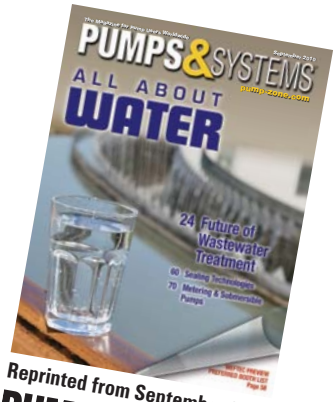
Cellular Communications for SCADA Applications



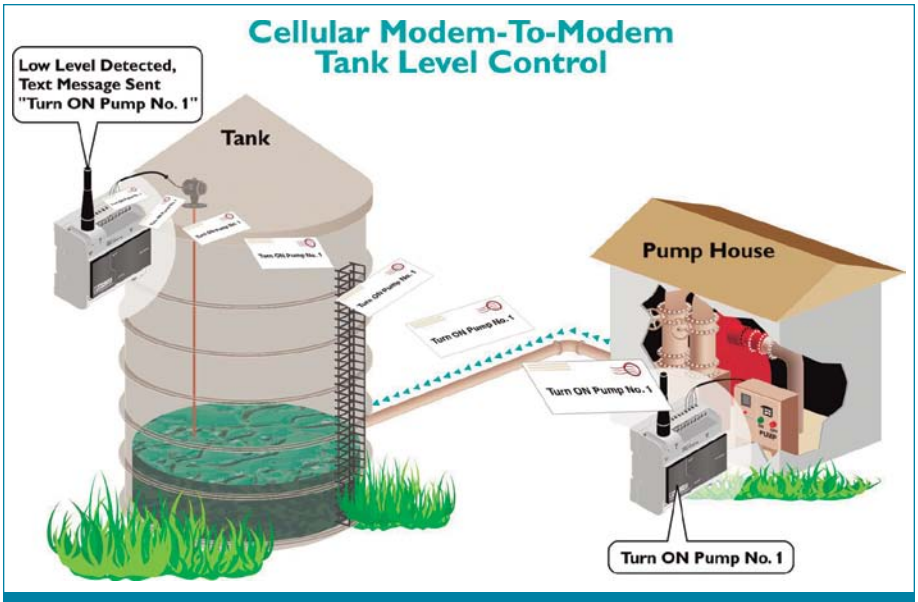
Reprinted from September 2010
PUMPS&SYSTEMS

Ira Sharp, Phoenix Contact

Effective and secure cellular communications for remote data acquisition.

Managers of water/wastewater facilities need to collect accurate information from remote assets such as pumps, tanks and booster stations. Traditionally, this information is collected manually by collecting the chart recordings. This might be done monthly, weekly or daily, depending on available staffing.

While manual collection of this data is the norm, plants want to move to an automated process using a central station for all monitoring and control, which can reduce or eliminate the need for manual data collection. This type of system is called a SCADA (Supervisory Control and Data Acquisition) system. These advanced networking SCADA systems can provide all the information from remote assets at a single location, improving the accuracy and timeliness of the operation.



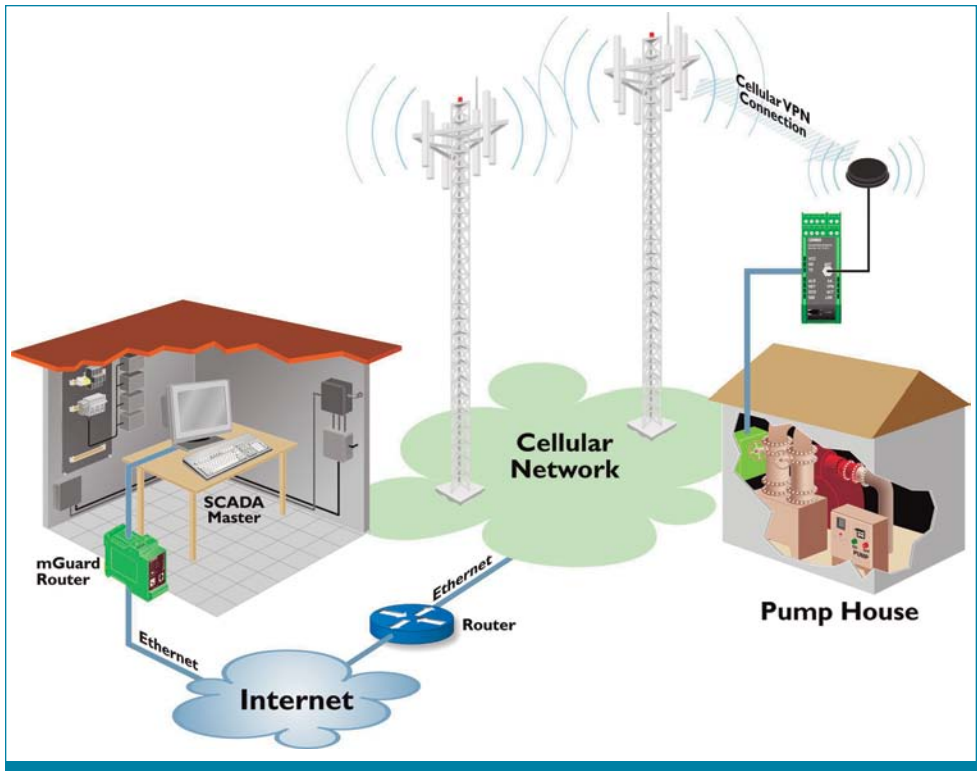
Cellular modem-to-modem text message communications can be used for autonomous tank-level control

A SCADA system requires a network with a secure communication path. Many different technologies—including dial-up, DSL, leased line and private radio—can provide this communications link. In water applications, networks must often reach areas where phone lines or traditional wiring does not exist. Conduits can be trenched and wire can be laid, but this is often cost-prohibitive. Radio can provide access to these remote locations without the need for wires. When it comes to radio, there are a variety of options available. This article examines the use of cellular technology in SCADA applications, how it can be implemented, the different networking options available and security.

Cellular Network Options

In the world of cellular communications, two network options, voice and data, are available. Each has different capabilities for SCADA applications. In this article, we will focus on the Global System for Mobile Communication (GSM) network for voice communications and General Packet Radio Service/ Enhanced Data Rates for GSM Evolution (GPRS/ EDGE) for data communications, but the same principles exist for other cellular technology segments.

The general difference between these types of networks is that the GSM network addresses all devices on the network by a phone number. On the GPRS/ EDGE network, all devices are addressable via an IP address, making data communications easy.



VPN tunnel to the remote modem

Simple Control with the GSM Network for SCADA applications

The GSM network connects with the Public Standard Telephone Network (PSTN), allowing communications from cellular devices to land-based modems using a phone number. This is used for voice communication and Short Message Service (SMS), also known as text messaging.

However, in the U.S., dial-up networking, where one modem calls another using the PSTN, is not permitted over the cellular infrastructure. This limits the use of the GSM network for SCADA applications in the U.S. to SMS-only. Despite this limitation, the GSM network can be useful for simple control applications in a SCADA system.

For these simple control applications, modems can use a text message to take an event—such as a door alarm, high- or low-level tank alarm, or change in pump status—and report it to a control room or another modem for autonomous system operation. In modem-to-modem communications, when the second modem receives a command, it provides some action or status update. The modems create an autonomous system that can control some part of an event-based process.

For example, Modem A receives a low-level alarm message from the tank. This modem then sends a text message to Modem B, which turns on the pump and fills the tank. Once the water reaches an adequate level, Modem A sends another message to Modem B, requesting that the pump be turned off. While this process occurs, the modems also send the text message to a second number for the control room. This provides real-time updates to the control room SCADA system about the actions occurring on site.

If an autonomous system is not necessary, the facility can still use text messaging. The modem can send information about the processes to the control room SCADA master, which will provide the needed logic for control. It can also send a text message directly to the technicians who are responsible for the system. The technicians can then make the necessary changes to the system. Text messaging can be an effective way to monitor and control simple processes.

Advanced Networking with GPRS/EDGE for SCADA Applications

For applications that demand more than simple, event-based monitoring and control, the GPRS and EDGE networks offer additional capabilities. The GPRS and EDGE networks can connect to a private network or to the Internet using standard networking protocols. Since this allows for more information exchange from the remote assets, greater flexibility is available for monitoring, controlling, or even programming over the cellular infrastructure than the GSM network allows. When

using the GPRS or EDGE network for data communications, you must decide if you will leverage a private network or use the standard public network.

Private networks offer a great deal of flexibility. Just about any network architecture can be realized, including host-initiated communication, and all communications do not need to flow over the Internet. However, to create a private cellular network, you must work with a carrier—such as AT&T, T-Mobile, Verizon, etc.—to define how your network should be constructed. These private networks typically charge a one-time setup fee to create the network. This fee can range from hundreds to more than $2,500, depending on the type of network being constructed.

With this type network, you will also need to do some network management to ensure proper network use. Private networking can be ideal for larger cellular networks, but smaller systems usually find the public network more suitable.

The public network does not require any special configurations. Service plans are easily accessible, and generally, no setup fees are required. However, all data communications will flow over the Internet, which heightens the chance of network security threats.

In addition, typical poll-response networks used in SCADA systems will not work over the public network without proper preparation. The public network is designed for mobile-originated communications. In other words, the remote device talks, and the host receives the information. In most SCADA systems, however, the host initiates the communication to the remote device. A VPN (virtual private network) can overcome both the security concerns and the remotely initiated communication issues.

Security with VPN Tunneling

A VPN tunnel is one simple way to ensure the security of the Ethernet traffic over the Internet. To use a VPN tunnel, the modem must support VPN networks. A router that supports VPN networking must also be at the control room.

Leveraging the VPN tunnel to secure the communicated information also solves other cellular issues. As mentioned earlier, cellular networks typically require that the remote modem initiate all data communications. Many industrial protocols, such as MODBUS and EtherNet/IP, however, are designed for poll response. The SCADA master at the control room must initiate the communications, not the remote modem.

By creating a VPN tunnel between the remote modem and the SCADA system, the modem will be available on demand. This allows the SCADA master to do the polling. The modem will initiate communications at startup and will keep the tunnel up, making access of the connected devices easy.

Using this type of network in a water application means that a SCADA master located in a control room can poll a remote PLC, which monitors various aspects of a process, for information on demand, such as pump status. This provides a real-time look at the water process without the need for manual interaction. In addition, changing variables or programming is possible in the remotely located PLC over the cellular network, eliminating the need to visit each location for a system update.

Whether the application involves simple data collection, non-critical control, or remote programming capabilities, the cellular network provides the network access necessary. I/O modems with text message capabilities provide alarm notifications based on a condition or control another device. Data modems provide data communications to remote assets. When used with a VPN, modem technology allows users to collect information, program controllers and access other critical information, all through a single secure wireless link.

P&S

Ira Sharp is Lead Product Marketing Specialist for Phoenix Contact's wireless products. Ira has a Bachelor of Science in Electrical Engineering from Pennsylvania State University. He has worked for Phoenix Contact with a concentration on wireless technology, industrial automation and process control for five years. His active professional memberships include: the Instrumentation, Systems, and Automation Society (ISA); Wireless Systems for Automation (ISA100); and Institute of Electrical and Electronic Engineers (IEEE). He can be reached at 1-800-888-7388, x3777, or isharp@phoenixcon.com.

Industrial Modem Solutions

Worldwide remote access to machines and systems

Phoenix Contact offers industrial modem and router solutions for machine-to-machine communications and remote equipment access.

- **High security connections.**
- **Fast and easy installation.**
- **Global remote access.**

For more information, call **1-800-322-3225** or visit **phoenixcontact.com/industrialmodems**

L002899a:10.10

PHOENIX CONTACT
INSPIRING INNOVATIONS