

Industrial Network Security

Combining Business with Displeasure

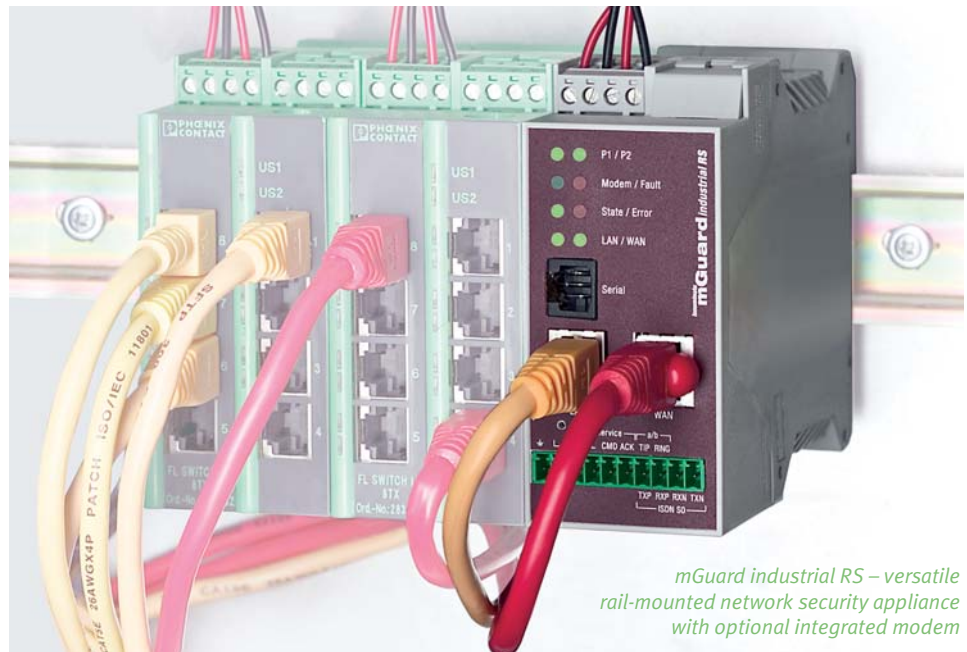
Investments in network security are like insurance premiums: rarely popular due to their negative motivation. After all, this money is being spent to prevent the unwanted from happening or rather limit consequential damages. In this article, you will learn how to combine business with displeasure and draw positive added values from capital well spent for the security of your industrial networks.

Torsten Rössel



Dipl.-Math.
Torsten Rössel
Director Business
Development,
Innominate
Security Techno-
logies AG

www.innominate.com



mGuard industrial RS – versatile rail-mounted network security appliance with optional integrated modem

Industrial systems are increasingly getting networked based on Ethernet and TCP/IP protocols. Unfortunately, as a result of that networking they are also at risk. While much of the attention particularly in North America is focusing on threats from targeted hacking and cyber terrorism attacks, more accidental types of events play a less spectacular yet more relevant role in practice: network overload by defects and broadcast storms, operating errors, and the intrusion or introduction of malware. Risks are substantial and range from loss of production to health and environmental damages.

As studies have shown, programmable logic controllers, the cornerstones of industrial automation, are

quite susceptible to disturbances via Ethernet interfaces as well. At European research lab CERN for instance, standard PLCs from well-known vendors have repeatedly been subjected to vulnerability tests with freely available tools. With newer firmware versions the latest findings turned out slightly better in 2006, however, the tests still resulted in failures for 34 per cent of the controllers and for 26 per cent even in total system crashes.

Besides the proliferation of Ethernet, use of standard IT components in the industrial environment is also growing. Systems are thus becoming more open for desired integration but regrettably for undesirable damage, too. Known vulnerabilities are spreading

from office networks into the world of production. So what is to be done?

Defense-in-Depth: distributed protection with central management

A defense-in-depth strategy is generally recommended as best practice with staged layers of protection reaching down to critical cells or individual systems, comparable to the endpoint security purposed by security software on PCs in office networks.

Protecting heterogeneous industrial systems purely by software, however, is usually not an option due to insufficient hardware resources for one, and because permanent security updates are

unacceptable in view of the “never change a running system” principle.

Innominate is specializing in the requirements of industrial network security and has been creating innovative solutions with its mGuard technology: tailored network security appliances with integrated firmware, ready to plug and protect. Access control and filtering of network traffic by firewall appliances with appropriate rule sets play a key role.

Depending on the target to be protected, a variety of form factors are eligible as optimal solutions. The lineup includes industry-specific rail-mounted devices for electrical cabinets, PCI cards for integration in PC-based HMI panels and controllers, as well as a 19” chassis with compact plug-in blades.

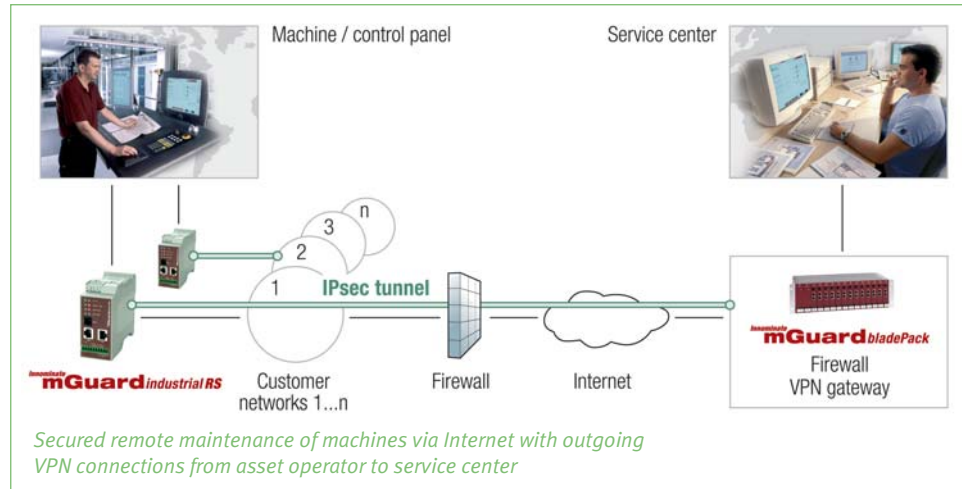
Distributed, decentral security appliances sustain freedom of network design and thereby allow for their flexible and cost-effective deployment. Not being restricted to operation in router mode but also suited for transparent, “stealth mode” insertion into a network or in front of a single system is another advantage of the devices, in particular for retrofitting.

Management software such as Innominate Device Manager, supporting comprehensive administration and largely automated configuration of distributed appliances from a central platform is absolutely essential to reap these benefits in large-scale deployments.

Learning firewall rules from scratch

How to obtain an effective set of firewall rules, though, in particular when retrofitting security to existing equipment with poor documentation? Again, mGuard appliances are up to the task and can help to literally learn an appropriate rule set from scratch. In “learning mode”, all connection attempts are initially accepted and logged.

With tool support, those connection logs can then be condensed into a human readable essence of rules which can be checked for plausibility and finally armed and activated. From then on, unknown and undesirable connections are reliably blocked.



Added value #1: efficient networking of cells with 1:1 NAT routing

Structuring complex production processes into networked cells is common practice. When numerous similar cells are used in a production line or multiple plants of the same type are being built, there is big advantage in a uniform design of the internal cell networks.

Significant efforts otherwise required by suppliers and asset operators for engineering, programming, documentation, and commissioning of individualized cell networks can thus be avoided by “cloning” the cells, using the same internal IP net and fixed component addresses over and over again.

This often conflicts, however, with the need for targeted communication from the higher-level production network to individual nodes in those cells. A router with simple network address translation (NAT) at the boundary between cell and production network falls short of the task, because the nodes in the cell network cannot be addressed from outside then. Instead, a router is needed that can map all or parts of the internal cell nets onto unique, virtual external networks by what is called 1:1 NAT. This holds even more so, when Industrial Ethernet is used pervasively instead of a fieldbus to also connect all input/output and sensor/actor components inside the cells, not uncommonly expanding the number of IP nodes by a factor of 10 to 20.

Innominate mGuard security appliances feature this 1:1 NAT routing functionality with flexible configuration and wire-speed performance of 100 MBits/s, combined with the network security of an integrated stateful inspection firewall that pure routers are missing. Thus, network access to the cells is perfectly under control.

Added value #2: secured remote services via Internet

Remote services are well motivated in all phases of the industrial equipment life cycle. Remote diagnosis and maintenance can support commissioning, save on avoidable on-site warranty and service assignments, and optimize system uptime and productivity.

To that effect, remote services are in widespread use and being offered since the mid 90s until today, still mostly through modem dial-up connections. Now, the emerging transition to secured Internet connections – essentially motivated by cost, availability, security, bandwidth, and stability reasons – represents a new challenge.

Innominate mGuard security appliances can provide for a very elegant solution to that challenge, connecting machinery to respective service centers by operator-initiated virtual private networks (VPNs). Such a solution satisfies the manifold requirements of both vendors and asset operators. Their common demand for network security is fulfilled

by end-to-end VPNs between equipment and service center. Of course, access through the VPN tunnels is again controlled by firewall rules.

Vendors can thus offer to their customers a uniform, scalable solution with central management which can be retrofitted to systems in the field without impacting their hardware or software. Also, IP address conflicts between the asset operators’ private networks can be overcome by virtual addressing.

Asset operators are provided with a demonstrably secure solution based on the leading public VPN standard IPsec which is minimally invasive to their networks and firewalls and gives them absolute control of the remote services connection.

CONCLUSION

Networked industrial systems are in more need of protection than often assumed. Yet, that alone may sometimes not justify or promise sufficient return on an investment. We have presented two relevant added value applications which can be combined with the fundamental protection of decentral security appliances to gain multiple benefits from the same infrastructure investment.

With the Innominate Device Manager and based on the mGuard firmware a field-proven family of centrally manageable industrial network security appliances is readily available for those applications.