Customer Case Study
Automotive

Secure remote maintenance for automotive companies

Summary

- FRIMO has long provided remote support via analog modems and telephone links, but as industrial computers have become more common in its operations, FRIMO found that analog systems no longer met its remote support needs
- FRIMO found that the mGuard industrial security device was secure and easy to use
- By using the mGuard as a centralized solution, FRIMO has created a uniform and standardized access solution for all its subsidiaries, simplifying operation and reducing administrative costs

Customer profile
FRIMO specializes in the development and manufacturing of production systems for high-quality plastic components for a wide range of applications. Today, the FRIMO network comprises 15 global locations with a total of 1,200 employees. FRIMO has many years of experience with remote service, especially in the automotive environment. Twenty years ago, machine operators were already supported by a remote service technician in the event of machine downtime via analog modems and telephone links. Despite the limited bandwidth of the analog 56 kbit/s modems, access to programmable logic controllers (PLCs) in the machines was still relatively efficient.

“The security requirements for a remote service solution are very high in the automotive sector. However, the benefits of rapid troubleshooting and the security features of our mGuard solution are very convincing,” says Axel Starflinger, IT Administrator at FRIMO.

Challenge: Troubleshooting and enhanced services from a distance
Automotive manufacturers and suppliers expect quick troubleshooting and maximum availability of machines from plant and equipment manufacturers. Remote maintenance solutions proposed for that purpose, however, often fail to fulfill the high security standards of IT departments. The equipment manufacturers at FRIMO have found a secure solution that not only requires less administration but is suitable as a centralized solution for a large number of subsidiaries.
Increasingly powerful industrial PCs have since taken over more and more functions in our machines. Analog connections are no longer sufficient to ensure remote maintenance for these computers,” says Axel Starflinger, IT Administrator at FRIMO.

Analog technology has meanwhile been replaced with broadband Internet access, which is used to establish tap- and manipulation-proof connections through virtual private network (VPN) tunnels. Thanks to the faster data connection between the customer’s plant and the manufacturer’s service technician, the machines’ industrial PCs can now be conveniently operated. Using virtual network computing (VNC) software, the entire screen content of the remote computer is transmitted and can be used by the service technician like a local PC.

FRIMO primarily uses remote service for rapid fault clearance. Additionally, expanded services are also available. As the support needs of its customers are continually rising, FRIMO intends to expand its remote service over time. “We adapt our machines to the specific requirements of our customers. With fast and secure VPN connections, we have access to all the devices in the machine. For example, our service allows us to remotely set up an extra checkbox in the PC’s visualization system or to adjust the parameters of a frequency converter,” explains Axel Starflinger.

**Solution: A secure, efficient and easy-to-use remote service solution**

FRIMO has integrated 80 mGuard remote service connectivity solutions from security specialist Innominate, a Phoenix Contact Company. In an initial attempt, though, FRIMO used a different broadband remote maintenance solution.

“Increasingly powerful industrial PCs have since taken over more and more functions in our machines. Analog connections are no longer sufficient to ensure remote maintenance for these computers,” says Axel Starflinger, IT Administrator at FRIMO.

Analog technology has meanwhile been replaced with broadband Internet access, which is used to establish tap- and manipulation-proof connections through virtual private network (VPN) tunnels. Thanks to the faster data connection between the customer’s plant and the manufacturer’s service technician, the machines’ industrial PCs can now be conveniently operated. Using virtual network computing (VNC) software, the entire screen content of the remote computer is transmitted and can be used by the service technician like a local PC.

FRIMO primarily uses remote service for rapid fault clearance. Additionally, expanded services are also available. As the support needs of its customers are continually rising, FRIMO intends to expand its remote service over time. “We adapt our machines to the specific requirements of our customers. With fast and secure VPN connections, we have access to all the devices in the machine. For example, our service allows us to remotely set up an extra checkbox in the PC’s visualization system or to adjust the parameters of a frequency converter,” explains Axel Starflinger.

**Solution: A secure, efficient and easy-to-use remote service solution**

FRIMO has integrated 80 mGuard remote service connectivity solutions from security specialist Innominate, a Phoenix Contact Company. In an initial attempt, though, FRIMO used a different broadband remote maintenance solution.

“The technology from a large manufacturer proved to be far too complex and expensive in daily operations. It was not an acceptable long-term solution. We tested various alternatives and decided to go with the Innominate mGuard. With the mGuard, we have found a very secure, efficient, and, above all, easy-to-use solution. The time we spend on configuration has been reduced from several hours to a few minutes,” the IT administrator says, describing his experience. Due to the uniform, standardized configuration templates for the mGuard, any configuration effort at the machine end is low.

**Configuring a VPN router in minutes**

Since then, if a machine needs to be equipped for remote maintenance, FRIMO uses mGuard technology exclusively. To set up the remote maintenance solution, a complete configuration template is read into the mGuard via an SD card. This defines almost all the required parameters. Then, the only items that need to be added are customer-specific entries for the VPN connection, the customer’s default router network, and the machine’s IP addresses. Address conflicts are avoided by mapping the real addresses of the machine network onto virtual IP addresses through the 1:1 network address translation (NAT) function of the VPN router. Additional adjustments to the machine’s internal address space are no longer necessary.

At its headquarters, FRIMO is deploying an mGuard bladeBase compatible with up to 12 mGuards in a 19-inch standard rack system. All technical parameters and authorizations are already set up so that a new machine can simply be added and connected without having to make any additional entries. All FRIMO locations are connected to the headquarters via an internal MPLS network. When servicing is required, a technician from any location obtains remote access to the customer’s machine via the blades in the headquarters using the VPN connection – depending on his or her authorization level. “With our centralized solution, we have created a uniform and standardized access solution for all our subsidiaries. This simplifies operation, and the administration costs are considerably less,” says Axel Starflinger.

**Results: A high security standard accepted in the automotive sector**

The FRIMO IT administrator confirms that machine operators are generally skeptical or hostile towards the idea of external access to their production networks. This is especially true for manufacturers and suppliers in the automotive sector. “Security
concerns are initially high. However, the benefits of rapid troubleshooting and the security features of our mGuard solution are very convincing,” says the IT administrator.

The mGuards integrate three coordinated security components on the basis of a hardened embedded Linux: a bidirectional stateful firewall, a flexible NAT router and a secure VPN router with IP security protocol (IPsec) encryption. The machine operators’ IT teams attach great importance to one protective aspect of the mGuard in particular: it prevents external access to the machine by default. A secure data connection can only be established with the explicit authorization of the machine operator via a VPN hardware switch. Access to the machine is thus always initiated by an outgoing connection controlled by the customer.

“The mGuard solution is suitable for industrial use. It is secure and easy to administer. Innominate’s support staff are very dedicated and will always find a solution, even for complex problems. For example, we recently had a large accumulation of open sessions in our MPLS network and suspected a remote service problem. A specialist from Innominate checked the log file of the central mGuard. His analysis helped us to find the problem within a few hours,” says Axel Starflinger, summarizing the good experience he has had.

“With our centralized solution, we have created a uniform and standardized access solution for all our subsidiaries. This simplifies operation, and the administration costs are considerably less,” says Axel Starflinger.