

Operators Extend SCADA Investment to Vital Cathodic Protection

David J. Southern P.E., Product Development Manager
FreeWave Technologies, Inc.

Changing Business Climate

Aging infrastructure, new state and federal regulations, new unfriendly neighbors, an aging workforce and heightened security restricting site access are burdening company operations with increasing costs and deteriorating operational excellence. Operating managers within energy, municipal and pipeline companies look to extend their investment in high performance SCADA networks in the hopes of gaining greater operational efficiencies and keeping costs in check.

Likewise, operation professionals look to their investments in SCADA networks and remote automation also to gain new operational efficiencies. Originally planned for integration to remote terminal units, and programmable logic controllers, SCADA systems now are used for AMR/AMI applications, and operators are looking for even greater leverage of their existing systems.

A New Direction

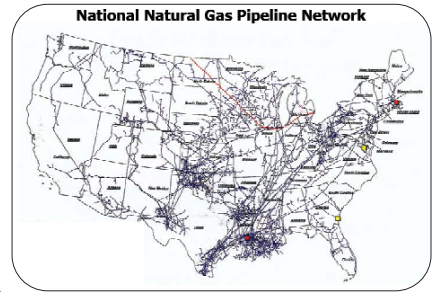
A large municipal water company in Denver, Colo. is experimenting with a new, low-cost remote monitoring solution specifically designed to monitor integrity management and corrosion prevention systems. Leveraging its existing SCADA infrastructure, it hopes to extend remote monitoring to critical cathodic protection systems as well.

Cathodic Protection (CP) systems for storage tanks, pipes and other buried infrastructure are often located in remote locations making them difficult to maintain and operate, let alone operate at peak performance. In some cases, unauthorized third parties strip the critical rectifiers and wiring and sell them for scrap, leaving tanks and miles of expensive metal unprotected. Theft results in an increased risk of damage or even total failure of a system from corrosion. Compounding operational difficulties of remote systems are site access issues stemming from land use disputes, Homeland Security and urban sprawl.

The cost of implementing properly installed and well-maintained CP remote monitoring equipment pales in comparison to the annual costs required to repair even a single leak. Reports estimate corrosion is responsible for costing US industries more \$270 billion per year, almost 3.1 percent of the GDP. The desire to reign in those costs has never been greater. Corrosion leading to leaks, lost revenue, groundwater contamination and other adverse scenarios affecting overall water quality, supply and/or public safety now can be prevented like never before through technological advances in the remote monitoring of critical tanks, pipes and casings.

Since the 1800s, when the first metal pipe was buried in North America, roughly 2.3 million miles of pipe and corresponding valves, tanks, vaults and structures were buried to carry vital water supplies across the country. Much of this buried infrastructure now celebrates its 50th year and some of this infrastructure is beginning to show its age by a few notable, recent and tragic events.

As tank and pipeline grew operations throughout North America, so grew federal and state regulations governing the industry. Recent legislation passed by the US Congress further develops the legal implications of pipeline integrity management. At the heart of this growing legislative effort is the protection of public safety, the environment, irreplaceable national energy reserves and the US economy.



Recent tragic events at the local, state, national and international levels place increasing focus on the protection and integrity of all US pipeline operations. Evidence of this increased national public awareness is demonstrated by the recent passage of the Pipeline Safety Improvement Act of December 2002, and the Pipeline Inspection, Protection, Enforcement and Safety Act of 2006. Both Acts serve not only to illustrate growing awareness, but also to educate the industry on pipeline operation best practices.

The Pipeline Safety Improvement Act of December 2002 mandates significant changes and new requirements in the way the pipeline industry ensures the safety and integrity of its pipeline facilities, including:

- Each pipeline operator must prepare and implement an Integrity Management Program (IMP)
- Participate in planned-excavation one-call notification programs
- Increase the penalties for violations of safety standards
- Authorize state participation in interstate pipeline oversight
- Offer a multi-agency program of research, development, demonstration and standardization to enhance the integrity of pipelines
- Develop an inter-agency task force to expedite environmental reviews when necessary to expedite pipeline repairs

Pipeline Inspection, Protection, Enforcement and Safety Act of December of 2006 requires certification procedures of annual and semi-annual pipeline integrity reports by a senior executive officer of each pipeline company to certify that the officer has read the report and, to the best of the officer's knowledge, that it is true and accurate.

Site access issues stemming from land use disputes, Homeland Security and urban sprawl, compound operational difficulties for remote systems. Recent tragic international events led many landowners, municipalities and government agencies to restrict access to sensitive areas making them onerous to enter for maintenance purposes. Many airports, office towers and mass transit sites are now "off ls" for routine CP maintenance checks. Restrictive site access procedures leave miles of buried infrastructure unmonitored and sometimes unprotected.

Rising energy prices, steel prices and labor costs add to operating budget shortfalls. The cost of repairing or replacing buried metal assets steadily rose over 300 percent through the last 10 years and is projected to continue. One analyst speculates that pipeline integrity issues alone could drive energy prices higher by 27 percent.

New Development in FHSS

New spread spectrum wireless data communication technology, first developed in the 1930s, known as Frequency Hopping Spread Spectrum (FHSS), is based on the concept that most radio frequencies are underutilized. FHSS allows multiple users to simultaneously operate across a spectrum of radio frequencies. Provided all radios within the data communication network operate at the same frequency and then all hop to new frequencies at the same time and in the same hopping pattern; then effective, safe, trouble free data communications exist.

An analogy of FHSS technology is illustrated by imagining a group of people wishing to carry on a conversation using Citizen Band (CB) radios. As long as all parties are on the same channel, they can communicate, and if they wish to keep others out of their conversation, they can carry on a private conversation by all agreeing to move from CB channel to CB channel on a random, yet, agreed upon, pattern of CB channel hopping. As long as all parties hop from channel to channel on the same pattern, at the same time, they can carry on an effective conversation. If they take roll call upon arrival at the new channel, they can further improve communication security. In some remote cases where a third party does hit the current CB channel at the right time, they only get part of the message, which means little to the third party.

FHSS Cathodic Protection Remote Monitoring Technology

Key advantages of this new technology as applied to remote monitoring include no monthly recurring fees or costs, no initial or monthly licensing fees, no lengthy legal contracts, minimized network interferences, network security and it operates behind

Wireless Monitoring & Control for Any Application

DNP3, Modbus, OPC • M2M • Low power • Multiple telemetry options





With over 34 years of proven experience in remote data acquisition and control, our rugged, stand-alone datalogging systems offer unmatched versatility.

Find out more:
www.campbellsci.com/m2m

CAMPBELL[®]
SCIENTIFIC, INC.

WHEN MEASUREMENTS MATTER

Feature

company firewall. Additional benefits include ownership of data, open protocol communications, system flexibility, infinite repeatability, maximum implementation into cabinetry and minimized field wiring.

The new FHSS wireless CP remote monitor units (CP RMUs) automatically monitor and report key corrosion protection activities including pipe-to-soil potential, rectifier output voltage, rectifier output amperage, rectifier input power status, critical bonds, interference points and interruption control. Modern CP RMUs monitor ambient temperature and, if connected to a solar power generation system, also will monitor the back up battery supply voltage.

The new FHSS wireless field located CP RMUs remotely monitor rectifier and pipe-to-soil voltages, currents and potentials and record them. Field data then is wirelessly collected from the field devices by a computer located in a central office or through a SCADA system for CP operator evaluation and monitoring.

Cathodic protection systems are highly susceptible to transient lightning surge. In addition to being directly connected to the field piping structures, CP rectifiers are also attached to overhead power lines making them more likely to receive damage from near strike lightning. To protect sensitive wireless electronics, manufacturers use fully isolated relay, sampling capacitor technology for maximum protection.

SCADA

Many companies already own and operate a SCADA network and can easily integrate these new remote monitoring devices through existing RTU's, PLC's or radio networks.

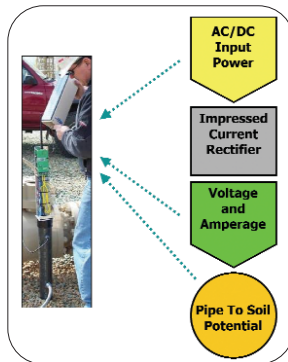
For companies that don't have SCADA, they can deploy, low cost data logging software readily available for less than the cost of a desktop computer. Below, is an example of this new CP data logging software.

Station	Rectifier	Output Voltage	Output Amperage	Input Voltage	Input Amperage	Pipe-to-Soil Potential	Temperature	Humidity	Power Status
CP-001	1000	10.5	1.2	120	1.5	-0.8	75	60	ON
CP-002	1000	10.5	1.2	120	1.5	-0.8	75	60	ON
CP-003	1000	10.5	1.2	120	1.5	-0.8	75	60	ON
CP-004	1000	10.5	1.2	120	1.5	-0.8	75	60	ON
CP-005	1000	10.5	1.2	120	1.5	-0.8	75	60	ON

Central data collection systems automatically inform CP Professionals of immediate system operation requirements leading to optimization in keeping critical CP equipment online and operating within guidelines. As a result, remote sites no longer are difficult to monitor.

Take a Test Drive Before You Buy

A great way to learn more about new CP remote monitoring technology is to test drive it before you buy. Manufacturers offer no obligation, demonstration systems prior to making key purchasing decisions. A test drive is easy to implement by first selecting a half dozen test points and a central office location and by providing the manufacturer or vendor with the site coordinates. For the purpose of the test drive, CP data either can be collected using the data logger software or by coordinating with your CP RMU provider to design a plan to integrate the equipment into the existing SCADA architecture.



Normal test drive intervals depend largely on the size and type of system deployment. However, 30/60/90 day test drives are not uncommon.

David Southern is a professional, licensed engineer with 25 years experience in corrosion prevention and industrial automation. Currently, Southern manages world-wide development of wireless, license-free, cathodic protection remote monitoring systems for FreeWave Technologies. For more information please visit www.freewave.com/CP7 or call 866-676-4046.

Hear David Southern and FreeWave Technologies Speak at the Remote 2008 Conference and Expo. While You're at it, Visit Their Booth!

Session Title: Pipeline Integrity Automation
Learn More At: www.RemoteExpo.com

Remote 2008

CONFERENCE AND EXPO

SCADA, Device Networking, M2M, Wireless Technology, Onsite Power, And Security for Remote Sites and Equipment

Expanded Exhibit Hall and Speaker Sessions Highlight Changes for 2008!

To better serve the remote site and facility market, the Remote 2008 Conference and Expo has made a few changes. First we've book the largest exhibit hall in the show's history, while also expanding the program to better serve your needs.

The largest addition to the program is an entire track, two days of sessions, covering cyber and physical security measures in remote applications. With the influx of new standards, wireless and homeland security concerns, this will be a popular topic in 2008 and beyond! Also new for the program are sessions relating to power protection in remote environments (UPS, lightning, back-up power) and sessions covering Remote Smart Services. To see our preliminary program please visit: www.remotemagazine.com/rem08_program.php. Contact Nick Depperschmidt at nickd@infowebcom.com or 800-803-9488 for more information.

Recently Introduced ISA Workshops!

Practical Applications of SCADA Systems Integration
Tuesday, November 4, 2008 - 8am - 4pm

Securing Industrial Networks: Cyber Protection for Automation, Control, and SCADA Systems
Tuesday, November 4, 2008 - 8am - 4pm

Visit www.remotemagazine.com/rem08_workshop.php for full workshop descriptions and information on how to register via the ISA website

For more information about sponsoring or exhibiting contact Scott Nash at: ScottN@infowebcom.com or 303-317-2505

NOVEMBER 5-6, 2008 - ATLANTA, GA.

WWW.REMOTEMAGAZINE.COM