

## SCADA Security for Municipal Water

### How One Major Utility Secures Their Automation Networks



Photo Courtesy of United Water

by Frank Dickman  
Consulting Engineer

#### Without Water

The fact that water is the elixir of all life forms was known and understood long before Ponce de León searched for his legendary fountain. Human beings can live for months without food, but only for a matter of days without water. Life can exist for centuries, for hundreds of centuries, without electricity and fossil fuels. Not so without fresh water.

Urban water usage worldwide is 31 gallons a day per person, with usage in undeveloped areas averaging 18 gallons a day. In the western world, 100 to 150 gallons per person per day is more typical, although people only consume 10% of the total production supply. Agriculture consumes about 70% and industry about 20%.

Providing and protecting the security of that supply is a reasonable mandate. The water supply is an essential part of the critical infrastructure.

The water industry recognized these systems needed even more security after the 2006 conviction of a hacker who seized control of a water treatment facility's SCADA system in Australia. This security breach resulted in the dumping of millions of gallons of raw sewage onto a resort hotel's grounds for a period of three months.

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

### United Water

United Water operates and manages water and waste water systems that serve about 7 million people across the USA. They are a subsidiary of SUEZ ENVIRONNEMENT, a global environmental services leader which supplies drinking water to 90 million people and provides wastewater treatment services for 58 million people around the world.

For over 30 years, United Water used a variety of methods to connect to their remote sites, including modems, leased lines, dry pairs, and licensed radio. United Water supports over 300 remote field sites company-wide.

In 2009, United Water was proactively planning to increase the security of their 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 considerations.

"We needed an industrial solution, particularly for our remote sites," reported Keith Kolkebeck, systems engineering project manager for United Water. "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, United Water was introduced to the family of award winning mGuard® industrial network security devices from Phoenix Contact, created and developed by their

### How About Bottled Water?

Millions of people drink bottled water on the marketing article of faith that it is safer, healthier and tastes better than tap water. Numerous laboratory analyses and blind taste tests have demonstrated that this is often a false assumption.

Unlike municipal water supplies, which are regulated by the U.S. Environmental Protection Agency, bottled water is largely unregulated. Production for Interstate sale is monitored by the Food & Drug Administration, which has one man assigned part-time. Intrastate production and sale is not regulated at all. Bottler water is not required to meet EPA standards of quality.

A substantial number of bottled waters originate from municipal sources or wells. Many people cannot distinguish bottled water from tap water in blind taste tests.

Bottled water is marketed at a price point nearly 1,900 times the price of municipal water. Tap water costs less than 1/5 of a penny for a gallon. Bottled water averages \$3.70 a gallon. In the U.S., one imported brand is \$16 a gallon. It is more expensive than gasoline.

The United States municipal water infrastructure delivers water of the highest quality to one of the highest standards in the world, at a rock bottom price. Your taxes built and support that infrastructure.

**Source:** "Bottled Water Quality Investigation: 10 Major Brands, 38 Pollutants." by Olga Naidenko, PhD et al, Environmental Working Group, October 2008, [www.ewg.org](http://www.ewg.org).

subsidiary Innominate Security Technologies. The system 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 factory enclosures, they are easily installed and enabled by technicians, rather than network administrators. Customers in the automotive and other industries have already used these versions with excellent results in providing security for older production systems.



**The mGuard security appliances protect industrial automation networks. They are cost-effective, network transparent, simple to install and easily managed. Available fiber connectivity can provide Gigabit bandwidth.**

After review of the technology, the United Water IT Department was receptive to the concept as it would allow process personnel to deploy and maintain their own networks, freeing up IT for other tasks. United Water 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

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.

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 login and authenticate themselves from varying locations, PCs, and IP addresses. Virtual Private Network functions provide for secure authentication of remote stations, and the encryption of data traffic. 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 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.

United Water 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 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.

“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 in a recent interview.

## Summary

A simple solution is available. There are proven “defense-in-depth” security products available to provide protection for 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 factory enclosures, easily enabled by technicians rather than 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.

## Contact

**Innominate Security Technologies AG**  
protecting industrial networks  
Rudower Chaussee 13  
12489 Berlin / Germany

Tel.: +49.30.921028-0  
Fax: +49.30.921028-020  
[contact@innominate.com](mailto:contact@innominate.com)  
[www.innominate.com](http://www.innominate.com)