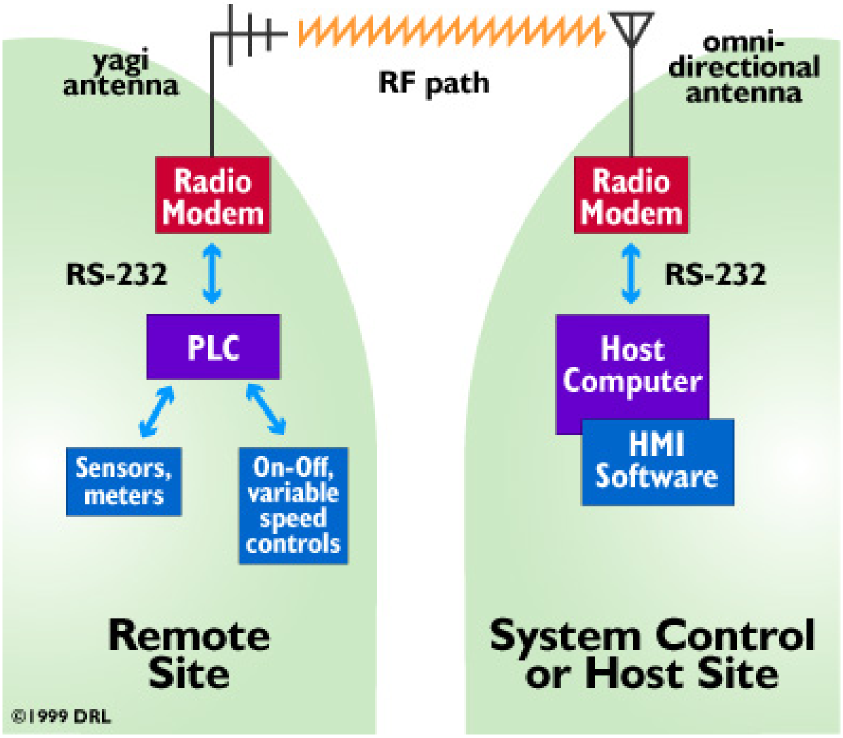
Design and Troubleshooting Wireless Ethernet/Serial Irrigation Systems

By Kim Heiner
Western Regional Sales Manager
CalAmp

SCADA: Supervisory Control and Data Acquisition

The purpose of this article is to provide some insight into design considerations for wireless communication networks as used in modern SCADA systems. With some basic knowledge of design considerations, it is easier to take the right automation approach and choose the right equipment for the task at hand.

Wide area SCADA systems provide a means of remotely monitoring events and controlling machinery at unattended locations. To accomplish this task, as in any system design, various disparate components must be integrated. In this case they include: sensors and metering devices, motor controls, programmable logic controllers, a communications network to link it all together, a host computer and HMI software. Sometimes, remote site hardware and wireless communications gear is packaged together in a NEMA outdoor rated equipment enclosure. In this instance, the equipment may be referred to as an RTU or a Remote Terminal Unit.



Making all these items work together harmoniously to achieve your objectives is the responsibility of the system designer and the system integrator, and this is where they prove their value.

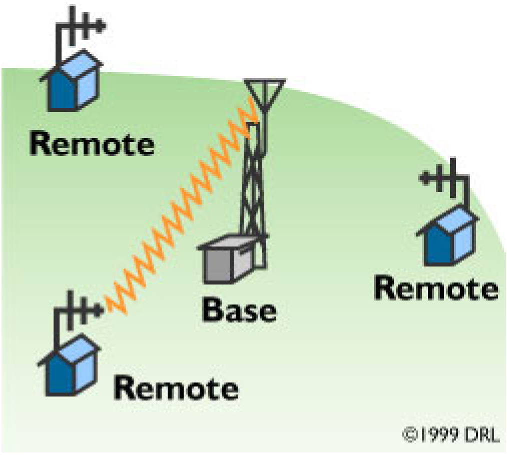
Where did it all start?

In any SCADA system, the remote site's PLC communications to the control point pass through an RS-232 serial port. In older designs, a modem converts the serial digital data into analog 'mark' and 'space' audio tones that are sent long distances over leased or dial-up communications lines. By this means, connectivity is provided for wide area SCADA applications.

Over time, licensed two-way radio displaced the phone line as the most popular communications medium. This has happened for two main reasons. First, though the reliability of the US telephone infrastructure is second to none, mission critical communications are best trusted to a network under one's own direct control. Second, and equally as important, is the high recurring cost of leased telephone lines. SCADA users have historically found that their wireless data network pays for itself in a relatively short period of time.

Architecture

In the SCADA world today, the vast majority of systems are set up in a 'polled' architecture, as opposed to a 'report by exception' architecture. In a polled architecture, the system control point, or host, initiates all data transmission sequences. No remote site reports its status until the host asks for it. Polled systems are designed to poll every few seconds or minutes or hours, depending on how often information updates are required. If pressed, the capabilities of modern high-speed radio modem hardware make it unlikely that any retrieved data will be 'stale.'



'Report by exception' may be utilized when constant operational updates from remote sites are not required and traffic volume is light. In 'report by exception' architecture, remote sites send updates only when a 'change of state' occurs. As remote sites are often out of radio range of each other, some provision must be made for avoidance, and recovery from, 'on the air' collisions as would happen during simultaneous data transmission attempts. This can increase system complexity and cost, and may not offer ideal performance, particularly if later system expansion is anticipated.

Unlicensed vs. Licensed Radio

Today, the savvy wireless data customer is presented with a wide variety of communications options. In addition to licensed radio, there is now unlicensed radio. Unlicensed radio has the obvious appeal of being license free. The downside is that since it is uncoordinated spectrum, unlicensed radio has become somewhat unreliable as it has become more crowded.

Unlicensed wireless SCADA networks find themselves sharing spectrum with an increasing number of industrial and consumer devices such as: cordless telephones, baby monitors, wireless LAN devices, and amateur radio operators.   Also, if used legally, the output power of the unlicensed radio must be reduced when very high gain antennas are used.   Additionally, radio propagation at higher unlicensed frequencies is relatively unfavorable as compared to the lower frequency licensed bands.

In the past, licensed frequencies were crowded and difficult to obtain. Sometimes it could take many months to obtain operational authority from the FCC.   However, since 1997, FCC 'refarming' has made it possible to obtain new communications channels and has greatly relieved communications congestion for wireless data users. Additionally, wireless data users have discovered that by utilizing professional licensing services, they can receive operational authority in a month or less. Be mindful, however, that not all FCC licensing services are experienced, nor up to date, with wireless data applications and the pertinent spectrum rules.

FCC Refarming

Overall, refarming is a decade long multi-step process. It is affecting both radio manufacturers and radio users. Existing users of two-way wireless devices will find the necessity, sooner or later, to upgrade their equipment to modern ‘refarmed’ equipment. They are, or will make, the transition for one of two reasons: 1) Future FCC regulation of some form will make it unattractive to continue holding a ‘full channel’ of spectrum. 2) The other more immediate and compelling reason is that the full channel user may receive harmful adjacent communication channel interference from newly established half channel users. Conversely, the new half channel user is less likely to receive interference from the incumbent full channel user. This is by virtue of the difference of bandwidth in the new and old design transceivers and the relative spectral position of the two signals. There are other more stringent requirements beyond channel bandwidth that refarming has brought to radio manufacturers, but that is beyond the scope of this article. Suffice it to say that today’s radios are designed and perform with a great deal more precision than in the past.

Radio Propagation Studies

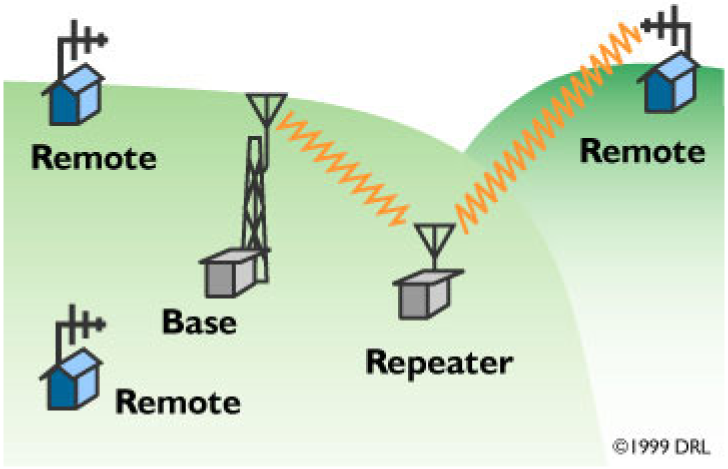
Radio propagation is the study of the behavior of radio waves at particular frequencies over terrain. Regardless of whether you choose licensed or unlicensed radio, it is absolutely essential that you have a propagation study conducted. A radio propagation or path study will determine with a fair degree of certainty whether your radio signal can get there from here. It may demonstrate the need to relocate certain sites or the need to utilize a radio repeater, or use an existing or proposed remote site as a relay station. Additionally, a thorough path study will take into account the need for a 20 to 30 dB fade margin. This allows for uninterrupted communications when the path undergoes temporary and periodic degradation due to atmospheric and/or seasonal changes.

For a small system path study, you may find you can verify radio line of site with portable radios. In doing this, it is essential to eliminate as many variables as possible. Try to simulate the same antenna height and performance and use the same RF output power as will be used in the built-out system. It is also necessary to realize that reliable data communications will require stronger signal strength than for voice communications.

For large systems, it is prudent to perform a computerized path study, preferably before placing a SCADA system job up for bid. Computerized path studies take into account terrain, ground clutter and vegetation profiles, and generally are a good value as they save you and your integrator time and money. If you put your system design out for public bid, you will find that having a previously conducted path study will facilitate the bidding and bid evaluation process for you, and your successful bidder to be.

Repeaters

In some instances, you may discover that your proposed communications to certain remote sites are marginal. Repeaters may be used to extend the communications reach of your control point. Most commonly, an advantageously located remote is utilized as a sub-master which forwards polling requests from the control point to other remote stations.



This type of repeating is called 'store and forward.' It is differentiated from full duplex repeating that performs simultaneous reception and transmission, and requires two radio channels. 'Store and forward' repeating is very common in SCADA system design and it is often chosen for its simplicity and relatively low cost. It takes advantage of features that may already be built into the remote site PLC hardware. Another alternative is to remotely locate your control point radio hardware if your control point does not provide radio coverage to your remote sites.

It may be difficult to justify the added expense of extending your wireless range, but realize that marginal communications will never provide you reliable SCADA system performance, and will cause you aggravation and untimely down time.

Antennas, Feedlines and Lightning Protection

Generally, in a polled system, an omni-directional antenna is employed at the system control point. Omni-directional antennas radiate equally well in all compass headings. The yagi antenna on the other hand is directional and must be pointed in the direction of intended communication. Often, remote sites that communicate only with the control point are equipped with yagi antennas.

Low loss antenna feedline and connectors are required when UHF (commonly 450-470 MHz) or higher frequencies are employed. This is because feedline and connectors exhibit greater losses at higher frequencies, on both transmit and receive. For this reason, UHF frequencies require hardline or rigid wall coax for all runs, whereas low loss RG-8 type coaxial cable can be used for VHF runs of less than 25 feet. Popular UHF (PL-259) feedline connectors can be used at VHF frequencies, but generally the lower loss 'Type N' connector should be utilized for VHF and UHF frequencies.

Lightning is more common in some geographic areas that others. Wherever it happens, catastrophic damage to communications and control system hardware can result. Using a bulkhead mounted lightning surge suppression device with single point earth grounding is a good investment. Many choose to cut corners here, but it is ill advised. Plan to spend money on this part of your system. If you choose to play the odds, you will at some point lose and suffer downtime and loss of system control.

Radio Modem Hardware and PLC Protocols

Customers are also faced with a wide range of radio modem products today. In the past, it was customary to use outboard Bell 202 type 1200 bps modems and interface them to two-way voice type radios. This requires the tedious adjustment, and periodic readjustment, of audio levels between the separate modem and radio.

The Bell 202 solution ignores technology advances that have been made in the last 5 years. Today it is less expensive, over the life of your system, to invest in high speed integrated radio modem products which offer the advantage of easier interfacing and swapping out, higher data and polling rates, more sensitive modem and radio technology, and features like wireless network diagnostics.

Additionally, many users today have a choice between ‘packetized’ and ‘transparent’ radio modem hardware. Before comparing these two alternatives, it is useful to note that PLC devices utilize communication protocols or languages that encapsulate the data stream in an envelope called a ‘packet.’ This envelope surrounds the data with a message start and end marker, an origination and destination address, and a CRC or checksum. These protocols were born in the hardwired world and have transitioned very well into the wireless data world.

As the PLC is already ‘packetizing’ your data, it is more efficient to employ ‘transparent’ communications hardware that does not add an additional second layer of error checking and addressing. There may be situations where this additional overhead buys you something, but in most cases, there is no added value.

MODBUS^{TM} is a popular protocol for wireless communications. Numerous PLC manufacturers have their unique implementation of this protocol. There are other protocols that operate similarly; some are proprietary. Generally, master slave protocols that are framed, employ message addressing, error checking and that are designed for Master-Slave polling, work well in the wireless environment. Truly transparent radio modem hardware requires RTS/CTS hardware handshaking for data flow control. Make sure that your PLC hardware supports this communications requirement if you elect to utilize transparent radio modem hardware.

Wireless Network Diagnostics

Investing your hardware dollars in integrated radio modem devices also provides new features that are becoming indispensable. Wireless network diagnostics is one such feature, which can reduce communication failures, minimize the potential risk of downtime due to equipment or system malfunction, and facilitate a speedy recovery from outages. This results both in a more favorable risk management scenario and a high return on investment for your automation dollars.

In practice, diagnostics at the wireless communication level makes it possible to verify connectivity to a remote site even if your PLC or instrumentation has failed. Some diagnostic methods can even be utilized concurrently with your regular polling cycle to warn of impending communication failures. Your ability to maintain or quickly return your system to service is enhanced by the performance statistics that you can remotely obtain. Diagnostic tools can also be utilized during system deployment, and can speed along the installation process.

Redundancy and Point of Failure

SCADA system designers strive in their work to eliminate as many single points of failure as possible. Redundancy is utilized to minimize the impact of system component failure, often at the system control point. Redundancy increases the system design and deployment cost. If carried to the extreme, it can make operation of the system more complicated and laborious.

In a recent study of automated SCADA systems[1], it was found that 50% of automated systems are run on manual mode. Among the reasons given in this study is "low user confidence in the technology." If system complexity and operator workload is a concern for you, having spare components can be considered a simple and valid safeguard.

In conclusion, it is wise to note that all system design involves 'trade-offs’. It is essential to know and understand the benefits and drawbacks of the individual elements of your system design. Only then will you be able to make the right choice for your application and needs!

[1] Manning, Alan W. 1999. “Status of Automation in the Wastewater Industry” (information presented at Automatic Monitoring Seminar. Water Environment Federation 72nd Annual Exhibition & Technical Conference).