Selecting the Right Wireless Communications Technology for Your Collection & Distribution Systems

Know Your Options:
Dustin Sayre¹

¹EMA Inc., 1970 Oakcrest Ave., Suite 300, St. Paul, Minnesota, USA
(*correspondence: dsayre@ema-inc.com, telephone: 407-786-5376)

KEYWORDS
wireless, telemetry, radio, technology, antenna, SCADA, security, remote site, remote station, lift station, distribution, collection.

ABSTRACT
Wireless technology changes constantly. For utilities, it begs the question: What do I need to know for my SCADA system to communicate wirelessly with my remote sites? For reuse collection and distribution systems, there are many issues and options to consider.

Collier County Public Utilities’ South County Water Reclamation Facilities (Collier County) uses Ethernet radios as an alternative to trenching hardwire IO to a nearby PLC to monitor conditions, automate operations, and communicate with in-plant lift stations. The goal: to prolong the life of existing equipment and operate pumps more efficiently. Located in a hurricane susceptible region, backup power and local data storage in case of power/communications loss was also important as well as timely notification of equipment failures/alarms.

Referencing Collier County’s story, this paper will help utilities better understand their remote site wireless communication needs, equipping them with knowledge to ask the right questions prior to selecting technology.

Defining Wireless Communications
The basic process of sending data wirelessly is the same regardless of the radio technology used. Process data is collected into groups of data, encoded into data blocks and piggy backed onto a carrier wave. These data blocks can have encryption and error checking encoded in them. This process is known as data modulation. The carrier wave with the data is sent over the air by the radio transmitter to the radio receiver where the data block is demodulated. The radio receiver can check the data block for errors and records an acknowledgement that the data block was received successfully. In some radio systems, such as Ethernet radios, the remote radios send the received data acknowledgement back to the master radio as a means of error checking. This entire process happens many times a second.
Reasons To Use Wireless Communications

Reliable, real-time process data is a lifeline for your organization. Wireless radios have become a very economical solution to communicating with those hard-to-reach remote locations that have previously only had local control. Traditionally, the use of wireless radios has been to monitor and control remote operations over long distances. Today, it is less expensive to use radios to talk to a lift station across the street than to trench underneath the road and use a hard wired connection.

Wireless technology is constantly changing. For utilities, it begs the question: What do I need to know for my SCADA system to wirelessly communicate with my remote sites? For reuse collection and distribution systems, there are range of issues and options utilities must consider relative to their wireless communication with remote sites.

Determine the Functional Requirements of the Radio System

Determining the functional requirements of the radio system first, ensures your organization is selecting the right hardware technology optimized for your specific needs. The following are functional requirements that should be considered prior to hardware selection:

*Location.* The directional location of the remote sites to the master site and the distance away from the master site will determine the antenna type.

*Bandwidth.* Determine the data throughput required by determining how many data points per site and how often the data should be gathered. The distance of each remote site from the central master location also plays a factor in the bandwidth. Bandwidth decreases as the distance between radios increases.

*Dependability.* How long can the organization make educated process decisions without remote process data during a storm event or power outage? System downtime is usually one of the most important factors in designing a wireless communications system. Support of local data storage in a communication loss event may also be important.

*Flexibility.* Should the remote sites be able to function in a standalone fashion when a communications loss event occurs? If a robust radio network with no downtime is required then an alternate communications path may be required.

*Security.* Does maintenance staff need the ability to make programming changes to the remote sites from a central location? Is data security at the PLC level important?

*Interoperability.* Design a system that integrates easily into the existing SCADA system architecture.

There are many questions to answer when considering what wireless technology to use for your organization. First determining the functional requirements of the system makes selecting the right technology much easier.
Factors for Determining the Right Communications Technology

Determine the available communication ports on the devices the radio system will use to communicate with the device. If the devices are serial (RS-232 or 485 connections on the device) then there are limitations on bandwidth and some advanced features that Ethernet radios offer.

The IT industry has paved the way for data security reliability and error checking with Ethernet communications standards, including wireless radio standards. If the devices with which the radios will communicate have Ethernet capability, then Ethernet radios offer many advantages over serial radios. Many radios on the market today offer both serial and Ethernet connections to make transitioning from an older technology serial radio system to an Ethernet radio seamless. These radios either talk Ethernet or serial communications but not both. A true hybrid system capable of communicating with both Ethernet and serial communications at the same time does not exist.

There are a few considerations to take into account when deciding between using licensed frequency bands verses unlicensed frequency bands. Using an unlicensed frequency band saves money over time by not having to pay yearly licensing rights to the FCC. In urban areas, where many unlicensed radios may be present or planned for in the future, a licensed frequency will save the headaches of intermittent radio communications down the road. By licensing a frequency, the FCC will regulate others from using that same frequency band in your geographic area. Most of the recent growth in wireless technology has been in the unlicensed spectrum.

Selecting the frequency of the radios is a tradeoff between bandwidth and the distance the radios have to communicate. Distance and obstructions are a very important factor in selecting the radio frequency. Generally lower spectrum frequencies will travel farther and have better ability to penetrate obstructions such as tall structures and trees. Higher frequencies are becoming more popular with low-power consumption and greater bandwidth, allowing more data to be transmitted. The higher the frequency of the carrier wave, the more susceptible it is to obstructions, especially pine trees and metal structures. Pine trees have dense needles throughout the year and hold moisture and snow creating a dense blanket through which the signal must shoot. Structures dramatically degrade radio signals, and metal structures can even completely block radio signals from penetrating. See the table on the following page for common frequency bands:

License-free, spread spectrum, frequency-hopping radios were developed for use in urban areas where there may be many radio systems on the same license-free band of the frequency spectrum. These frequency-hopping radios are designed to operate under the FCC’s Part 15 license-free rules. These radios allow the radios receiver to avoid interference from other radio system transmitters in the same frequency band by changing the frequency in set pattern with its paired transmitter. Frequency hopping also provides frequency diversity for more reliable transmission.
Frequency Band vs. Data Throughput

<table>
<thead>
<tr>
<th>Frequency Band</th>
<th>Data Throughput</th>
<th>Type</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>136-174 MHz</td>
<td>&lt; 1 Mb</td>
<td>Licensed</td>
<td>10 miles</td>
</tr>
<tr>
<td>215-240 MHz</td>
<td>&lt; 1 Mb</td>
<td>Licensed</td>
<td>10 miles</td>
</tr>
<tr>
<td>406-512 MHz</td>
<td>&lt; 1 Mb</td>
<td>Licensed</td>
<td>10 miles</td>
</tr>
<tr>
<td>902-928 MHz</td>
<td>1 Mb</td>
<td>Unlicensed</td>
<td>10 miles</td>
</tr>
<tr>
<td>928-960 MHz</td>
<td>1 Mb</td>
<td>Licensed</td>
<td>15 miles</td>
</tr>
<tr>
<td>2.4 GHz</td>
<td>1 Mb</td>
<td>Unlicensed</td>
<td>10 miles</td>
</tr>
<tr>
<td>4.9 GHz</td>
<td>50 Mb</td>
<td>Unlicensed</td>
<td>10 miles</td>
</tr>
<tr>
<td>5.3/5.4/5.8 GHz</td>
<td>100 Mb</td>
<td>Unlicensed</td>
<td>50 miles</td>
</tr>
<tr>
<td>6.0 GHz</td>
<td>2000 Mb</td>
<td>Licensed</td>
<td>50 miles</td>
</tr>
<tr>
<td>13.0 GHz</td>
<td>2000 Mb</td>
<td>Licensed</td>
<td>75 miles</td>
</tr>
<tr>
<td>23.0 GHz</td>
<td>2000 Mb</td>
<td>Licensed</td>
<td>75 miles</td>
</tr>
<tr>
<td>57-64 GHz</td>
<td>1000 Mb</td>
<td>Unlicensed</td>
<td>75 miles</td>
</tr>
</tbody>
</table>

*This table provides estimated data throughputs and distances based on typical environmental factors. The data throughput and range varies greatly with environmental factors and hardware.*

Selecting a radio technology usually requires a balance between distance and bandwidth. There are many testing companies that offer radio studies to determine the best radio frequency and path to avoid signal loss.

**Communications Protocols and Drivers**

Communication drivers act as the interface between the Human Machine Interface (HMI) software and the controller. Selecting a driver protocol that can grow with the organizational needs and the SCADA system is important. This paper discusses three of most commonly used drivers in industrial process monitoring and control.

**Modbus** was developed in 1979 as a communications driver between instruments and controllers. Modbus has since grown without regulation to encompass wireless communications, TCP/IP encapsulation (Modbus-TCP) and many other industrial applications. Modbus is a simplistic driver with very little security and limited data types. Many manufacturers of devices that support Modbus add custom extensions to their devices to extend the functionality of the driver. Modbus has proven to be a reliable driver for wireless communications but due to the simplicity of the driver and limited data types, this driver language does not have room for expansion to new security regulations and evolving technologies. Modbus requires additional protocol converting hardware to communicate with many controllers. Modbus can be very efficient communication driver when using limited bandwidth serial radio systems.

**OPC Data Access** was developed in the early 1990s by Microsoft for process control and automation systems to interface with the Microsoft Windows operating system family. This standards based
architecture defines data types and protocols for accessing data from any device in the same manner. The easy interoperability between different industrial devices has made OPC an industry standard and the most widely used communications protocol in SCADA systems. Many automation products name the driver developed from these standards “OPC.” This driver is compatible with almost all industrial devices. This driver is TCP/IP compliant, making it compatible with Ethernet radios, and this driver has data encryption capability built in.

**DNP3** was developed in 1990 specifically for electrical utility SCADA applications. DNP3 offers a complex driver structure that supports many different data types with or without device time stamping and offers PLC level data encryption, meeting the new utility security standards. DNP3 has recently grown in popularity in other industries like water/wastewater because of new standards on the horizon. DNP3 is compliant with TCP/IP protocol, making it a good driver to use with Ethernet radios. DNP3 also supports dynamic failover of wireless communication links and can store data locally on communication failure. If the system supports multiple radio paths DNP3 will try the alternate path on communications failure of the primary. If the primary and secondary path fails DNP3 can store up to 200,000 data points that will automatically transmit and backfill the historical server once communications have been restored. The historical server must be able to accept device-based time stamps for data backfill to work correctly. This is a very helpful feature during severe storm events. Not all devices offer all the features of DNP3, and some controllers are not DNP3 compatible.

**Cyber Security**

Cyber security and network security is a big concern for all organizations and a big topic as well. This paper focuses on some basic concepts for wireless security. There are two main pieces to wireless security: network security to access to the communications infrastructure, and security of the data itself. A compromised Ethernet radio is as good as letting a hacker into your server room to connect directly to the network switch. Most Ethernet radios make use of 802.1x authentication, AES-128 encryption and automatic rotating key algorithms to combat data intercepting and unauthorized access.

All radio equipment should be kept in a locked secure location. All radios should be set up with a static list of approved devices with which to communicate. After three failed login attempts, the radio should ignore login requests for a period of time. There is a lot of information on wireless security available. The following are recommended articles on SCADA security information:

- 21 Steps to Improve Cyber Security of SCADA Networks
  www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf


• DHS Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies (2009)

Selecting a Controller

Determining the functional requirements of the radio system first, ensures your organization is selecting the correct hardware technology optimized for its specific needs.

Remote I/O Module. Remote I/O has limited expansion and data handling capabilities. Remote I/O modules purely move data to and from a remote location; there is no local control with remote I/O modules.

Remote Telemetry Unit. Also called RTU; is specifically designed for remote wireless applications. RTUs are not designed to handle a medium amount of I/O and offer local control. RTUs make use of many of the advanced features of wireless technology and drivers. Many RTUs are DNP3 compliant.

Programmable Logic Controller. Also called a PLC; has capabilities for large I/O counts and advanced local control. PLCs usually require communication cards and IO cards making large systems expensive. Some PLCs are not DNP3 compliant yet.

Antennas

An antenna can be defined as a length of conductive metal that radiates radio signals usually a quarter or half the wavelength of the carrier frequency. There are three general types of antennas: yagi, omni, and parabolic antennas. Yagi antennas are uni-directional antennas usually a horizontal pole with rings or bars protruding from the top and bottom. Yagi antennas emit a focused energy transmission in one direction resulting in benefits of higher signal gain and reduction in outside noise and interference. Omni antennas usually look like a vertical rod and radiate a signal in all directions. Omni antennas are usually used to communicate with more than one remote location. Parabolic antennas resemble a flat or slightly curved dish or square. These antennas are focused transmission directional point to point antennas generally used in high bandwidth applications. With yagi and parabolic antennas positioning is very crucial for good signal strength.

Case Study in Collier County, Florida

Collier County had a need to monitor remotely and control lift stations close to their wastewater treatment plant. The lift stations previously had limited local control. A preliminary price comparison
was done to determine if a radio system would be the most economical way to achieve remote control of the lift stations.

There was concrete and asphalt between several liftstations on the wastewater treatment plants property and the control room. In a price comparison it was determined that a radio system was cheaper than trenching conduit, slab sawing, or directional boring under the concrete. The project was to install a new PLC at each lift station for control and a radio system to communicate to a central location, the control room. 900 MHz frequency-hopping Ethernet radios were chosen due to their low cost and high reliability. Yagi antennas were used at the remote sites to reduce noise from other 900 MHz radio systems in the area. An omni antenna was mounted on top of the control room with line of sight to all the lift stations. The master radio was able to be directly polled by the SCADA software without the need for a polling PLC due to the radios Ethernet compatibility. The SCADA software used the OPC driver to communicate with the liftstations because it was already employed in the current SCADA system. The polling scheme was setup directly using the OPC driver configuration tools. An ups system was installed at each liftstation to maintain radio communications in a power outage until the generators could be started. To increase security remote administration was disabled on all radios. The radios were programmed to only communicate with radios in the current system using both IP addressing tables and the radios host name.

This was a simple cost effective application of how radios can save your organization time and money. Radio systems are becoming very popular to communicate with remote sites in short proximity to the central control room as well as those distant remote sites over 50 miles away.

---

List of Acronyms:

SCADA .............. Supervisory control and data acquisition
FCC ................... Federal Communications Commission
PLC .................... Programmable logic controller
Omni.................. Short for omnidirectional
TCP/IP ............... Transmission control protocol/internet protocol
RTU ................... Remote telemetry unit
I/O ..................... Input/output
HMI................... Human machine interface
AES .................... Advanced encryption standard

---

Dustin Sayre has been a Project Engineer with EMA for over 5 years. He specializes in control system automation, wireless telemetry and photovoltaic systems. Dustin is currently upgrading a water distribution system from licensed serial radios to unlicensed Ethernet radios using a phased approach where downtime is a critical concern.