Water/wastewater

Customer case study

Secure remote access to SCADA networks via the cloud

Considerable relief during maintenance

Highlights

- Hermes Systeme GmbH supports industrial and municipal customers in complex applications, such as designing SCADA systems
- To support customers without incurring travel costs, Hermes Systeme needed a remote maintenance system that ensured a secure connection
- The mGuard Secure Cloud gives Hermes Systeme a flexible and cost-effective solution to securely access end customer applications

> "We can remedy about 80 percent of all the problems completely by means of remote access."
>
> **– Christian Nölker, electrical engineer**

Customer profile: Hermes Systeme GmbH

All machine operators want their machines or systems to operate at the highest level of availability. For its remote maintenance concept, Hermes Systeme GmbH relies on the Phoenix Contact cloud as a flexible and cost-effective solution for secure access to the end customer applications (lead image).

The employees of Hermes Systeme GmbH, located in Wildeshausen near Bremen, Germany, develop innovative solutions for MCR and automation technology. In addition to system modernization, their range of services comprises maintenance and repair of the existing technology, as well as supply and installation of new systems. Hermes Systeme focuses on industry and building automation, along with water technology, swimming pool technology, wastewater treatment technology, cooling technology, information technology, and central control engineering.

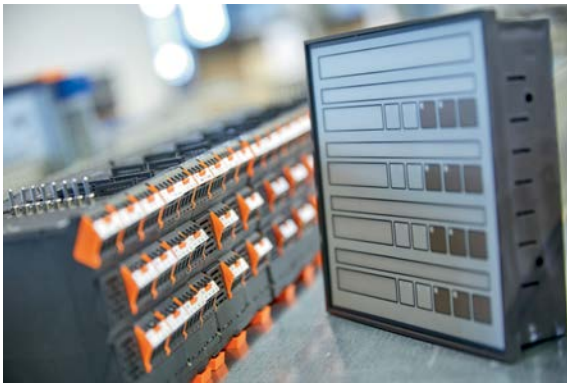

Figure 1: Some SCADA systems use an I/O station developed by Hermes Systeme.

As a system integrator, the company has supported industrial and municipal users for more than 30 years in many applications, such as implementing SCADA systems. Here, an I/O station designed by Hermes Systeme is used (Figure 1).

Hermes Systeme specializes in the development of proprietary SCADA solutions that control and monitor the processes. In water management, this can be small pumping stations and also complex distribution systems (Figure 2). The company has already been involved in many control projects, from simple pump control to large-scale projects. The comprehensive services include research, analysis, programming, installation, and troubleshooting in the process systems of the plants.

003955A 6.18

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

Figure 2: System integration experts create complex control cabinets.

Challenge: Getting the competitive edge with remote maintenance

"Nowadays, systems without remote maintenance technology are no longer competitive, because every operator requires high availability, which means that any interference must be removed as quickly as possible," Ingo Hermes, executive vice president, reports.

"It is not enough to look at the technical parameters and prices to make the right choice of remote maintenance technology," Christian Nölker, electrical engineer, emphasized. With an increasing number of systems, managing the online accesses and configuration of the remote router stations can become time-consuming.

Other issues to consider include secure authentication, managing customized access, and configuration data. "We were looking for a supplier offering a solution for easy management of the systems as well as of the service personnel," Ingo Hermes explains. "It was also important that this was a renowned manufacturer in order for our customers to accept the remote maintenance concept."

Solution: Using the cloud solution is free

Because of these factors, the decision-makers chose Phoenix Contact's complete solution for remote maintenance. These mGuard security devices provide secure access to the corresponding SCADA network for the service engineers (Figure 3).

The primary focus is not only on the fast removal of errors, but also on a transparent security standard requested by the system operator to accept remote maintenance. Using the Phoenix Contact cloud is an optimal solution for the relevant applications and saves resources of Hermes Systeme. This is possible because using the cloud is free of charge and because Phoenix Contact is responsible for providing the cloud functions. Using a cloud-based solution offers the following advantages:

- No hardware costs for remote maintenance center
- Easy-to-use cloud services via a web browser
- Stationary and mobile access is possible
- Many service engineers can access at the same time
- Phoenix Contact is responsible for cloud security
- Reduced capital commitment and labor costs
- High availability
- Phoenix Contact is responsible for scaling and adapting performance

In the event of maintenance, the service engineer can immediately and remotely obtain information on the system's operating state. The engineer simply presses a button to evaluate a large number of log files and other historical data that give information about the error cause. The records from the system sensors indicate errors and suggest options for optimization at the same time. SCADA systems usually consist of one or more controllers and a graphical user interface.

Figure 3: Hermes Systeme GmbH, located in Wildeshausen, Germany, has supported users implementing SCADA systems for more than 30 years.

"We can remedy about 80 percent of all the problems completely by means of remote access," explains Christian Nölker, electrical engineer and programmer at Hermes Systeme. "To do so, our service engineers view the operator's screen of the system on their computer and then work on error removal together with the employee on-site." (Figure 4).

Easy management of systems and service personnel

The solution comprises system and service personnel management in addition to a high IT security standard. The required configuration of the terminal devices is automatically generated in the cloud and

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

Figure 4: The FL mGuard RS2000 combines IT requirements and robust hardware for harsh industrial environments.

downloaded to the devices. Any processes, such as VPN (virtual private network) configuration, routing settings, and certification management, are implemented using the cloud. "The Phoenix Contact cloud as a portal manages the increasing variety of different maintenance environments of the systems and automatically provides the right environment to the service engineer," Christian Nölker is pleased to say. Every service access starts a temporary virtual machine, which is deleted again afterwards. This machine also allows for parallel operation of different software generations. For Hermes Systeme, this type of remote maintenance has proven to be an efficient solution that ensures increased system availability for the company's customers.

Robust solution for harsh industrial environments

"We were looking for a solution that uses the Internet to dial into the SCADA network of the system. At the same time, we wanted to protect the network against unauthorized access," Christian Nölker continues. Ideally, the solution was suited to an industrial environment. "However, the majority of security applications on the market have been developed for the office environment," Nölker explains. Hermes Systeme has opted for the FL mGuard product range, so the security appliances meet all the requirements of the industrial environment. This series comprises security components with integrated firewall, routing, and VPN functions for industrial networks. The devices combine IT requirements and robust hardware in a metal housing for harsh industrial applications.

"The FL mGuard RS2000 version we use can be mounted on a DIN rail and features a 24 V DC power supply. Based on the local situation, we either use the RJ45 version or the mobile network version to connect the system to the cloud," the programmer continues. The FL mGuard RS2000 acts as a secure gateway that protects the system against unauthorized access.

Therefore, the SCADA network can be connected directly to the Internet and thus to the cloud. The service engineers use a VPN software client to establish a connection to the cloud. The VPN function ensures that only authorized persons can initiate communication using the corresponding access data. If the VPN connection has been set up, it works like a direct connection to the local network. In this way, the programming software of the controller recognizes the security devices and can simply connect them.

Results: Secure remote access

Modern plants are often composed of complex machines and systems with a high level of automation. As digitization in the industrial environment increases, a rising trend can be expected. These applications must have IT-level security, based on both the users' and the systems' requirements, that builds up suitable protection against the typical attack vectors, such as the Internet. Access security is a constant process that can be operated only by new security architectures — such as the Phoenix Contact cloud — that the user can control.

High level of security in any application area

The new generation of fanless industrial security routers ensures reliable security and performance in a compact metal housing, which can be installed on a DIN rail. The components have an SD card slot for easy device replacement and connections for inputs and outputs. Based on a robust embedded Linux operating system, the RS400x series includes four coordinated security components:

- A bidirectional stateful inspection firewall with conditional firewall
- A DMZ port for an additional, shielded network (variant)
- An extremely secure VPN gateway
- Optional protection against malware using CIFS Integrity Monitoring

The RS200x series devices are designed for use in the field as an industrial VPN router, where they can be used directly on the machine or as central security components in branched networks. They have up to two parallel VPN tunnels, a stateful inspection firewall, an integrated switch (variant), and flexible routing functions.

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com