New Options for Cathodic Protection Remote Monitoring

Craig Held, *FreeWave Technologies, Inc., Boulder, Colorado*

For several years, automated remote monitoring has increased in popularity with pipeline, energy, and utility operators. It is critical for operators to understand which technologies are available and for decision makers to thoroughly examine their options and be aware of advancements in cathodic protection remote monitoring. Security, pipe-to-soil requirements, and awareness of potential alternating current interference are key areas to evaluate when selecting a monitoring system.

New technologies introduced over the past several years have streamlined the processes for cathodic protection (CP) monitoring. Previously, a time-consuming manual method was the only option. Now, pipeline operators have a handful of options. Automated remote monitoring in particular has increased in popularity as a viable tool for pipeline, energy, and utility operators. Many of these technologies can send data directly to a computer or smart phone from a remote location. At the touch of a button, operators are able to understand the status of their entire system. In a market saturated with options, where some are much more reliable and efficient than others, it is critical for operators to be well informed and understand which technologies are available and best suited for their communications network and their impact on the company's CP efforts.

Options

The large range of communication technologies available for remote monitoring applications can be daunting when it is time to make a decision. Before selecting any sort of communications network, operators must be familiar with the options and their capabilities. Spread spectrum, licensed wireless data radios that collect mission-critical data, in particular, have become a strong option for automated monitoring. Some of their most compelling features include the benefit of real-time data and the ability to be used in the most remote locations without monthly and recurring fees (Figure 1). These wireless data radios have established themselves as one of the most flexible, reliable, and low-power consumption options available. They offer more security within their proprietary networks than established communications solutions that rely on public infrastructure, and they share the same benefits of real-

time data and operational feedback as other systems without the added costs of monthly connection fees.

Recently, these same technologies have been introduced for pipe-to-soil (P/S) applications in a submersible, waterproof, battery-powered option. Designed for operators in need of a less conspicuous deployment, this P/S monitoring option helps reduce the cost of theft, vandalism, and use in target practice. In regions of the world where theft is prevalent, companies can find themselves spending thousands of dollars in replacement costs and maintenance man-hours.

In difficult environments, users can implement these new submersible radios for their monitoring needs. The radios are placed underground, with only the antenna visible. They require battery replacements about once every two years and are ideal for a polling requirement of once a week or less, making them a good fit for areas with limited access. With a new submersible option, valuable electronics can be kept safe, secure, and operational because of waterproof protection.

While these additions to CP remote monitoring are the newest to the marketplace, operators also have several different existing options to choose from. These include:

- Manual systems, which are the most traditional, require a field technician to physically access the monitoring point to collect data. This is a time-consuming process, especially when assets are located in remote or limited access locations. In addition, this makes the resources devoted to mitigation become scarce as time and efforts are spent on measurement.
- Satellite systems have broadband capabilities, but have monthly recurring costs (based upon the amount of bandwidth used each month). They are generally quite reliable once they are set up, and also are quite capable of being deployed in remote locations.
- Cell phone systems function in a similar fashion as satellite systems in that they use an existing public network of communication devices and also have monthly charges—either for a connection or connection and data usage. If users are within range of a cell tower, cell phone systems are very much "plug and play" in their simplicity. Monthly recurring costs associated with satellite or cell phone systems can become a burden on the operating budget of a department that is held accountable for yearly productivity improvements. Money spent on both satellite and cellular system connection costs, if deployed against capital costs, may be able to pay for a wholly owned proprietary network in less than three years.
- "Drive-by" systems can be appealing because they keep the process of the field visit intact without the need to leave a vehicle. One can simply drive up and take measurements, which is very efficient. A benefit to a drive-by system is the reduction or elimination of any connection fee; however, the drawback is the amount of time and man-hours required to access the data.

FIGURE 1

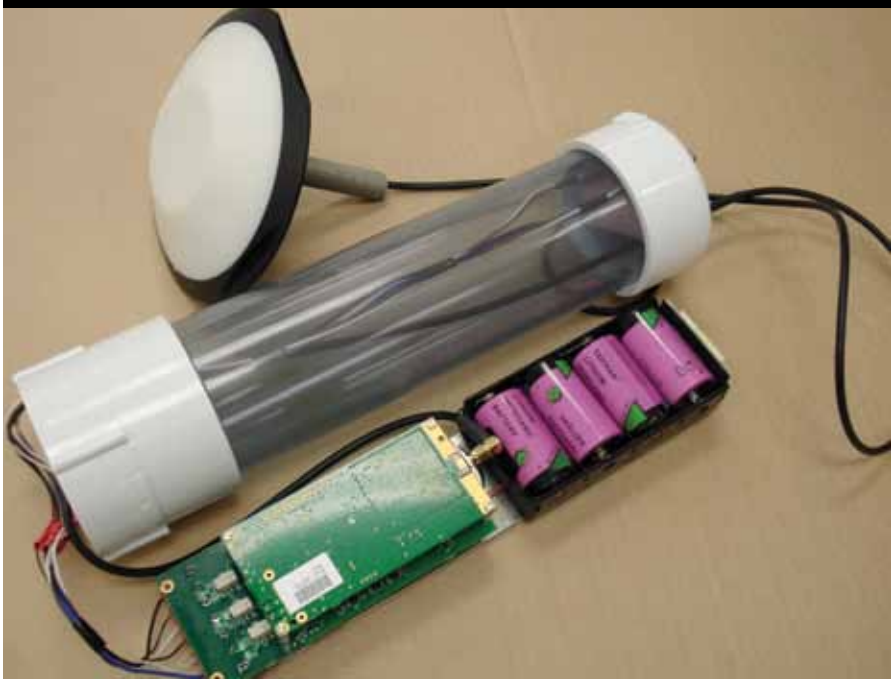
Spread spectrum data radio for CP remote monitoring.

Security

With all these different communications systems, it is critical to understand security threats and system features before purchasing a CP monitoring system. The two most common threats to data communication networks are Denial of Service (DoS) and Intrusion. DoS is an attempt to make a computer resource or network unavailable to its users. This type of service interruption ranges from something as simple as jamming an electric or electromagnetic signal to preventing access to critical data. The consequences of intrusion range from spying or stealing information to corrupting data or taking over an entire network's computers and control systems.

Spread spectrum wireless data radios can offer secure proprietary networks for CP remote monitoring. They are avail-

FIGURE 2



A new waterproof, battery-powered option for CP remote monitoring.

able in transmission control protocol/Internet protocol (TCP/IP) networks with encryption and frequency hopping spread spectrum (FHSS). Unlike traditional wire-lined data communication, which typically uses copper or fiber-optic cable between communication end points, wireless data communication is based on electromagnetic waves using radio frequencies (RF), which gives wireless some unique advantages. FHSS wireless systems are very resilient when it comes to impairments such as interference and "jamming." The key to this resistance is that wireless signals travel through space and small amounts of the radio spectrum are used at a time. The signals do not remain at any particular frequency very long, instead quickly "hopping" to another frequency. This makes a DoS attack on FHSS systems very difficult, if not completely impossible. While these features place spread spectrum wireless data radios ahead of some other systems, it does not ensure full security coverage. There are wireless data radio providers that also account for access control and privacy to ensure optimal security.

Access Control

For critical system monitoring, it is essential to use a technology that is not easily accessed. Proprietary systems and devices offer a high degree of security. But even those devices can be penetrated if you know how and where to get access. A well-known Internet auction site often serves as the source, so that a patient hacker can figure out settings to gain access even if it may take a while. Access control is one of the most important security features and there are wireless data radios available that utilize it.

Privacy

A good network security strategy should go even further and protect data "in transit" as well. Even if an unauthorized device manages to gain access to the network, it won't necessarily gain access to the actual data without passing yet another layer of security. For thousands of years, cryptography provided this extra security layer and maintained the privacy of the data between the sender and recipient, even if others had access during transit or transmission. Methods of encryption and deciphering have come a long way since then. Today, the Advanced Encryption Standard (AES) is *the* industry standard for encryption. As a federal government standard used by the National Security Agency (NSA), it can be trusted to protect sensitive information and maintain data privacy. Some wireless data radio providers offer solutions that meet the AES.

As automation and wireless technologies begin to play a leading role for CP and many other supervisory control and data acquisition (SCADA) applications in various industries, security also becomes an increasing concern. The key to protecting data and transmission of data is to use the technologies that are able to handle potential security threats.

Meeting Pipe-to-Soil Requirements

The new waterproof, battery-powered option (Figure 2) offers coverage for up to three P/S measurements. Some operators with more P/S requirements may need to add additional measurements to an existing or new network and want the most cost-effective solution available. Recent modular approaches can offer virtually unlimited rectifier and P/S counts at affordable costs.

Alternating Current Interference Detection

Monitoring of alternating current (AC) interference is becoming more and more important. When left unmonitored, AC interference can impact the effectiveness of CP, and also pose a risk of personal injury to operating personnel. When considering technologies, an operator should evaluate whether the system has the ability to monitor AC interference. Some manufacturers of spread spectrum wireless data radio technology can accommodate this in their remote monitoring units, and suppliers are beginning to see an increase in demand for this type of technology. AC interference detection can potentially help avoid personal harm and CP impact.

Conclusions

With so many communication options to consider when implementing a remote monitoring system, it is critical for utility operators to ensure they have selected the best communication network for their organization. A reputable manufacturer will allow decision makers to do a pilot test and path study to gain confidence in the installation and also understand how it works. This ensures that the end-user has chosen the best possible system to meet its needs. Additional factors that must be taken into consideration include security offerings, multiple P/S and rectifier monitoring capabilities, and AC interference detection. Today, there are wireless data radios available that address and streamline the process for all three.

Bibliography

Held, C. "Applications and Innovations for Battery-Powered CP Remote Monitoring." *MP* 50, 5 (2011): pp. 33-35.

CRAIG HELD is the CP product manager at FreeWave Technologies, Inc., 1880 S. Flatiron Ct., Ste. F, Boulder, CO 80301, e-mail: craigheld@freewave.com. He also serves as the general manager of international markets for the company. *MP*