Customer Case Study

Worldwide remote service has become more secure

Eliminates risk of tampering

Summary

- ZIPPE Industrieanlagen has long offered its customers remote service, but the original system did not meet the demand for real-time diagnosis and problem solving.
- ZIPPE turned to the FL mGuard industrial security device for a modern approach.
- With the mGuard’s broadband and secure IP/VPN connections, ZIPPE can provide real-time diagnostics and troubleshooting.
- The investment in the hardware easily pays for itself, when compared with traveling to a distant country to provide in-person support.

Customer profile

ZIPPE Industrieanlagen is an equipment manufacturer that provides systems for the glass industry in 75 countries. ZIPPE designs and manufactures state-of-the-art, proven plant technology such as scraper conveyors, crushers, glass batch chargers, and glass level controllers. All systems are unique and tailored to the customer’s requirements.

Challenge: From commissioning to troubleshooting

ZIPPE has provided remote service to its customers for the past 20 years. The remote service enables them to react quickly when system errors occur, and to provide an additional range of services. This service is more now powerful and secure than ever before, thanks to new technologies.

Solution: Real-time diagnosis and problem solving with mGuard technology

ZIPPE currently uses remote service for 200 installations in 75 countries. Every new plant is now equipped with the mGuard infrastructure by Innominate, a Phoenix Contact Company. This technology facilitates remote maintenance via broadband and secure IP/VPN (virtual private network) connections. “Real-time problem diagnosis and problem solving are becoming increasingly important, because spontaneous, unpredictable errors cannot be ruled out in such complex systems. The customer often finds it difficult to carry out a quick, targeted problem analysis and to introduce and implement the necessary troubleshooting measures,” said Thorsten Zimpel, head of process control system at ZIPPE Industrieanlagen GmbH.

Specialists can provide worldwide support for the commissioning of every system from their headquarters in Wertheim in the north of Baden-Württemberg. The use of broadband connections has
ZIPPE specialists can provide worldwide support for the commissioning of every system from their headquarters in Wertheim in the north of Baden-Württemberg.

opened new possibilities for remote service. In a modern plant, a software update alone can easily amount to several hundred MB. During the warranty period, the performance of the system is continuously optimized via remote service. Even after the warranty period has expired, ZIPPE can use online access to resolve errors or provide additional maintenance and services in line with the customer’s order.

“Remote service means that we can employ less staff on-site, while expanding our service offering at the same time. In case of more distant system locations, the investment in the technical components already pays for itself after only one saved trip,” stated Zimpel.

Improved system performance
Modern ZIPPE systems, such as fully automatic glass batch production systems, are controlled and monitored by automation devices, weighing and dosing computers, and networked control systems. The automation systems take over the control of cyclic processes and accurate dosing and weighing of raw materials. The control system includes the visualization of the system with manual control, the monitoring and reporting system, data entry, recipe handling, reporting, and production data archiving.

The control system provides numerous “adjustment screws” to fine-tune such complex systems for optimum performance.

Remote service makes it possible to retrieve statistical functions, which can control product quality. The analysis of this data indicates whether the scales are still within the tolerance range, dispensing services and dispensing times become visible, and operating protocols provide an insight into the control of the system. Many customers request ZIPPE technicians to help interpret this data and the resulting measures derived from it. The technicians remotely configure and optimize all relevant parts of the system, as well as the software modules used to plan and organize maintenance. But before service technicians can access the system online, an important security feature of the mGuard technology comes into play: The customer must first use a hardware switch to enable any online access.

Security features protect the customer network
The basic package of the mGuard solution includes a VPN-enabled Ethernet router with IPsec (IP security protocol) encryption, a configurable firewall, and the VPN hardware switch. After online access has been enabled via the hardware switch, the mGuard establishes a VPN tunnel. This tunnel is safe from eavesdropping and manipulation between the customer-side system and the service technician at ZIPPE, using hardware-based encryption. In addition, the firewall isolates the systems from the customer’s network.

After approval by the customer, a connection is established between the customer-side system and the service technician at ZIPPE, using a VPN tunnel that is safe from eavesdropping and manipulation. In addition, a firewall ensures that the systems are isolated from the customer’s network.
Results: Easy and dependable security, even with older Windows versions

“We have been convinced by this total security concept provided by the Innominate solution. It is designed for the industrial environment, administration is relatively easy, and we can integrate the DIN rail-mountable metal housings into our control cabinets,” Zimpel explained. He also referred to the excellent support provided by Innominate, stating that the company always helped very quickly when problems arose. The possibility of also integrating the secure remote service technology into existing systems without “default gateway or standard gateway” was important to ZIPPE. The “Remote VPN NAT” function is used to map the entire data traffic, which travels over the VPN, on the local network via the configured address. As a result, a default gateway is not required.

In the near future, a new mGuard Firmware feature will also support remote service within legacy systems. Until now, plant operators have refused access to legacy systems running Windows NT or Windows 95 for security reasons. mGuard CIFS Integrity Monitoring, an optional mGuard Firmware module, provides an industrial-strength alternative to antivirus software (see sidebar on CIFS Integrity Monitoring). In connection with the firewall, which isolates the customer network, even poorly secured legacy systems can also achieve VPN.

CIFS Integrity Monitoring

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). Such a change can indicate if the system has been attacked and/or manipulated by malware.

CIFS monitoring provides improved protection based on the Common Internet File System/Server Message Blocks (CIFS/SMB) protocol family for file shares frequently used for data exchange within the environment. The infamous Stuxnet and Conficker worm used these gateways for its dissemination.

In addition, CIFS monitoring prevents damage from zero-day attacks. Traditional antivirus software needs to be updated to recognize a new vulnerability. However, 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.