maximum data throughput for VPN and firewall

The basis of the integrated security solution is the embedded Linux configured by Innominate, running on a special network processor with XScale core by Intel (IXP 42x), with up to 533 MHz processor capacity, up to 64 Mbytes of SDRAM working memory and 16 Mbytes of Flash memory. The Intel processor features hardware-based DES, 3DES and AES encryption. This guarantees maximum data throughput for firewall (up to 99 Mbit/s) and VPN (up to 70 Mbit/s). VPN connections are also quickly and reliably established in Stealth Mode.

At a glance:

- “device attached security” system: independent of hardware platform and operating system used.
- Simplest integration: no system adaptation, driver installation, never any updates.
- Reactionless network integration when using the transparent Innominate Stealth Mode.
- Maximum data throughput using hardware-based encryption for high speed VPN/firewall.
- Highly efficient anti-virus solution based on Kaspersky technology (optional).
- Full interoperability with other standard security solutions (IPsec) within the LAN/WAN.
- Fully integrable in central management environments (SNMP).
- Convenient company-wide configuration of all security devices via drag and drop with the Innominate Security Configuration Manager (optional).

Convenient integration and administration

Configuration, roll-out and administration of mGuard devices is supported centrally with the Innominate Security Configuration Manager, based on the tried-and-tested, rule-based technology of the Solsoft Policy Server. Using a graphic network model, the security adjustments for several mGuard systems can be quickly and conveniently configured. The defined rules are automatically verified. Firewall rules, VPN configurations and NAT settings are loaded directly onto all devices and activated immediately. In addition, the VPN connections between mGuard devices, both between one another and with the gateways of other manufacturers, are set up and managed. Everything is displayed conveniently on the graphic interface for easy operation via mouse click.

What was once complex, time-consuming and error-prone due to the configuration of individual systems is now quick and flawless with the Innominate Security Configuration Manager. The overwhelming benefit: operating expenses and manpower are reduced significantly.