Wireless Communications in SCADA Systems
Table of Contents

Executive Summary ................................................................................................................................. 3
Introduction .............................................................................................................................................. 3
Wireless Communications in the Power Grid: An Overview ................................................................. 4
Advantages of Wireless Communications for SCADA Systems .......................................................... 5
Wireless Technology Options ............................................................................................................... 6
Requirements for Wireless Solutions Supporting Critical Infrastructure ........................................ 7
Best Practices for Cellular SCADA Solution Design and Implementation ........................................ 8
Laying the Foundation for a Smarter Grid ............................................................................................. 9
Executive Summary

Energy suppliers rely on Supervisory Control and Data Acquisition (SCADA) systems to enable remote telemetry functions in the power grid. Historically, SCADA systems have employed wireline networks to link remote power grid elements with a central operations center. Today, more and more utilities are turning to public cellular networks to provide these vital communications functions. Modern cellular networks are just as secure and reliable as wireline infrastructure, and can be faster, easier, and less expensive to deploy and operate. This paper examines the benefits of wireless communications in SCADA systems, and offers guidance on building a successful wireless-enabled SCADA system.

Introduction

Browse through any news media today, and you’re likely to find a headline about the “Smart Grid.” By building end-to-end, two-way communications across every element of the power transmission and distribution infrastructure, energy suppliers aim to deliver energy more efficiently and better manage consumption. To make this vision a reality, however, suppliers need up-to-the-minute infrastructure intelligence, and the ability to remotely monitor and control equipment across the grid.

Energy suppliers have long employed such communications and telemetry systems in the energy grid in the form of Supervisory Control and Data Acquisition (SCADA) systems. Indeed, the first SCADA systems to provide rudimentary monitoring and control functions of remote power grid equipment appeared in the 1930s. More recently, suppliers around the globe have been modernizing their SCADA systems, transitioning from closed, analog connections to digital, Internet Protocol (IP)-based systems.

As energy suppliers update SCADA systems, many are also reexamining the communications media those systems employ. Yesterday’s SCADA systems relied almost exclusively on analog phone lines. Today, most suppliers use wireless wide-area network (WWAN) communications for at least some segments of the grid. And, the use of public cellular networks in SCADA applications grows each year.

This paper discusses the role of cellular communications in SCADA systems. It provides an overview of the areas of the power distribution system where wireless technologies can be used and discusses the benefits they can provide. Finally, the paper examines the requirements and best practices for wireless communications supporting critical transmission and distribution infrastructure.
Wireless Communications in the Power Grid: An Overview

Given recent media buzz about wireless Smart Grid technologies, it may seem like wireless is a new solution in power grids. In fact, while the use of wireless connectivity at the individual meter is a relatively new phenomenon, energy suppliers have relied on wireless communications to support SCADA systems in other parts of the grid for many years.

Wireless communications can be applied to any situation where an energy supplier needs to communicate with a device or piece of equipment. In practice, most utilities use primarily wireline connections within power plants, simply because they are freely available. At peripheral and remote locations, however, wireless is a common and increasingly popular solution.

Wireless connectivity can be employed for:

- **Electrical substations, including transmission, distribution and connector substations.** In the modern power infrastructure, these substations are responsible for connecting transmission lines and converting voltages at various points in the grid, and are therefore key elements in the SCADA system. In the past, operators chiefly used analog modems, but today, most newer substations (as well as a large number of older sites that have been retrofitted), rely on cellular connectivity.

- **Auto re-closures and sectionalizers.** This equipment protects against faults and allows operators to isolate faults and breaks when they occur. Many operators now integrate wireless connectivity with auto re-closures and sectionalizers so they can control and monitor them from a central distribution operations center. (See sidebar.)

- **Programmable logic controllers (PLCs) and remote terminal units (RTUs).** Industrial-grade PLCs are now used as sophisticated computers to connect a variety of equipment with SCADA systems. RTUs also provide onboard computing intelligence to serve as an interface between legacy equipment and the control system. Both RTUs and PLCs are essential in a modern SCADA system, and both now commonly integrate wireless communications to enable remote management.

---

### Wireless Saves Time, Hundreds of Thousands of Dollars for Pennsylvania Energy Supplier

**Challenge**

Duquesne Light distributes power to nearly 600,000 customers in southwest Pennsylvania.

To improve service, the company wanted to manage 700 sectionalizers and reclosers from its central distribution operations center. To build out this capability using wireline connections, however, would take many months, at a cost of about $10,000 per location.

**Solution**

The company deployed intelligent cellular gateways on all sectionalizer control cabinets.

The solution was deployed for just $640 per location—a savings of more than $9,000 per site. More important, supervisors can now address problems in near-real time, anywhere in the grid.
• **Wind farms.** Cellular communication technologies can be used in a variety of ways in wind farms, from monitoring power output to selecting the optimal location and positioning of windmills. (See sidebar.)

• **Distribution network endpoints.** Wireless communications are also employed at the edge of the distribution network, where power is consumed (and in a modern Smart Grid that supports micro-generation, where it is added back onto the grid). Wireless modules can increasingly be found “under glass” in individual power meters. Many operators have also long used cellular modems as meter aggregation solutions in “neighborhood-area networks” (NANs). In this scenario, the wireless solution collects data from dozens of meters equipped with another near-field communications technology (e.g., WiFi, ZigBee, power-line communications, etc.), and sends that data back to a central operations center over a public cellular network.

Depending on the energy supplier, there may be hundreds, thousands, or (for suppliers using cellular solutions in the meter) tens of thousands of connected wireless devices communicating as part of the SCADA system. In all cases, operators manage these communications using a management application, either internally developed or provided by a third party.

### Advantages of Wireless Communications for SCADA Systems

Cellular WAN solutions offer a number of advantages in supporting SCADA systems and critical infrastructure. Benefits include:

• **Easy installation.** By an order of magnitude, wireless solutions are simpler, faster, and less expensive to deploy in locations that do not already have wirelines installed. Establishing new wireline services at a remote substation site, for example, could take weeks or even months, and cost thousands of dollars. With a wireless solution, connectivity is simply a matter of switching on the device. Since today’s cellular networks cover approximately 99 percent of the population worldwide, connectivity is likely to be available virtually everywhere suppliers need it. Indeed, most areas are now covered by multiple cellular networks, allowing utilities to deploy wireless-enabled equipment using the best cellular network available depending on location and maintain backup network capabilities.
• **Lower operational costs.** Some utilities build and operate their own private radio networks to support SCADA communications. When a utility uses cellular, they can rely on the mobile operator to provide that network – instead of having to bear the cost of deploying, operating, and maintaining that infrastructure themselves. In addition, energy suppliers can often work with a single wireless carrier for all locations, which may not be possible with wireline connections that are typically controlled by regional providers.

• **Proven technology.** Cellular technology has existed for more than 20 years. Modern cellular networks are just as secure and reliable as wireline connections, and more than capable of supporting critical infrastructure and SCADA systems. In fact, 1 billion machines already use cellular networks today, supporting SCADA applications, as well as sensitive financial transactions and critical government communications. Data communication (typically IP-based) now makes up 20 percent of all cellular communications worldwide. And, given the huge investment that major carriers make in constantly monitoring and protecting against network security threats, a cellular network may actually be more secure than a privately operated infrastructure.

• **Competitive rates.** From a market perspective, the cost of cellular services continues to decline as technology advances and carriers begin to compete more fiercely for utility customers. Mobile operators increasingly view machine-to-machine (M2M) services as an important and growing subscriber market. In the United States, for example, all three major carriers have established M2M and utility teams to pursue this business.

### Why Cellular?
- Fast, low-cost installation
- Lower operational costs than building and operating a private network
- Global coverage
- Proven and secure technology
- Competitive pricing for wireless SCADA services

## Wireless Technology Options

Energy suppliers have traditionally had two primary WAN/cellular technology options: second-generation (2G) and third-generation (3G).

While many energy suppliers have used 2G services in the past, many carriers are now touting the advantages of higher-bandwidth 3G networks to support SCADA systems, especially in meter aggregation applications that transmit a large amount of data. Suppliers have a choice of data services over 3G networks: Wideband Code Division Multiple Access (W-CDMA) and High-Speed Downlink Packet Access (HSDPA). Newer HSDPA technologies can now be acquired at comparable cost to W-CDMA and have become the preferred solution.

Looking forward, Long-Term Evolution (LTE), a fourth-generation (4G) cellular technology is also likely to play a role in power grid and SCADA communications, especially at meter aggregation points. As more utilities begin to connect hundreds or thousands of individual meters, the exponentially greater capacity and lower latency of 4G and LTE technologies will offer a compelling connectivity option. Given the pace at which wireless technology can evolve, LTE technologies may also offer the greatest longevity for solutions that will continue to operate for many years.
Requirements for Wireless Solutions Supporting Critical Infrastructure

No matter which cellular technology energy suppliers employ to support SCADA systems, the wireless solution must have several key attributes:

- **Industrial-grade construction.** Any cellular router or gateway deployed as part of a SCADA system must be a ruggedized solution, capable of withstanding a number of extreme environmental conditions including very high and very low temperatures, humidity, corrosion, vibration, and more. Cellular communications devices also must be Class 1, Division 2 (C1D2)-certified for use in hazardous environments.

- **Reliability and longevity.** Power grid and SCADA equipment may stay online for decades. Any cellular solution supporting this equipment must also be designed to function reliably for 10, 15, even 20 years, without requiring that components be directly maintained.

- **Low maintenance and remote manageability.** All cellular technologies supporting SCADA systems must be fully manageable and upgradable remotely. During the 10- to 20-year life span of a SCADA communication device, for example, the device’s firmware will likely be upgraded to add new features, enhance security, or maintain compliance with the latest wireless communication standards. IT managers need to be able to remotely manage, configure, test, validate, update and troubleshoot both the wireless gateway and the underlying asset, over the air, from anywhere in the world. A wireless solution that requires an onsite technician to upgrade firmware or change settings has a far higher total cost of ownership over the life of the device.

- **Flexible and configurable.** Given the need to interact with a broad range of equipment and software systems, wireless devices and management applications used in SCADA systems must incorporate protocols to communicate with legacy equipment and convert legacy data traffic to IP. This capability is essential to modernize SCADA systems and take advantage of ubiquitous, low-cost IP networks, without having to upgrade the entire legacy infrastructure.

- **Strong security.** When providing remote command and control capabilities for critical infrastructure, several security threats must be addressed. The most important: assuring data integrity and maintaining continuity of service throughout the grid. Wireless solutions should have built-in security protocols to further bolster the already-secure public cellular network. At a minimum, wireless solutions must support encryption and secure sockets layer (SSL) transmission.

- **Simple installation.** Energy suppliers should be able to deploy cellular solutions relatively easily, even at remote substation sites, without requiring technicians with extensive expertise in wireless technologies. Along these lines, cellular SCADA solutions should support broad-based over-the-air setup and configuration capabilities to allow IT managers to configure wireless solutions for entire network from a central operations center.
• **Intelligent management.** Essential for any wireless SCADA solution is a robust, intelligent management platform that can assure a reliable connection, facilitate comprehensive remote management and programmability, and provide a broad range of application services. IT managers must have complete control over what data to collect, when and how often to collect it, and where to send it.

**Best Practices for Cellular SCADA Solution Design and Implementation**

As energy suppliers have incorporated more cellular WAN technologies into power transmission and distribution systems over the years, the industry has established a number of “best practice” design guidelines for wireless solutions. By following these guidelines, utilities, power equipment manufacturers and other industry stakeholders can realize the best results from their wireless-enabled SCADA implementations.

The most critical requirement is to choose devices that build ample intelligence into the endpoint. IT managers should have access to hundreds of options, all configurable over-the-air, to control, maintain, manage, secure and troubleshoot devices, from anywhere. The degree of intelligence the endpoint provides often correlates directly with the device’s total cost of ownership, as it is the ability to reconfigure and update devices remotely that reduces truck rolls. Endpoints should provide:

• **Session persistence intelligence.** The wireless solution should be designed to maintain connectivity and maintain uptime at all times. Devices should employ watchdog timers and data retry algorithms to not only maintain session persistence, but assure that in the event a device is knocked off the network, it fights to get back on.

• **Ample flexibility to interoperate with legacy equipment.** Look for wireless devices that offer support for a large library of embedded machine protocols (e.g., Modbus, DNP3, TCIP, Bristol Babcock, etc.). Wireless solutions should also be able to perform Packet Assembly Disassembly (PAD) to allow them to receive data in the form of a legacy protocol, assemble the data into IP packets for transmission over the cellular network, and then, when received at the other end of the network, disassemble the packets, sending the payload data out to the locally-connected legacy equipment.

• **Strong security.** While any wireless solution will provide baseline security features, look for wireless products that go even farther to secure SCADA communications. Endpoints should support virtual private network (VPN) pass-through at a minimum, and ideally include built-in IPSec-compliant VPN that can be managed with the same remote management tools. The ideal wireless gateway for SCADA implementations also incorporates embedded firewall capabilities with port and MAC address filtering.
In addition, energy suppliers should seek out products that go above and beyond baseline requirements for ruggedness and manageability.

- **Choose solutions that meet industrial-grade specifications.** Cellular equipment housing, for example, should be solid aluminum, not folded sheet metal or plastic.

- **Use products with built-in wireless modules.** Devices with integrated wireless connectivity are far more rugged and tamper-proof than equipment that relies on a USB stick or PC card to connect to the cellular network. Solutions with embedded wireless capabilities are also likely to have more tightly integrated remote management functionality.

- **Choose solutions that can be upgraded efficiently over-the-air, via software patches.** Energy suppliers don’t want to have to deploy a field service technician every time they need to change the frequency at which they collect data, or update firmware. They also don’t want a bandwidth-hogging solution that requires the entire firmware package to be replaced every time the operator needs to implement a security patch or change a configuration to comply with an evolving wireless standard. IT managers should be able to download new features and patches on a standalone basis, over the air.

- **Choose experienced wireless equipment vendors with global expertise.** Given the long expected operational lifetime of SCADA equipment, energy suppliers need to assure that wireless vendors will be able to support and continually evolve the wireless technology for many years. Seek out wireless vendors with ample experience developing a broad range of wireless solutions, who have certified devices with major cellular carriers in multiple markets worldwide, and who have proven expertise developing wireless solutions for power transmission and distribution systems.

---

**Best Practices for Cellular SCADA Solutions**

- Use endpoints with built-in intelligence to manage session persistence and security.

- Choose solutions with embedded support for hundreds of machine protocols and the ability to incorporate legacy equipment into IP-based systems.

- Choose solutions that meet industrial-grade specifications.

- Choose devices that support remote software upgrades via patches – not just complete firmware upgrades.

- Work with proven, experienced cellular vendors who understand the unique requirements of SCADA systems and critical energy infrastructure.
Laying the Foundation for a Smarter Grid

As energy suppliers continue to build advanced power transmission and distribution intelligence into their infrastructure, wireless communications will present an increasingly compelling option to support SCADA systems. The low operation costs, quick implementation, and broad flexibility of equipment that uses cellular networks makes it an excellent choice for virtually any location not already served by wired connections.

To fully capitalize on the benefits of cellular communications in SCADA systems, energy suppliers should look for wireless solutions that meet core requirements for security, reliability and manageability. They should also look for solutions that embed ample intelligence and flexibility into the endpoint to reduce total cost of ownership over the life of device. Finally, they should seek out wireless partners with proven expertise in cellular solutions for critical energy infrastructure, and extensive experience working with multiple devices and carriers.

For more information about how wireless technologies can support SCADA systems in critical infrastructure, visit www.sierrawireless.com/energy.

Sierra Wireless: A Proven Leader in Cellular Communications for Energy Infrastructure

Sierra Wireless is leading the way in wireless communication technologies for energy transmission and distribution. Sierra Wireless AirLink™ intelligent gateways, routers and programmable modems, and AirLink Management Software, provide a comprehensive portfolio of solutions for energy suppliers and SCADA systems.

Sierra Wireless provides:

- Fifteen years experience in wireless communications for utilities
- Global leadership in M2M communications and industrial-grade terminals
- Industry-leading ALEOS embedded intelligence in AirLink devices, with support for hundreds of protocols and application and security services
- Established relationships with cellular network operators worldwide
- Proven reliability delivering industrial-grade wireless solutions