Secure cloud-based remote maintenance and engineering

Plants that work efficiently must be continuously available. When disturbances occur, quick assistance via remote maintenance is essential, but operators often avoid maintenance access for security reasons. Manufacturers shy away from investing in a infrastructure that constantly needs to be state-of-the-art.



SOURCE: INNOMINATE

The equipment manufacturer STOPA ensures the highest possible availability of its storage systems via remote service.

A SECURE CLOUD PLATFORM can address this conflict between plant operators that avoid remote maintenance access for security reasons, and the need to invest in a state-of-the-art security infrastructure. New solutions can now offer the latest security standards, meaning that plant manufacturers do not require their own infrastructure.

"As an equipment manufacturer, our core competency does not lie in constructing complex IT infrastructures, but service-friendly plants for our customers," said Ettore Caurla from the Customer Service Department at STOPA Anlagenbau GmbH, a leading European provider of automatic storage and retrieval systems.

Avoiding 80% of the disruptions

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 of the 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, customer plants were remotely accessed using analog modems. However, with the rising scope of automation technology services and data volumes, this was no longer enough. Slow connections led to a situation in which the sensor data status changed during transmission, for example. So the modems were replaced by broadband IP connections. One service employee reported that 1,000 of its 1,600 plants are connected via remote service. Only smaller and older plants have not been included, and new plants are fully equipped with remote service features.

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% of these cases, the problem could be conclusively resolved within 24 hours. Only the remaining 22% required longer processing times, for instance due to spare parts for defective devices not being available locally.

Reducing fault-clearing times

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

With the conversion to mGuard VPN (virtual private network) technology from Innominate, the average connection time was reduced 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 was 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," said Caurla. Not only was the IP connection technology replaced, but with the cloud platform "mGuard Secure Cloud", a new remote service approach was introduced.



SOURCE: INNOMINATE

The operator retains control. VPN connections can only be established from the machine outwards using a hardware key switch.

Remote 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," said Caurla.

According to a service technician working on the system, "The cloud solution is the perfect approach. The hardware is already pre-configured 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."

Using this solution, a bug and tamper-proof VPN tunnel is established with hardware-based encryption between the customer's plant and the service technician. The connection is established via the company's Secure Cloud, a turnkey VPN infrastructure for operators and plant and equipment manufacturers. The cloud platform is operated in a German data center implementing high security and privacy standards.

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."

From a previous job as an IT administrator, Caurla has extensive experience with various VPN technologies: "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 the 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).

Cost-effective and efficient

The service technician emphasizes that with over 1000 plants, customized solutions are impossible. 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% of the costs," said Caurla.

*Application case study by **Innominate Technologies**.*