Customer Case Study

Machine building

Engineering company chooses mGuard to protect and maintain network

Summary

• Big Drum Engineering needed a system that would guarantee constant availability of its network for customers like Nestlé and Unilever.

• The company implemented the mGuard from Innominate, a subsidiary of the Phoenix Contact Group, to provide secure, reliable connectivity.

Customer Profile

Big Drum Engineering develops, constructs and installs filling machines for the international ice cream and general foods industry. The company's machines fill liquid products in containers from 50 ml to 5 liters with an output of up to 50,000 units per hour.

Challenge: Ongoing monitoring of machine parameters

Big Drum Engineering adapts to trends set by major companies in the food industry. For 100 percent system availability, customers expect a permanent online connection as a prerequisite for better service standards, preventive maintenance, and higher security levels.

In this industry, any downtime can quickly lead to significant losses. “Large customers such as Nestlé and Unilever expect us to deliver services in accordance with total productive maintenance (TPM). The demand from other companies has also increased strongly in this area,” said Andreas Itter, sales and marketing manager at Big Drum Engineering. This requires constant monitoring of the machines, the transmission of key parameters to the machine manufacturer's headquarters, and ongoing control of data by service technicians.

The company has relied on remote service for a decade. All systems with programmable logic controllers from Allen-Bradley have been routinely equipped with a remote service module. Meanwhile, there were already over 100 of these systems in use. As the demand for remote service increased, Big Drum Engineering began searching for a remote system that would provide security while being constantly available.

continued >>
Solution

For secure online connectivity, the machine manufacturer chose the mGuard from Innominate, a subsidiary of the Phoenix Contact Group. The mGuard’s flexible configuration allows for the provision of machine-specific and customer-specific services.

The mGuard meets the demand for need-based maintenance, a recent trend in the sector. Some machine components are subject to greater wear than others. Therefore, it is necessary to keep a closer eye on these machines, with a particular focus on continual monitoring of the servo drives. Sensors register various factors, including the temperature of the servo motors, and data can be continuously transmitted to the machine manufacturer. If predefined tolerance values are exceeded, an automatic e-mail can be sent with a warning message to the service team. Rising temperatures of the servo motor are an early indication to the service technician of possible problems due to wear. A timely inspection of the servo motor can prevent interruption, avoiding system downtime.

To ensure 100% system availability, large companies expect a permanent online connection as a prerequisite for better service standards, preventive maintenance, and higher security levels.

More services through the connectivity platform

During startup, the system’s continuous online connection is an advantage. Frequently, 100% functionality of the new system can only be verified on-site under real production conditions. Through the continuous online connection, specialists can access the startup remotely. During the warranty phase, service technicians can introduce other optimizations based on the online machine log, and immediately handle problems. In the final service phase, remote service allows ongoing monitoring of machine parameters and troubleshooting. This enables permanent monitoring of deviations in filling volume, compliance with predefined opening and closing times of the valves or machine-specific cycle times.

Improved system availability through remote service

Secure broadband IP/VPN connections are used for online monitoring. These are significantly more reliable and stable compared to the previous modem connections. They also cover ever-increasing data volumes and expanded services. “We have had very good experience with the mGuard solution. The technology is very reliable, it ensures the highest security standard and Innominate’s service is very good,” said Itter, who gives high marks across the board for the mGuard solution. Because Big Drum experienced difficulty in communicating with other manufacturers in the past, Itter emphasizes the value of the permanent availability of his contact person at Innominate.

“The remote service further increased system availability, and we were able to reduce fault-clearance times by 70 percent. With access to remote data, not only can we troubleshoot faster, but we are significantly less expensive for our customers due to the elimination of travel costs”

Secure IP/VPN connections

Several functions are integrated into the mGuard to protect IP data connections. These include a VPN-enabled Ethernet router and a configurable firewall with dynamic packet filter. Service technicians connect to plant operators via a virtual private network (VPN). The mGuard takes on the role of the VPN

continued >>
gateway in this process, connecting service technicians to the plant network in a common network via the Internet. The use of cryptographic protocols safeguards confidentiality and authenticity. The process uses hardware-accelerated encryption via 3DES (168 bits) or AES (128, 192, 256 bits) and the IP Security Protocol (IPsec).

The integrated firewall helps to seal off Big Drum Engineering’s system from the customer’s production network. The configurable stateful packet inspection firewall protects against any unauthorized access. The dynamic packet filter scans for new connection attempts based on their addresses and ports of origin and destination, blocking any unwanted traffic. The parameters of authorized connections are stored in a connection tracking table until they are terminated and all corresponding (response) packets are automatically recognized and accepted.

**Results: Increased customer acceptance**

Overall, the mGuard has been of great service to Big Drum Engineering. Itter reports that many customers’ IT departments were initially reluctant upon hearing that interventions would come from outside their corporate network. However, acceptance has increased with the verifiably secure connectivity solution. The mGuard contains security features developed specifically for the field of industrial systems, a key factor that end customers appreciated.

**CIFS Integrity Monitoring provides security**

Common Internet File System (CIFS) monitoring is an industry-suitable alternative to antivirus software. CIFS monitoring can detect any change in a Windows-based system (controller, control unit, PC), which can indicate if it has been attacked and/or manipulated by malware.

CIFS monitoring provides improved protection based on the protocol family CIFS/SMB (Common Internet File System/Server Message Blocks) for file shares frequently used for data exchange within the environment. For example, the infamous Stuxnet and Conficker worm used these gateways for their dissemination. In addition, CIFS monitoring prevents damages from zero-day attacks. Traditional antivirus software needs to be updated to recognize a new vulnerability. On the other hand, if the vulnerability modifies the system, CIFS monitoring will recognize changes, additions or deleted files during the same-day scan, even if a new malware signature has not been created yet.