

IT Security in Production

Security for Industrial Ethernet Networks Based on Accepted Standards



Torsten Rössel is the Director of Business Development for Innominate Security Technologies AG in Berlin.

Machinery and production systems are increasingly managed over the worldwide Internet via Ethernet. Security is obviously of critical importance throughout the network. But Enterprise networking and common network interfaces are potentially more vulnerable than ever. There is, however, an economic solution capable of providing effective protection devices for a distributed architecture, explains Torsten Rössel, Director Business Development, Innominate Security Technologies.

Corporate firewalls provide access security against Internet attacks from the outside world. But the most harmful programs, capable of paralyzing automation systems, are often introduced internally. The average damage caused by viruses or worms is around 1.5 million (€2.4 million US-\$), as reported by the PA Consulting Group in a highly respected report. Defeating such threats must be part of the security strategy of every automated production enterprise. Cert Institute registered incidents and vulnerabilities since the year 2000 are growing at 50–100% per year.

Major Trends in Automation

The success of the programmable logic controller (PLC) began in the 1980's. A central control panel previously read the signals from hundreds of sensors, actuators and other control devices. (Before PLCs, logic was designed with banks of relays within the panel.) The disadvantage was long cable runs from the equipment to the panel. This has far reaching practical consequences, even in today's networks, when up to 80% of the failures of automation systems occur as installation issues and cable backbone problems. At the beginning of the 1990's, established fieldbus systems, such as Interbus, improved this problem. I/O cards and other peripheral devices can be installed in a decentralized network along a single cable link. This provides several advantages. The decentralized approach allows for the review of individual plant components.

Errors are easier to locate and can be immediately fixed because a single cable can be checked quickly for damage and replaced. This is equivalent to the replacement of patch cords used in the distributed architecture of an Ethernet network.

Security Issues Are Neglected

It is common in Ethernet-based production networks to find that security aspects are given far too little consideration. Given the growing connectivity between production and office networks, it is imperative that potential interactions, security consequences, and maintenance costs be considered. As with the development of industrial switches, evaluating the equipment requirements for automation include determination of durability, long life, production availability, ease of use, assembly, installation and administration.

Particularities of Industrial Networks

The consequences of production interruption in the Industrial sector are much more serious than failures within the office network. Firewalls can protect corporate networks from most external intruders. External service technicians have access, however, and employees and visiting consultants with laptops can inadvertently (or deliberately) introduce malicious software behind the external firewall. The so-called security cordon of firewalls at border crossings between depart-

ments often does not provide adequate protection. Effective decentralized approaches are required – referred to as “Defense in Depth” and “Endpoint Security” in the literature – as are corresponding systems for the security of end-point devices. In principle, architectures with small, distributed security systems are preferred.

Security with Security Appliances

For the protection of individual production cells, the Innominate Mguard security devices are used in a decentralized, distributed architecture. These security appliances have been designed specifically for use in industrial environments. They combine the characteristics of a “stateful inspection firewall” (incoming and outgoing data packets are monitored and eventually blocked based on predefined rules) with options for encrypted, authenticated communication via Virtual Private Network (VPN) connections. High availability is provided through router redundancy. Their specific suitability for industrial applications lies in the fulfillment of relevant industrial standards and the ability to integrate with industrial controls, such as controllers, IPCs, Panel PCs, machinery and plant networks.

The Mguard firewall acts as a self-contained system in the network and can protect a production cell or a single automated device. The advantage lies in this protection being completely non-reactive to the protected system(s) thanks to Innominate’s patented “stealth mode firewall” principle. Updates to the security device can be made without interfering with the protected system itself. Existing systems can thus be easily retrofitted. In router mode, with the Network Address Translation (NAT) function, the devices can also provide secure connectivity of numerous production cells with the same internal address space to an overall network.



An Innominate Mguard Remote Services unit for mounting on DIN rail with optional integrated Analog modem or ISDN terminal adapter.



An Innominate network security unit in PCI card format for use in industrial PCs and PC-based controls

Integrated Protection for the PC Industry

Mguard PCI provides integrated firewall protection for PCs and industrial robots, which are often controlled via standard PC-based systems. The compact firewall appliance has a PCI card format and is powered over the PCI bus of the host system. It can be used similar to all Mguard systems, without data communication via the PCI bus, completely transparent to the operating system. Alternatively, Mguard PCI with a driver can perform as a network interface card and firewall at the same time.

Distributed Security Architecture

In a 2006 study, industrial network planners Roewaplan in Germany compared the total cost of distributed and centralized security architectures. In a centralized approach, production system wiring leads to high initial investment costs. The concentration of data terminals in the production area is usually low, so that the utilization

of switch and router modules for a centralized architecture is not high enough to provide a cost-effective solution.

Management Solutions

Early users of the system were concerned about the costs of commissioning, configuration and maintenance of the network components. But the cost is not linear, and decreases per device as the number of security devices rises, thanks to a central device management solution. The Innominate Device Manager (IDM) software provides sophisticated templates, automated inheritance of configuration properties, and an integrated Certificate Authority to produce VPN certificates with a high degree of automation in the configuration and updating of individual devices. With a push-pull mechanism, a central management console supplies needed information to the decentralized components.

Conclusion

Machinery and production systems today are being interconnected to the outside world via Ethernet-based networks. This ensures high flexibility and cost savings. The traditional network interfaces are vulnerable, however, as much as corporate network access over the Internet can be. Innominate offers an economic solution to provide decentralized security with effective protection devices arranged in a distributed architecture. Yet this advanced security infrastructure can be administered and maintained from a central console, thus adding no higher administrative burden – and it is available today.

CONTACT

Innominate Security Technologies AG, Berlin, Germany
 Tel.: +49 30 6392 3300 · Fax: +49 30 6392 3307
 contact@innominate.com · www.innominate.com