Case Study

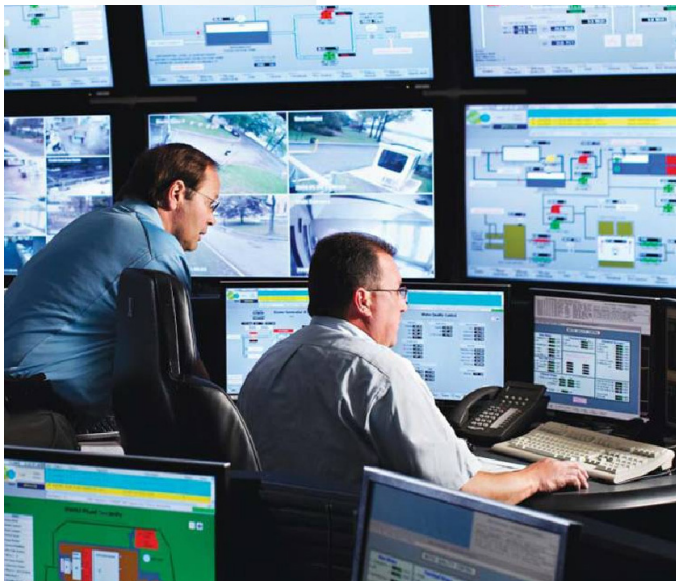
Water | Wastewater

SCADA security for municipal water

A major utility secures its automation networks

Summary

- A water utility needed to improve the security of their SCADA control networks.
- They needed an easy-to-configure solution that could meet IT security standards but also exceed harsh industrial conditions.
- The utility selected the mGuard® network security devices, an all-in-one VPN, firewall and router available in several industrial packages.
- The mGuard is easy for field technician to install and provides multiple measures to monitor and protect the SCADA system from unauthorized activities, while allowing for secure communication between locations.



SCADA systems need a cyber security solution that is IT-friendly while meeting rugged industrial conditions.

Customer Profile

United Water manages water facilities in 23 states. They support more than 300 remote field sites company-wide with an extensive network of underground piping. For more than 30 years, they have used a variety of methods to connect to their remote sites, including modems, leased lines, dry pairs and licensed radio.

Challenge

In 2009, United Water was proactively planning to increase the security of its SCADA control networks. The systems engineering group, corporate IT department and an outside consulting firm were involved in the project and the security product evaluations. A leading IT network solution was initially considered, as this path reflected the corporate office network standard. But there were other important considerations.

"We needed an industrial solution, particularly for our remote sites," reported Keith Kolkebeck, systems engineering project manager for the company. "We needed a solution that was easy to configure, powered by 24 V DC, met our IT security standards, and could hold up to years of operation in a harsh

environment. In the past, we had mixed results using office network-grade products that were expensive, required special skills to configure, and failed frequently."

Solution

In early 2010, the utility was introduced to the mGuard® industrial network security devices from Phoenix Contact, created and developed by their subsidiary Innominate Security Technologies. The mGuard line was designed for harsh environments. Its features includes router, firewall and encrypted VPN tunnels. This allows for filtering of incoming and outgoing connectivity, authentication and other functions to provide layers of distributed "defense-in-depth," economically and without disturbing production.

Availability is in various industrial-rated designs; for DIN-rail mounting, for 19-inch rack mounting in cabinets, as PCI cards or as dongle-style patch cords for roaming technicians. The hardened, industrial version of mGuard has been in production since 2005 and has proven effective in tens of thousands of demanding installations. Rated IP20 for mounting in NEMA enclosures, they are easily installed and enabled by technicians, rather than IT network administrators.

After review of the technology, the utility's IT Department was receptive to the concept as it would allow process personnel to deploy and maintain their own networks, freeing up IT administrators for other tasks. The company installed a dozen devices as a test bed.

Engineer Kolkebeck continued: "The ability for the mGuard to do AES-256 encryption along with its industrial design was key. Again, the mGuard was easy to deploy, cost effective, and met our standards. By default, the mGuard is configured in its most secure configuration. Previously, it would require a day's time of an experienced IT technician, whereas now we can rollout a new VPN device in 10 minutes. The mGuard is very easy for someone with minimal network knowledge to rollout."

In "Stealth Mode" these products are completely transparent, automatically assuming the MAC and IP address of the equipment to which they are connected, so that no additional addresses are required for the management of the network devices. This was a feature that appealed to initially skeptical IT personnel. No changes need to be made to the network configuration of the existing systems involved. Yet the devices can operate invisibly and transparently, monitoring and filtering traffic to the protected systems by providing a Stateful Packet Firewall according to rules that can be configured via templates from a centrally located server. And with bi-directional wire speed capability, the devices will not add any perceptible bottlenecks or latency to a 100 Mb/s Ethernet network.

The mGuard security appliances protect industrial automation networks. They are cost-effective, network transparent, simple to install and easily managed.

If required, the security of networked equipment may be further enhanced. Configuration of specific user firewall rules can restrict the type and duration of access to authorized individuals, who must login from specific locations, PCs, and IP addresses before authenticating themselves. Virtual Private Network functions provide for secure authentication of remote stations, and the encryption of data traffic. Optional CIFS Integrity Monitoring functionality can monitor file systems against unexpected modifications, by Stuxnet or other malware for instance, notifying operators by sending alerts to administrators. While this will not prevent an infection, early detection can mitigate the harmful effects.

Results

"We were implementing multiple measures into our SCADA network in order to activity monitor our system. We utilize network segmentation, VLANS, and centralized firewalls and were looking to introduce intrusion detection (IDS) and intrusion prevention (IPS) systems into our network. The mGuard is a tool that allows us to perform these functions," Kolkebeck stated.

The company needed to protect Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), remote card access and video systems. As industrial systems migrate toward an Internet Protocol (IP) network, more timely information and control is available. All new PLCs have IP capability. Power monitoring is another example. All new Variable Frequency Drives (VFDs) for motors, switchgear, pumps, compressors, and generators have power efficiency monitoring capabilities that need to be tied into the SCADA systems. Following field trials, the mGuard appliances were utilized to provide protection from vulnerabilities through firewall, VPN, routing and trap functions.

"We currently have mGuard security modules deployed in multiple locations throughout the Northeast. We have used the products both for our SCADA networks and our security networks at remote unmanned locations. We have interfaced the mGuard devices with our existing Cisco infrastructure. We are saving money on remote support from our staff and outside contractors. Site visits are no longer required for minor code changes and troubleshooting," Kolkebeck concluded.

At a time when industrial cyber security is more important than ever, there is a simple solution. The mGuard devices combine high-level networking and security functions and the rugged hardware needed on the plant floor, all while playing nicely with existing network infrastructure.