

Hardware firewall provides security in industrial Ethernet systems

**Translated by
Innominate**

Virus protection for automation technology

Ever since industrial Ethernet has found its way into production, the world of automated production is no longer a secure oasis. But many companies have yet to seriously consider the problem of network security. In this area, Innominate offers relevant security solutions – which can now also be utilized in production networks.

Increasingly, Ethernet-based communication systems are reaching the field level in automation technology. Proprietary data protocols and network technologies for production control units are gradually being replaced by the standards Ethernet and TCP/IP, which are widely used in office environments. On the basis of this shared infrastructure, office and production networks are increasingly becoming consolidated. In terms of efficiency, this opens up great potential for industrial firms, as the production control technology can be merged with ERP (Enterprise Resource Planning) systems and the supply chain management. Another plus is that only *one* technical infrastructure must be set up and maintained.

So much for the plusses. A trans-sectoral infrastructure also opens the floodgates for viruses, Trojan horses and attacks from hackers, which until now have been uncommon in industry networks, due to their relatively secure isolation. These are security problems that the office world has long been subject to – in the past worms and viruses have been responsible for paralyzing complete office networks. And their danger to automation networks will only increase over time. Yet many companies are only now becoming conscious of this serious problem. "It surprised us how naïve firms are concerning the security risks connected

with the use of industrial Ethernet systems," says security specialist Olaf Siemens, CEO of Innominate Security Technologies. And this, even though downtime for machines or a production plant is enormously expensive. Indeed, a disabled production line causes much higher costs than the temporary loss of a mail server, for example.



Olaf Siemens, Innominate: "Many companies have not yet seriously considered the security risks that come with using industrial Ethernet."

In addition, the fact that Windows is being increasingly used in automation raises the necessity for fundamental solutions in safeguarding the operability of Ethernet and TCP/IP-based networks. Not to mention the fact that with the fusion of office and production networks, a security solution should be implemented which meets the requirements of both network environments.

The Berlin-based company Innominate, which has specialized in security, has recognized this gap and develops products which deal directly with such security problems. The individual members of the "Innominate mGuard" product family are tailored for

corresponding use in office or production environments. The company is clear on its focus: "We want to offer security solutions for industrial production, an environment that is increasingly characterized by standardization and networking," explains Siemens.

Invisible virus protection for the DIN rails



Innominate mGuard industrial The patented Stealth Mode of the "Innominate mGuard industrial" makes the firewall invisible for attackers.

This is the reason why Innominate has added a solution for industrial production IT systems to its product palette for "device attached security". The "mGuard industrial" is a hardware firewall, which can be mounted on DIN rails. It protects individual systems or functional groups in the industrial Ethernet from attacks from the outside, as well as from unauthorized access from inside. As the first device available for production networks, the "mGuard industrial" also offers the option of comprehensive virus protection. "Our configurable firewall mGuard industrial protects automation networks and industrial machines individually from unauthorized access and security dangers of all kinds, regardless of the operating system currently being used," describes Siemens.

The security appliance is simply switched on between Ethernet interface and

production line machine, adopting its MAC and IP address. With the patented "Stealth Mode", it receives a kind of invisible cloak, becoming undetectable for exterior intruders. The mGuard recognizes the corresponding IP and MAC address of "its" protected computer and adopts these for itself. In this way, the firewall can be accessed in the network under the address of its computer and configured. For hackers, however, this makes the mGuard indiscernible. "The system cannot be bypassed, for it is directly connected to the Ethernet interface of the production machine," Siemens emphasizes. In addition, the Stealth Mode allows the integration of an mGuard without the need of re-configuration to the overall network.

By protecting each individual machine with its own firewall – Innominate calls this principle "device attached security" – a production network remains operational, even in the case of faulty operation or viral infection of a machine. In addition to protection against hackers, the mGuard industrial also allows encrypted connections to be established between individual systems. These Virtual Private Networks (or VPNs) enable pinpointed access control. Strategically placed VPNs in connection with individually coordinated security policies prevent inadvertent misentries by internal employees. External maintenance technicians can be given access rights for individual machines. In the process, all other systems remain inaccessible to them.

Another novelty in industrial automation is the Innominate Security Configuration Manager (ISCM). With this innovative tool, the security policies for all the mGuard systems can be defined centrally on the graphical user interface via drag-and-drop. The policies can then be loaded onto the individual mGuard firewalls. Similarly, VPN connections between individual mGuards or other gateways are easy to configure.

Because the mGuard industrial does not contain a ventilator or any other moveable parts, it can be used for periods of up to 15 years. The device is available in two versions. The “mGuard industrial enterprise FW” (firewall) can be obtained from international Innominate distribution partners at a list price of 690 euros. The “mGuard industrial enterprise XL” (firewall plus VPN) costs 940 euros.

The security specialists at Innominate, who have developed four new products

within a span of twelve months, are currently working on both wireless security and support systems for the realtime standard Ethernet Powerlink. Its advantage: due to the standard processors and ASICs used, the same hardware can be employed.

Further information:

www.innominate.com