

Harnessing SCADA without undermining security

Events of the past few years have had an effect on almost every aspect of our daily lives, including the manner in which a water utility runs its daily operations. Although it has always been the purpose of my water district to provide safe, reliable, and affordable water and sewer services for its customers, the terrorist attacks of September 11, 2001, made each of us more aware, not just of the potential for terrorist actions, but of our vulnerability to vandalism and other types of malicious mischief.

By nature, a water utility's service area can span a large distance. Many equipment sites and assets are in remote locations, making them ideal targets for intruders. Although staffing limitations prevent us from keeping an ever-present eye on our respective areas, modern supervisory control and data acquisition (SCADA) technology has given us a tool that significantly extends our ability to oversee our resources. It can allow a single user working from a central location to monitor and control the operations of an entire utility area. Unless the system is carefully designed and the user is cognizant of the potential for intrusion and misuse, however, a SCADA system can create as many security problems as it solves.

I manage telemetry networking systems for a utilities district that provides water distribution, wastewater collection, and treatment services for more than 12,000 customers in California's Sierra mountains foothills. The area was originally developed during California's Gold Rush, and the surface water distribution ditches were actually constructed in the middle 1800s for the gold mines.

When I assumed my position in 1999, it was apparent that our existing telemetry system, an obsolete tone-based radio system, was in need of an upgrade. It operated on a "quiescent, 'pop-up'" basis, meaning that a radio could fail or be stolen and we wouldn't know about it until we performed our daily manual poll of the system components. As a result, we missed many critical alarms. When the manufacturer went out of business, the decision to upgrade became a quest for a



new system. There were many challenges associated with the project.

First, I was determined that the system we chose would allow us to take advantage of the capabilities offered by a modern SCADA system without undermining our security concerns. I had to decide on a design criteria that would minimize our vulnerabilities.

Second, our district not only covers a large geographic area, but must cope with a topography that ranges in elevation from 1,200 ft (360 m) to above 5,000 ft (1,500 m). We have many deep canyons that challenge the capabilities of the most well-designed radio communications systems.

Third, our existing system contained more than 110 remote terminal units (RTUs) at water treatment plants, tanks, wells, wastewater lift stations, sewer treatment plants, and so on. Because we were not in a position to replace the entire system at once, I planned to convert the most critical sites to a new system and then add additional sites as time and budget would allow.

special section: security

I began compiling a list of the features our SCADA system needed to include:

- ease of installation and service;
- the ability to import and display the old alarm system in the new user interface;
- accessible operator interface;
- controllable security features;
- good lightning protection;
- remote control capability;
- ability to communicate reliably in our varying terrain;
- analog reporting;
- alarm notification via web browser, e-mail, telephone or pager; and
- compatibility with standard spreadsheets for easy report generation.

Simplicity was another factor. Even though our staffing limitations were considerable, I believed it would be a distinct advantage to install our own system. I was convinced that the right system for our district would not only have the capabilities we needed but would be simple enough for us to install. Aside from the budgetary advantage, I knew that we would have a better understanding of the system and ultimately use more of its benefits if we were instrumental in its implementation.

TWO-YEAR SEARCH YIELDS OPTIMAL RESULTS

The selection was a long process that included most of the “major players” in the industry. As I searched for the right system, I added quite a few items to my list of concerns. Excessive costs for software development, licensing, upgrades, support, hardware, and integration would undermine our finances. We needed a vendor who could create an interface to our existing system so that we could run old and new RTUs through the same system. Some systems lacked a concept for security. Others were overly complex. Most systems did not have a single point for contact, which, in my experiences both in the electronics industry and water treatment, was a recipe for finger-pointing in the event of a problem.

Fairly early on in the investigative process Aqua Sierra Controls, an integrator located outside Sacramento, brought a Florida-based manufacturer to show its product. Instead of a generic system that could be adapted to our needs, Data Flow Systems specifically designed its HyperTAC II telemetry system for use in the water industry. Some of the vendors who visited had been unable to get their products to work during the demonstration, whereas others lacked an understanding of our specific needs. The HyperTAC II system demo went smoothly, but most important, the vendor showed a clear insight into water utility operations as well as an understanding of our specific needs. Nevertheless, I proceeded with my search, which lasted almost two years, only to return to the HyperTAC II in the end.

The manufacturer had agreed to create a driver that would allow alarms and status points from our older RTUs to be viewed on the new system so that we could replace our old

system at a pace we dictated. Their system also offered the ability to digitally forward messages to and from any remote site through other radio locations in the system. This feature allowed telemetry messages from hard-to-reach sites to be relayed to our main office, despite our diverse topography. Most systems use a single, central repeater on a mountaintop, through which all sites must communicate. However, Data Flow’s distributed “digirepeaters,” which are spread over a large area, eliminate a major flaw in the repeater concept—failure of the single, central repeater can bring down the entire system.

None of the systems I’d seen was able to satisfy all of my security concerns. The very features that make a SCADA system useful are frequently the ones that make it vulnerable to hacking—or worse. But the manufacturers of the HyperTAC II controlled the entire system design, including server, software, radios, RTUs, and communications protocol. The systems that used more diverse sources for equipment were more difficult to protect from a security perspective.

Realizing that I had only seen a brief demonstration of the system’s capabilities, I knew there were other issues to consider that were at least as important as the system design. Namely, how do the manufacturer’s customers view them? Many utilities don’t consider the fact that they will be “married” to the manufacturer for the life of their SCADA system. I contacted about 50 HyperTAC II users by telephone and asked each of them the same set of questions:

- Were they satisfied with the product and the after-purchase service?
- Were there unresolved problems or concerns?
- Would they purchase the system again?
- Would they continue to purchase from this vendor?

I assured myself that the manufacturer was responsive to the inevitable technical issues that arise, was solution-oriented, and had a history of being cooperative after the sale.

Finally satisfied with the results of this inquiry, I asked the vendor to install a pilot system at one of our remote locations. This was a full, operational system that allowed the district to use the operator interface, configure stations, test the radio-based communications link, create screens, and check security and general usability. Interestingly, the system’s lightning vulnerability was tested on the day it was installed. Lightning-related losses were so common in our old system that we made lightning protection an important requirement of our new one. When a Sierra thunderstorm swept through the area and a lightning strike hit our building, we lost some modems, a fax machine, and one of our old telemetry boxes, but the SCADA system was not affected.

BOTH SYSTEM AND USERS PRESENT POTENTIAL SECURITY PROBLEMS

Once the physical installation of the central equipment and the first group of RTUs were complete, I turned my focus on the task of tightening our security measures. Worst-case scenarios included terrorist attacks using biological agents or causing long-term loss of power, hackers gaining

access to the system and interrupting water services or spilling raw sewage into a waterway, or even a disgruntled employee gaining access to the control system. Some of these issues were best dealt with using traditional security measures to limit and control physical access to our facilities. My concerns relative to our new SCADA system could be broken into two major areas: network concerns and the SCADA system itself.

It's important to start with the basics. I prefer to keep a low profile, which is the reason that this article has been authored anonymously and my utility is not named. Simply stated, the less that's known about our utility, our network, and our SCADA system, the less likely I'll have to fend off an intruder or system attacker.

Like all networks, ours is vulnerable to intrusions, viruses, loss of data, and so on. Unfortunately, many network administrators don't install strict security measures until they've experienced a security-related loss. Hackers, from the "recreational" sort who are simply looking for a challenge and don't intend to do any serious harm, to the vandals who intentionally cause damage and mayhem, have one thing in common: they are constantly arming themselves with new and better ways to find their way into your network. Therefore, it's vital for the network administrator to constantly update security measures. A variety of products have helped us in our security efforts.

Firewalls, which make use of a set of configurable rules, allow you to determine what types of protocols are permitted to enter and leave the network. A firewall examines each packet of data that attempts to enter the network and decides whether to admit it. The firewall on our network server isolates us from the outside world, while internal software firewalls further protect several critical computers. Firewalls, however, are simply the first line of defense.

Perhaps one of the most useful tools is an intrusion detection system (IDS). An IDS is set up outside our firewall to detect attempts to enter our networking system. The IDS allows you to see the number of break-in attempts as well as each IP address from which an attempt originated. A second IDS can be set up inside the firewall to determine what has made it through to the network. I recently detected about 5,000 attempts to break into our network, all of which originated from the same IP address. Hackers use standard port-scanning tools—software programs that can be set to search thousands of IP addresses—looking for open ports or unlocked entrances to a network. Once the program finds an opening, the hacker is able to concentrate his efforts to exploit that weakness. We also use these "port sniffers" to search our own system. Because certain open ports are necessary for functions like Internet access, e-mail, and access to the SCADA system, it's important to keep a close eye on these unlocked entrances and keep the unnecessary ports closed.

Remote access service (RAS), which allows legitimate users to access their systems from off-site locations, is a very useful tool. I administer my system from home during off-hours and

use RAS to dial in and check to be sure that SCADA alarms are being acknowledged and that proper responses are forthcoming. However, an RAS is yet another vulnerability. Ours is set to operate only on call back, which is the most secure method. When an attempt is made to dial in to the system, the RAS hangs up and initiates a callback. But the RAS is only permitted to call back the numbers we've configured. So even if a password has been compromised, it is useless to someone calling in from an unrecognized location.

Another security challenge involves insiders. In order to be useful, a network and a SCADA system must be accessible by certain employees of the utility. As a result, a significant percentage of vandalism is generated from within the network. We've had to deal with many "typical" issues. An employee working late at night may browse onto an inappropriate Internet site. Some of these sites can deposit programs, called "spyware" on a computer. Once in place, the spyware can control some of the computer's functions and even open ports to allow illicit entry into the network. I use two programs to search for, remove, and immunize our network from such programs and another to keep an eye on how our computers are being used. Employees who unwittingly open e-mail attachments are the most common pathway for viruses to get into a system. Once again, commercially available virus protection programs—when installed, regularly updated, and activated—can offer a degree of protection from viruses.

Some of the "insider" problems can be controlled through user education, strict password control, and the use of some of the software programs I've described. But perhaps the most dangerous interloper is an angry or disgruntled employee. It's harder to protect against this possibility because employees must share files during the normal course of their work day. Our servers' file systems require user logins. I carefully review the server logs in search of unusual activity. I don't allow portable data assistants (PDAs) or wireless devices on the network unless there is an important and specific reason for using them.

SUMMARY

SCADA has become a powerful tool for utilities, providing the ability to monitor and control vast service areas from a single location. However, as computers become more tightly integrated with telemetry systems and remote field equipment, the related security problems become more severe. Suddenly, we're not just worried about mischief or lost files. There is real potential for serious property damage and even harm to the public as a result of an intentionally disrupted water treatment process or a disabled sewer pump. A utility that harnesses the power of SCADA while vigilantly guarding against its potential misuse offers its customers the safest, most cost-effective service.

Steve Whitlock, vice-president of customer relations at Data Flow Systems Inc. in Melbourne, Fla., contributed to this article. If you would like to communicate with the author of this article, please contact the editor at mlacey@awwa.org.