kontron

»Application Story«

KISS in Communications

Highly available embedded server for secure teleservices

Kontron KISS servers in use as a high-end firewall & VPN gateway for industrial teleservices

For secure remote maintenance and diagnosis of machines and systems via the Internet, Innominate has developed a highly-available 19-inch network security solution, which is used in service centers as a high-end firewall and VPN gateway. There it handles the specific requirements for building VPNs and then maintains these secure virtual private network connections to remote industrial systems. Because this node is responsible for up to 1,000 simultaneous VPN connections, the highest availability requirements are placed on it. For this reason, server hardware from Kontron is utilized. It meets availability requirements that are usually only found in carrier-grade telecommunications platforms, but at industry-standard pricing.

To support system operators, manufacturers of machinery and equipment more and more frequently provide teleservices for remote maintenance and monitoring. Through the global communication connections between local operators and experts in remote service centers, cost-intensive site visits can be cut down and downtime greatly reduced. In addition, the high bandwidth of Ethernet ports, which are usually already integrated into machines, creates new, highly-efficient service prospects and competitive advantages, for example through the use of current Internet technologies such as Voice over IP and streaming image and video data.

Modems are now obsolete

Since the mid-90s and up until today, teleservices have been largely provided via dial-up lines with analog modems or ISDN terminal adapters. Besides the high cost of telephone infrastructure, the additional connection costs and low-speed data throughput, modem connections also have the disadvantage that each individual connection to the telephone network constitutes a so-called “backdoor”, and this represents an additional security risk to the company network. Thus, there has recently been a strong trend towards modern, broadband Internet connections through VPN and firewall technology for such services.

Since modern machines and equipment generally have Ethernet interfaces and are often integrated into corporate networks, it seems only natural to carry out the remote maintenance of systems over a TCP/IP Internet connection via Ethernet. The use of Internet connections for remote maintenance of industrial equipment and machine systems has several advantages. The cost of the telephone infrastructure, which must be installed for each machine using the modem-based teleservice is eliminated. At the same time, no overseas connection costs are incurred, and data throughput is greatly increased. Additionally, through current Internet technologies such as Voice over IP and the streaming of image and video data, there are also new and very efficient service prospects and thus competitive advantages.

However, to take advantage of this brave new Internet world and to be able to profit on the machine level, some safety precautions must first be implemented, because no machine should be readily accessible directly from the Internet by a third party and thus be technically compromised. To provide the desired secure access to systems, machinery and entire machine networks via TCP/IP, manufacturers and operators are looking for an economical security solution for teleservice applications, which ensures authentication, confidentiality and integrity of data traffic through various encryption methods and eliminates unwanted data traffic through firewalls. Ideally, this should be integrated into existing network structures with minimal effort.

An all-round security solution for enterprise networks

Innominate, a specialist in network security appliances, offers such a security solution with its mGuard product portfolio. One innovation of this integrated complete solution, based on proven standard technologies, is to reverse the approach for the implementation of remote maintenance. Up until now, a connection must be established by the service technician to the system. With the mGuard teleservice concept from Innominate, the connection is made from the system to the service. Thus, the connection to the machine is no longer initiated externally, but begins with the machine as an outbound connection to a previously defined remote peer. Thus, the typical access problems due to security policies and firewalls are resolved, as outgoing Internet-connections with clearly defined VPN tunnel partners are easier and safer to administer. The MGuard concept was specifically developed for use in industrial environments and combines the properties of a so-called stateful inspection firewall that monitors incoming and outgoing data packets according to predefined rules, with the possibility of safe and confidential communications via encrypted virtual private network connections (VPNs).

The right solution for each installation

In order to protect networks, production cells or individual automation equipment, Innominate offers the mGuard portfolio of diverse network security appliances that are easily integrable into Ethernet-based production networks. mGuard components for field use are ready to be integrated into decentralized systems as, e.g., external DIN rails or PCI cards. Furthermore, an interesting design variation for 19-inch environments with high availability requirements is the mGuard blade pack. With redundant power supplies and hot-swappable blade inserts, up to twelve systems or subnets can be individually networked and protected and scaled from 250 to 3000 VPN tunnels as a VPN gateway.

In addition to an integrated WebGUI for local administration, all devices feature centralized management through the Innominate Device Manager (IDM). This provides a template mechanism that allows the user to centrally configure and manage all its mGuard devices with highest efficiency. When installation is complete on the field side, the devices can be set up on an as-needed basis or via permanent VPN connections to the central service points of teleservice providers. Typically this is handled by the machine or system operator who can use the teleservice as needed and monitor the connection status at any time. Establishing a VPN connection, of course, requires a remote station at the central service site. Innominate has now designed a new system precisely for such remote stations to make this central hub for the connection to large quantities of field devices even more efficient to configure (see Figure 1).

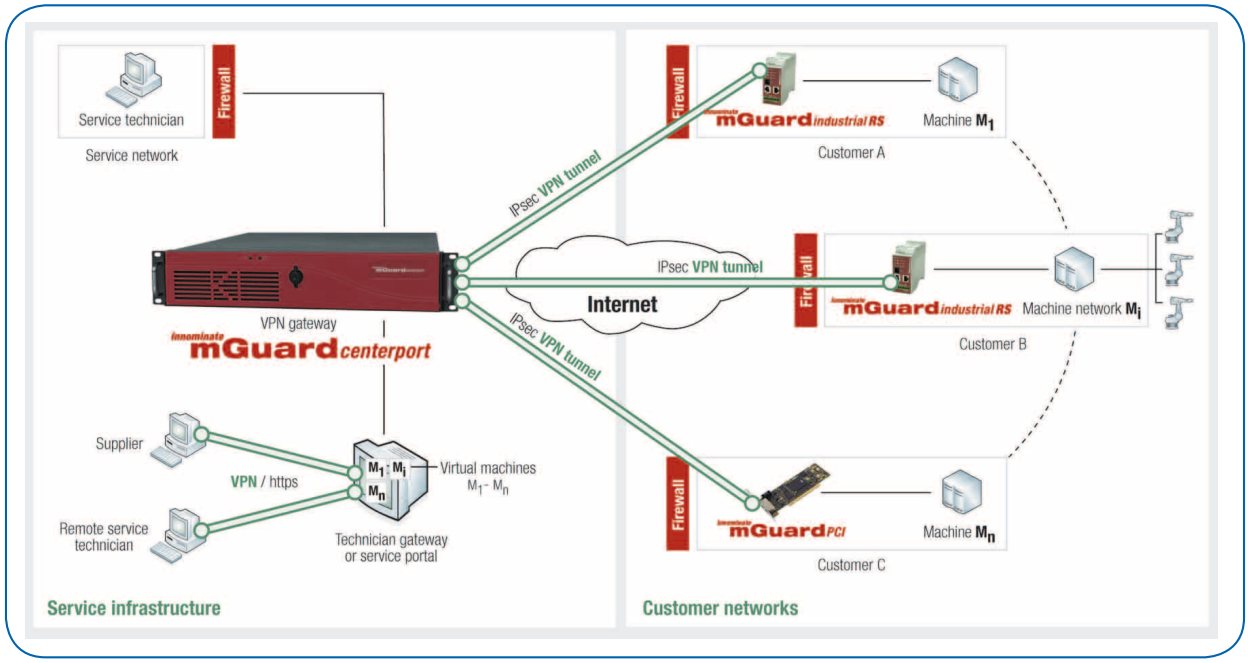

Figure 1: Efficient service infrastructure. Based on the Kontron KISS 2U industrial server, the mGuard centerport serves as a central gateway for mGuard field equipment with the specific requirements for building VPNs and maintaining secure virtual private network connections to a wide range of distributed industrial systems. Systeme.

New Firewall & VPN Gateway complements the mGuard Family

The new Innominate mGuard centerport in 19-inch format handles all high-end firewall and VPN gateway functions, which are needed for a secure connection to a very large number of decentralized field devices. The advantage of the new system is that all VPN connections are routed through a single public IP address. Until now, with the modular mGuard bladePack, up to twelve IP addresses where needed, with one IP address per blade slot. Configuration and administration are thus much easier with mGuard centerport, because one doesn't need to deal with load balancing between different gateway addresses, and just a single public IP address is required. Furthermore, instead of Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps) interfaces are now deployed, through which the mGuard Centerport can sustain 1000 simultaneous VPN tunnels, while achieving an encrypted data throughput of 300 Mbit/s — four times the performance of an mGuard blade. The mGuard centerport is fully compatible with all mGuard VPN field devices and the Innominate Device Manager, thus allowing for easy integration and installation. On the hardware side, one simply connects the service network to the rear-mounted LAN port and provides the WAN port with Internet access. Once the two redundant power supplies are provided with electricity, and after its initial startup via the integrated web interface, the gateway can then be administered with high automation via the Innominate Device Manager. Should the system be rebooted, up to 1,000 VPN tunnels can be rebuilt in less than 5 minutes due to the high system performance, thus ensuring maximum availability for teleservice applications.

"Six nines" in sight

For the new 19-inch solution, which is a node on the corporate network of the teleservice and thereby assures the availability of many machines and devices, high demands are placed on its hardware. The system should offer high performance for the efficient handling of up to 1000 VPN tunnels without significant delays. Second, the high-performance systems should also offer the highest possible MTBF (mean time between failures), because on such a server, platform requirements are placed that are comparable with those of carrier-grade telecom networks. Although it is not always necessary that the systems be designed with redundancy or have hot-swap modules, in terms of the quality of the components and board designs a solution is necessary that is designed for highest availability. Such a design should offer, for example, a redundant power supply and RAID support in order to give the most vulnerable components in computer systems the highest fail-proofing to ensure minimal downtime. "Ideally, systems should offer an availability as high as 99.9999 percent, in other words, Six Nines," says Torsten Rössel, Director of Business Development at Innominate. "We were searching for an affordable solution in that direction."

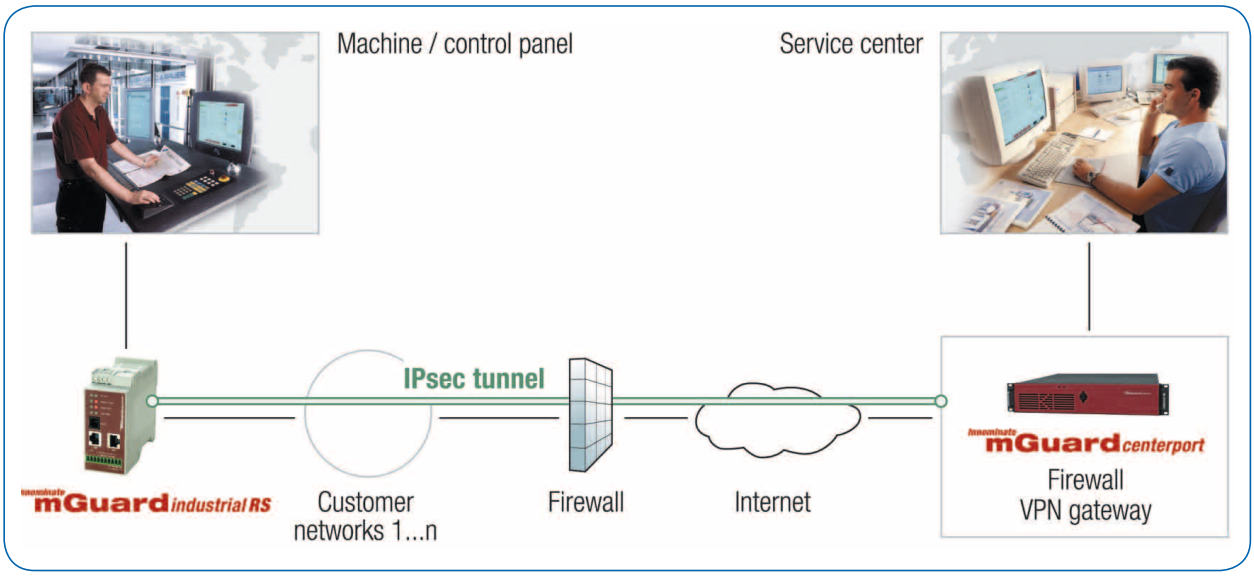

Figure 2: Scalably connected. With the new mGuard centerport, service centers and condition monitoring services can be simultaneously connected via encrypted VPN tunnels with up to 1000 globally distributed systems.

System hardware and components from a single source

Innominate has opted for the KISS server family (Kontron Industrial Silent Server) from Kontron, which is also used in the power system management by power supply companies, in the control technology for railways, in medical technology, and even in nuclear power plants and must be correspondingly highly available. Thanks to Intel® AMT support, they can even be optionally fitted with in-band and out-of-band monitoring functions and thus, with the exception of hot-swap capability of the modules, nearly all requirements essential in carrier grade telecom networks are fulfilled. For Innominate, equipped with redundant power supplies, Gigabit Ethernet and Intel® Core™ 2 Quad processor, the 19-inch / 2U KISS 2U Server is currently one of the smallest and fastest high-availability servers for long-term available and robust applications.

According to Torsten Rössel, Director of Business Development at Innominate, there were several reasons for choosing a hardware platform from Kontron. "Kontron is well known to us, and as a supplier to our parent company Phoenix Contact, already a proven manufacturer of industrial PCs. Other important considerations included a suitable range of models with upwards and downwards scalability, the possible design of the system as an OEM product with its own branding, the long-term availability of a precisely specified hardware configuration, product quality, and local support from a German manufacturer."

For Innominate, the server from Kontron was individually furnished with a space-saving PICMG 1.3 slot board, a high-performance backplane, 4-port Gigabit Ethernet card and a custom front-end design. With Kontron, the system and all components come from a single source, ensuring the highest compatibility and reliability of the system. The MTBF is 50,000 hours, which roughly corresponds to 5.7 years of continuous use. In addition, the server is available for at least 5 years from Kontron. Thus, a homogeneous hardware structure is made possible that allows for particularly efficient service for Innominate and also makes the investment in customer-specific hardware platforms especially safe.

KONTRON KISS 2U SERVER

Highly Configurable Kontron KISS 2U industrial server is used by Innominate as a specifically-designed high-availability OEM platform for high-end firewalls and VPN gateways. As COTS systems, the Kontron KISS-2U servers are individually equipped with PICMG 1.3 and PICMG 1.0 slot boards or Flex-ATX motherboards and are accordingly very flexibly expandable. Space-saving PICMG 1.x configurations can be very densely packed with up to five expansion cards. In the standard upgrade with Flex-ATX motherboards, two PCI expansion cards are possible.

OEM SECURITY APPLIANCES

Customer-specific Network Security Appliances based on the introduced Innominate mGuard and Kontron KISS technologies are realizable as further OEM variants. Interested? Feel free to contact us!

About Innominate Security Technologies AG

Innominate, a Phoenix Contact Company, is a leading supplier of components and solutions for controlled and secured communication in industrial networks. The German company specializes in the protection of networked industrial systems and the secure remote diagnosis and maintenance of machinery and equipment over the Internet. Its mGuard product line of network security appliances provides router, firewall, virtual private network (VPN), as well as quality of service (QoS) functionalities and helps with intrusion detection and antivirus protection.The mGuard portfolio is complemented by a highly scalable device management software. Innominate products are marketed worldwide under the mGuard brand through system integrators and OEM partners.

Further information can be found at **www.innominate.com**

About Kontron

Kontron, the global leader of embedded computing technology, designs and manufactures standards-based and custom embedded and communications solutions for OEMs, systems integrators, and application providers in a variety of markets. Kontron engineering and manufacturing facilities, located throughout Europe, Americas, and Asia-Pacific, work together with streamlined global sales and support services to help customers reduce their time-to-market and gain a competitive advantage. Kontron's diverse product portfolio includes: boards and mezzanines, Computer-on-Modules, HMIs and displays, systems, and custom capabilities.

Kontron is a Premier member of the Intel® Embedded and Communications Alliance.

For half-a-decade now, Kontron has been named a VDC *Platinum Embedded Board Vendor*. Based entirely on user feedback, industry professionals evaluate vendors on over 45 non-product related criteria. Kontron is only one of two companies to receive the Platinum award 5-years running.

Kontron is listed on the German TecDAX stock exchange under the symbol „KBC".

For more information, please visit: **www.kontron.com**

CORPORATE OFFICES

Europe, Middle East & Africa
Oskar-von-Miller-Str. 1
85386 Eching/Munich
Germany
Tel.: +49 (0)8165/ 77 777
Fax: +49 (0)8165/ 77 219
sales@kontron.com

North America
14118 Stowe Drive
Poway, CA 92064-7147
USA
Tel.: +1 888 294 4558
Fax: +1 858 677 0898
sales@us.kontron.com

Asia Pacific
17 Building,Block #1,ABP.
188 Southern West 4th Ring Road
Beijing 100070, P.R.China
Tel.: + 86 10 63751188
Fax: + 86 10 83682438
kcn@kontron.cn