SCADA Security for Critical Infrastructure

FRANK DICKMAN, Consulting Engineer

The economy of every developed country in the world depends on the supply of oil, gas and water, as fuels for transportation, heat, electric current production and survival. The average American consumes 2 gallons of gasoline, 220 cubic feet of natural gas for heating and cooking, 30 kilowatt-hours of electricity — produced primarily from fossil fuels, and 150 gallons of water a day. The supply is an essential part of the critical infrastructure. Providing and protecting the security of that supply is a clear-cut mandate.

Utilities quickly recognized these systems needed even more security after 9/11, and the increased reports of malicious viruses, hacking and the cyberwar capabilities as discussed in numerous whitepapers, including “Hacking the Industrial Network” and “Post-Stuxnet Industrial Security.”

As a result, utilities realized that many industrial control networks would benefit from diverse firewalls behind the front-office firewalls and encrypted Virtual Private Network (VPN) connectivity. Here is how one leading and progressive utility is securing the industrial control networks of their extensive network infrastructure.

The Utility

The utility operates or manages facilities in 23 U.S states with an extensive network of underground piping. It supports over 300 remote field sites company-wide.

For over 30 years, it has used a variety of methods to connect to their remote sites, including modems, leased lines, dry pairs and licensed radio.

Security Today: More Than Padlocks

In 2009, the utility 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 Cisco® 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 VDC, 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.”

Finding a Solution

In early 2010, the utility was introduced to the family of award-winning mGuard® industrial network security devices from Phoenix Contact, created and developed by its subsidiary Innominate Security Technologies. The system was designed for harsh environments and includes small industrial-rated modules that incorporate router, firewall, encrypted VPN tunnels, 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 IP 20 for mounting in NEMA enclosures, they are easily installed and enabled by technicians, rather than IT network administrators. Customers in the automotive and other industries have already used these versions with excellent results in providing security for older production systems. Clients include a major natural gas and electricity provider, and a defense and telecommunications provider.

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 continues: “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 roll out."

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 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 do not add any perceptible bottlenecks or latency to a 100 Mb/s Ethernet network.

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 may log in and authenticate themselves from varying locations, PCs and IP addresses. VPN functions provide for secure authentication of remote stations and the encryption of data traffic. Common internet file system (CIFS) integrity monitoring functionality can protect file systems against unexpected modifications of executable code, by Stuxnet-derived malware for instance, by sending alerts to administrators.

"We were implementing multiple measures into our SCADA network in order to actively 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, switchgears, pumps, compressors and generators have power 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.

Are Your SCADA & DCS Networks Really Secure?

"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 further concluded in a recent interview.

Summary

The story you have been reading documents how one major utility is protecting access to vulnerable SCADA control systems, distributed over a wide area network with unmanned locations. The network in the story actually belongs to a utility company managing and operating water facilities in 23 U.S. States. The application, however, is pertinent to any extended or wide ranging distribution network, such as those operated as natural gas, crude oil, power, petrochem, steam, water distribution and other critical infrastructure delivery systems.

It could be wagered that every engineer reading this is easily able to recognize situations and issues that match those of his own facilities. Each of these utility applications include a harsh environment, remote facilities, access control, video security, rotating equipment — whether pumps, compressors or turbines — and control equipment applications delimited by simple PLCs. All of these systems can include built-in IP capability, and are vulnerable to virus propagation and deliberate hacking by individuals, foreign governments and non-government failed states.

A simple solution is already available. There are proven "defense-in-depth" security products available to provide protection for utilities and critical industrial networks. The mGuard industrial network security appliances have been widely utilized to protect industrial automation equipment, and processes running the newest and oldest operating systems.

Among other formats and applications, the mGuard is available as a small DIN-mount module for NEMA enclosures, easily enabled by technicians rather than IT network administrators. It incorporates router, firewall, encrypted VPN tunnels, filtering of incoming and outgoing connectivity, and CIFS functions, to provide distributed defense-in-depth, economically and without disturbing production.

Frank Dickman is an engineering consultant based in Chicago, available at frankdickman@yahoo.com *[1]. Keith Kolkebeck at* www.unitedwater.com *[2] also contributed to this story, as did the licensed professional engineers with global oil and gas experience at Piping Design Consultants,* www.pdc1.com *[3]. For more information, please visit* www.innominate.com *[4],* www.phoenixcontact.com/usa_home *[5] or* www.phoenixcontact.com/securitywebinar *[6].*

Links:
[1] mailto:frankdickman@yahoo.com
[2] http://www.unitedwater.com/

[3] http://www.pdc1.com
[4] http://www.innominate.com/
[5] http://www.phoenixcontact.com/usa_home
[6] http://www.phoenixcontact.com/securitywebinar