Cloud-based remote maintenance in plant engineering

Remote service ensures a quick solution for almost 80% of disruptions

Summary

- To work efficiently, plants must be continuously available. If disturbances occur, quick assistance via remote maintenance is essential.
- The dilemma: plant operators tend to avoid such maintenance access for security reasons. Small- to medium-sized manufacturers, in particular, shy away because they don’t have the knowledge or resources to invest in a high-technology infrastructure to allow secure remote access.
- A secure cloud platform addresses this conflict. It can offer the latest security standard, meaning that plant manufacturers do not need their own infrastructures.

Customer profile

STOPA Anlagenbau GmbH is a medium-sized independent equipment manufacturer based in Achern-Gamshurst, Germany. Founded in 1963, STOPA is now one of Europe’s leading providers of automated storage and retrieval systems. The central business area, storage systems, is flanked by the engineering and steel construction divisions, as well as the design and implementation of parking systems.

More than 200 employees at the Achern-Gamshurst location primarily manufacture storage systems for a variety of goods, with a focus on sheet metal and long materials. STOPA references include over 1,800 completed projects worldwide – including both integrated automation modules for processing machinery and stand-alone equipment for various storage tasks.

This range of production activities is supplemented by retrofit and after-sales services. STOPA provides national and international customers with the highest degree of availability and return on investment.

Challenge: Gaining a competitive edge through excellent customer service

“As an equipment manufacturer, our core competency does not lie in constructing complex IT infrastructures, but service-friendly plants for our customers,” explains Ettore Caurla from the Customer Service Department of STOPA Anlagenbau GmbH.

STOPA’s storage systems need to ensure a quick and efficient material flow for operators. If a storage system is disrupted, the entire production process can be quickly compromised. Common causes of disruptions include plant and operative problems, including a proper handling under Windows or the configuration of Interbus or Profibus applications. Many problems can quickly be solved online or by telephone.

Service and system availability have always played a decisive competitive role for the manufacturer. For this reason, remote service has been a common means of support at STOPA for 20 years. Initially, STOPA used analog modems to remotely access customer plants. However, with the rising scope of automation
technology services and data volumes, this was no longer enough. For example, a slow connection could lead to a situation in which the sensor data status changed during transmission. So the modems were replaced by broadband IP connections.

“1,000 of our 1,600 plants are connected via remote service. Only smaller and older plants have not been included. New plants are fully equipped with remote service features,” reports the service employee.

The STOPA Customer Service Department systematically evaluates the duration and success rate of the remote service. It received 5,000 calls last year. These included requests for appointments, documents, or other service information. Remote support was initiated for 600 calls to resolve disruptions. In 78 percent of these cases, the problem could be conclusively resolved within 24 hours. Only the remaining 22 percent required longer processing times, such as cases where spare parts for defective devices were not available locally.

**Solution: New technology reduces fault-clearing times by 50%**

Previously, the STOPA had used a modem-based service solution for remote support. The average connection time per assignment was 75 minutes. Establishing the connection and the exchange of extensive program files with Siemens Step 7 alone required 20 minutes. A rather complicated handling also extended the support time.

Converting to mGuard virtual private network (VPN) technology from Innominate, a Phoenix Contact Company, reduced the average connection time to just 37 minutes. Here, establishing the connection initially required 30 seconds but was reduced to just a few seconds after a software update. Basically nothing changed in terms of the accessibility of the Simatic S7 or S5 systems. The processes merely became more streamlined due to the intuitive operation. “The connection time for remote service is an important variable, because the faster we can help the customer, the more cases the support team can attend to,” says Ettore Caurla. Not only was the IP connection technology replaced, but with the cloud platform “mGuard Secure Cloud,” a new remote service approach was introduced.

**Remote service via a cloud platform**

“We were looking for an easy-to-manage and economic solution. It had to ensure the highest security standard for our customers. At the same time, we did not want to deal with complex security architectures or the configuration of VPN clients, proxies, and firewalls,” explains the STOPA service technician.

From the perspective of the plant manufacturer, setting up an in-house security infrastructure would be too costly: “State-of-the-art security requires a reliable and fail-safe infrastructure, disaster recovery, and ongoing updates. Due to the high infrastructural and personnel costs involved, these factors are not economically feasible for a medium-sized manufacturer,” says Ettore Caurla.

He became aware of the mGuard technology from a business partner, Trumpf, a leading German manufacturer of machine tools and laser systems. “The cloud solution is the perfect approach. The mGuard hardware is already preconfigured for use. Just two outgoing ports need to be set up once for customer-side integration. That’s it. We do not intervene in the customer’s IT, nor does the customer have to install any software,” emphasizes the service technician. As the supplier of the cloud platform, Innominate has longstanding experience in security solutions for industrial networks and secure remote maintenance via the Internet.

In the mGuard solution, a bug and tamperproof VPN tunnel is established with hardware-based encryption between the customer’s plant and the service technician. The connection is established via Innominate’s mGuard Secure Cloud, a turnkey VPN infrastructure for operators and plant and equipment manufacturers. The cloud platform is operated in a German data
The operator retains control
Having set up 1,000 installations, the STOPA service technician names the most important requirements for a remote service solution: “For the operator, system availability has become even more important in recent years. For this reason alone, operators are willing to allow external access. At the same time, they want to retain control. For us as a manufacturer, the costs and efficiency level are decisive factors.”

Ettore Caurla has extensive experience with various VPN technologies from a previous job as an IT administrator: “Centralized IT demands reliable protection of one’s own plants. Especially in large companies, access to the in-house network is therefore largely restricted. In addition, many security requirements for authorization of remote service connections make handling extremely inefficient.” He cites the example of security tokens that generate a new, one-time password every ten seconds. Once the connection is made, the password has often already expired. In other cases, an IT employee or the supervisor must be called in to enter the password. Such processes make customer support difficult and ineffective.

The STOPA service technician finds Innominate’s secure cloud approach much more efficient – yet still very secure: “The machine operator must first enable the connection with a VPN hardware switch. It can only be initiated from the plant operator’s network. While the connection is being established, an indicator light blinks. Once the connection has been made, this light is permanently illuminated. One push of the switch button is enough to interrupt access. “This ensures that there is always an operator on site. For service access, no one can be endangered (safety). What’s more, the operator always maintains control over access to his network because a connection is only possible after his consent with the hardware switch (security).”

Results: The cloud approach is both cost-effective and efficient for the manufacturer
The service technician emphasizes that customized solutions are impossible with over 1,000 plants. Acceptance for the uniformly utilized mGuard technology is also very high due to the operator’s exclusive and permanent control over the VPN connection. Even 20-year-old Simatic S5 systems can be remotely serviced via Ethernet adapter:

“This cloud approach is perfect for manufacturers who want to maximize their efficiency: quick connection establishment, ease of use, and a security level that only large companies could otherwise attain. Because no in-house infrastructure is required with the cloud platform, we save about 30-40 percent of the costs,” says Ettore Caurla, summing up the advantages. In so doing, he stresses the good collaboration with the supplier: “Innominate is very customer-oriented. The annual mGuard User Conference hosted by Innominate with diverse practice-based reports on secure remote maintenance is also very helpful to us.”

Remote maintenance as a cloud solution
The mGuard Secure Cloud provides medium-sized machinery and system manufacturers and their customers with a turnkey VPN infrastructure. The cloud platform is operated in security-certified data centers in both the U.S. and Germany. The cloud solution avoids any user-side problems with the configuration of certificates, NAT, proxies, firewalls, etc. Neither the manufacturer nor the plant operator needs to install any additional software. The mGuard VPN technology is based on the IPsec security protocol with high-level encryption, allowing the mGuard to ensure the confidentiality, authenticity, and integrity of all information and data transmitted between service technicians and machines.

Because no technical details need to be clarified, the remote service application is available within a few hours via a secure VPN connection. New mGuard field devices for the integration of further machines and systems are put into service using a preconfigured SD card. The VPN configuration is automatically uploaded, saved, and activated on the mGuard from the SD card, allowing the customer’s machinery to go online with minimal effort. All operating processes and administrative tasks can be taken care of within the mGuard Secure Cloud publicly via a web browser.