System integrator improves customer service with secure industrial VPN

Summary

- Morehouse Engineering, an engineering firm in New Jersey, had traditionally used dial-in Ethernet modems to provide customers with remote service, but the aging phone lines were proving unreliable.

- The company needed a new system that would:
  - Accommodate the customer’s needs to remotely manage their facility
  - Allow Morehouse Engineering to remotely connect to the PLCs with the programming software
  - Protect the system from Internet-based threats

- After switching to the FL mGuard, Morehouse Engineering can now quickly and securely connect to the plant network and go online with the processors.

Customer profile: SCADA expertise

Morehouse Engineering, Inc., is an engineering firm located in Hopewell, New Jersey. Since 1993, the company has been involved in a variety of control projects ranging from basic pump control to instructional tools for laparoscopic surgery. Today Morehouse Engineering provides clients with full service, from research, analysis and design to fabrication, programming, installation and troubleshooting of plant process systems.

One of Morehouse Engineering’s specialties is designing proprietary Command and Control SCADA systems. SCADA, which stands for Supervisory Control and Data Acquisition, is the term used for systems that monitor and control various processes. These processes can be as simple as a small pump station to a distribution system that covers thousands of square miles. SCADA systems are used in many industries, such as water/wastewater, oil and gas, electricity, and transportation.

Any SCADA system typically uses one or more Programmable Logic Controllers (PLCs) and a Graphic User Interface (GUI). The PLC portion can consist of a single small unit with a couple dozen input/output (IO) points or a hundred controllers with thousands of IO points. In these larger systems, the various PLCs may be located in a single plant or scattered over an entire county.

The GUI is the visual interface that the operator uses to monitor and control the process. This is usually a program running on a PC but often includes small operator interfaces located near the process equipment. All of these components are all connected, and this connection is very often a standard Ethernet network. Ethernet offers a resilient standardized and economical communications platform that is being used in all industries.
Morehouse Engineering's SCADA systems make the most of the PLC and GUI capabilities. The SCADA systems have online troubleshooting and complete Web-enabled access. The SCADA systems are often integrated with historical databases. The historian provides the basis for efficiently recording and managing large volumes of time-stamped data for analytical evaluation.

Morehouse Engineering deploys robust, reliable, and configurable SCADA systems across the area in a number of different applications. To maintain these systems, and troubleshoot the problems that arise, engineers could spend time and money traveling to the sites, or they could remotely access them via phone or the Internet.

Figure 2: The FL mGuard RS2000 can be mounted on a DIN rail and uses 24 V DC power, making it better suited for industrial installation than VPNs designed for commercial use.

Challenge: Remote technical support

As a systems integrator, Morehouse Engineering is frequently called upon to troubleshoot problems at various plants. Matt Maloney, Systems Engineer at Morehouse Engineering, Inc., stated, “Our customers have come to expect outstanding technical support.”

In the past, Morehouse Engineering used remote access dial-in Ethernet modems to go online with the PLC processors with many clients. Recently, however, it has found telephone lines are becoming troublesome. Phone systems’ aging copper lines are more prone to noise and connection problems, especially with data. Minor noise or static is not a problem when two people are talking, but it can distort data communications. The slower speed also proves to be a frequent problem. Morehouse needed more reliability to ensure the best service possible to its customers.

One customer, a water treatment facility, was somewhat ready for Internet-based remote access. The original SCADA network was connected directly to the Internet, which allowed the operating staff to easily monitor the plant from home using pcAnywhere. However, being connected directly to the Internet poses tremendous security risks, both from hackers and from viruses and malware. Furthermore, this approach prevented the PLC programming software from properly connecting to the PLCs, as the software is not designed to deal with the complexities of Internet traffic.

Morehouse Engineering needed a solution that would allow its staff to connect to the plant’s SCADA network through the Internet, but protect it from unauthorized access.

Figure 3: Any SCADA system typically uses one or more Programmable Logic Controllers (PLCs) and a Graphic User Interface (GUI). The GUI is the visual interface that the operator uses to monitor and control the process.

Solution: Access for the industrial environment

The new system would need to provide remote access that could:

A. Accommodate the customer's needs to remotely manage their facilities
B. Allow Morehouse Engineering to remotely connect to the PLCs with the programming software
C. Protect the system from Internet-based threats
With the installation of the mGuard RS2000, Morehouse engineering can quickly and securely connect to the plant network. The industrial VPN has a more reliable connection and has proven easier to use than a dial-up connection.

Ideally the solution would be designed for an industrial environment. Unfortunately, most of the security appliances on the market are designed for the office environment, but Morehouse Engineering found Phoenix Contact FL mGuard met the needs of an industrial installation.

The mGuard product line is a family of security devices that provides all-in-one firewall, routing and VPN capability for industrial networks. The mGuard devices combine the needs of the IT world with rugged hardware for harsh environments. The specific model used, the mGuard RS2000, is DIN rail-mountable and has 24 V DC power, making it better suited for industrial installation than the previous solution.

It is the VPN, or Virtual Private Network, capability that provided the solution needed. This feature allows a network to be connected to the Internet, but acts as a very secure gateway, preventing unauthorized access to the system. The VPN, along with free software that provides the encryption and security keys, ensures that only those who have been given the access information can connect to the SCADA network. Furthermore, once the VPN connection is established, it is like you are connected directly to the local network. The PLC programming software easily recognizes the equipment and can connect without a problem.

Originally Morehouse Engineering had hoped that the mGuard’s input signal would make it easy to enable and disable the VPN connection. However, this feature only works when the unit is configured as a client and not as a server. The applications required Morehouse engineers to use the devices as servers, so this feature was not usable in this case. This was a bit disappointing, but the mGuard’s Stealth mode was very helpful to the Morehouse team.

When the mGuard is operated in Stealth mode (the factory-default setting), you don’t need to reconfigure the clients connected to the internal interface of the mGuard (the local SCADA network). You simply need to connect the mGuard between the clients that need to be protected and the Internet-connected network. When operating in Stealth mode, the mGuard is completely transparent. The IP addresses of the clients do not change. This hides all processes listening on the TCP and UDP ports from the outside network, which prevents a port scanner from detecting them. All unwanted or unauthenticated traffic from the outside is dropped.

The mGuard’s Stealth mode allowed the main Internet-connected network to interact with the SCADA sub-network. With the mGuard in Stealth mode, Morehouse Engineering simply configured the internal and external ports to allow easy but protected access from remote PCs, even though they were on different networks. The firewall, antivirus, and VPN settings can all be made using a web browser, so that no changes need to be made on the computer itself. The units can also be configured to all Internet-based connections between different SCADA networks, for when a PC is not needed.

Matt Maloney said, “With the first installation, I spent more time on the setup than I had expected, but some of that was due to my lack of experience with some advanced details of networking. The second installation was peculiar due to the strange way the customer’s networks were configured. It took some extra effort from me and Gus Vargas’, the Phoenix Contact Automation Sales Engineer who assisted, but the mGuard was able to handle the odd circumstances, which indicates its usefulness. Gus guided me through some of the details of networking I was not familiar with and was always available to call for help.”

**Results: Easy and reliable connection**

Shortly after installing the mGuard, the plant contacted Maloney with a problem and asked him to look into it. He says, “I was able to quickly and securely connect to the plant network and go online with the processors. Since then, the ease and reliability of the connection are a great relief compared to the dial-up connection.”