

Radio waves

Data able to travel distances, through obstacles.

By Davis Mathews

Users can go wireless today especially if they need to securely move small amounts of sensor and control information, and at times, mission critical data. This can all happen through spread-spectrum radio—especially in wide-open oil fields and municipal water facilities.

One reason for the greater reliability in these areas is there are no other radios competing for the bandwidth. In addition, because of the 1987 Federal Communications Commission ruling that allocated industrial, scientific, and medical (ISM) spread-spectrum bands, the transmission of data can travel great distances through obstacles.

This provides greater ability to monitor and control some industrial environments. Oftentimes a municipal wastewater facility has scattered I/O modules from multiple tanks located on opposite sides of the highway, and they need to transmit data back to

a central control system. In the past, they used to dig trenches, lay conduit, and pull cable to acquire these signals, which was very costly. In addition, the costs associated with the engineering, inspections, and time needed to acquire right of way before even implementing a solution were also very high.

Wireless I/O interfaces are gaining acceptance in the industrial environment as a solution to this problem. They are less expensive and, with frequency hopping spread-spectrum capability, are proving reliable. An industrial wireless I/O interface can send analog and discrete signals from a sensor to a programmable logic controller (PLC) or from a PLC to a pump specifically, reporting levels, pressure, flow, and alarms to control pumps, valves, and switches by updating data far more than required.

This is the type of situation that faced a water/wastewater facility in Texas. The city of San Antonio owns the public utility called

the San Antonio Water System (SAWS). The city created the utility in May 1992 through the consolidation of three predecessor agencies. SAWS services 1 million people in the San Antonio area. In addition to serving its own retail customers, SAWS also provides wholesale water supplies to several smaller utility systems within the area and provides wastewater collection and treatment.

SAWS had several applications in need of signal readings and indication notifications from remote well sites that had to go back to their control center. One application involved a fluoride residual analyzer, where a 4–20 mA reading from this system was to feed to a supervisory control and data acquisition system and then back to a main control center located downtown. Other applications included remote tanks that needed to send level indication, suction pressure, and well flow information from various remote sites back to the central control center.

By using a wireless I/O interface module, SAWS avoided installing excess conduit and signal wiring. “If we didn’t utilize the MCR-RAD modules we would have had to hard-wire by cutting into streets, and that can get expensive. Not to mention the additional cost and time associated with getting a permit from the city to cut streets,” said Phil McDonald, system manager at SAWS.

SAWS also experienced savings in installation time by not trenching, installing traditional conduit, and hardwiring. They also realized more efficient and less costly labor, as well as reduced start-up costs. The MCR-RAD modules are transmitter-receiver pairs that come factory programmed, calibrated, and tested as sets, capable of carrying one 4–20 mA current loop and two digital status signals. Typical in-plant range is 600–1,000

feet with no line of sight, and they can transmit up to 20 miles. The transmitter and receiver receive power separately with a 12–30 volt direct current source (power supply, battery, solar, etc). The process signals wire to the input terminals of the transmitter and output via wires connected to the receiver. There is no wiring in between. “I hadn’t seen this type of technology before, and it was the best fit for our application,” McDonald said.

The added benefits from this radio module include frequency hopping spread-spectrum (FHSS) technique, which guarantees a license-free, interference-tolerating link between remote devices and the control room.

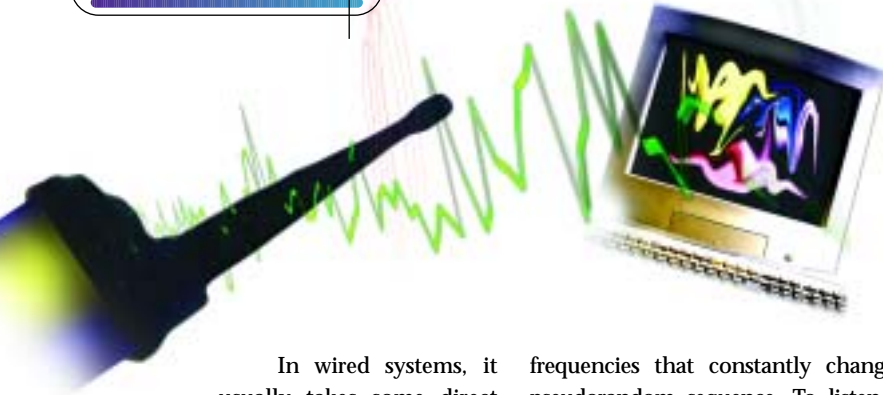
System expandability tends to be an inherent problem area for customers that decide to use single point wireless I/O tech-

nology to transfer or monitor several points located in the same location. The aesthetics of multiple antennas on a control cabinet roof creates confusion and possibly an eyesore. As customers decide on industrial wireless technology, future project planning becomes a key factor in the decision-making process. There are several forms of system expandability to consider, including the ability of bidirectional I/O connectivity and communication integrated on an existing wireless loop. This allows several analog and digital signals (inputs or outputs) to wire onto simple I/O blocks coupled on the FHSS radio platform, making this a wireless multiplexer (MCR-RT-I/O series), eliminating the need for multiple antennas in a similar location.

All types of data transfer offer the opportunity for data interception and injection.



Radio attached to equipment outside the San Antonio Water System.



In wired systems, it usually takes some direct physical connection to gain access, with tampering possible anywhere along the transmission wires. Radio systems, on the other hand, take the potential for data interception or injection out of the realm of actual physical contact, and in addition, different radio systems and technologies set up roadblocks of varying degrees that must be overcome by the wireless intruder.

Going conventional

A single channel radio (where listeners find the radio frequency used and then listen to the bits being sent) has an added element of security over a wire because the data sent by the radio is often encoded and listeners can only make sense of it when they have the appropriate receiver. People without the appropriate equipment to decode the message must therefore find the frequency used and then gain some knowledge of the protocol before they can decode the signal not intended for them. Likewise, injection of data can only happen if the code is broken. This differentiates radio signals from wired communications, which are typically not encoded, for example standard industrial signals such as ON/OFF status and 4–20 mA current. When passing through a radio, these signals become encoded. But when they pass along via wire, they usually are not encoded.

Spread spectrum

To further inhibit unwanted intrusion, the military developed frequency hopping radios that add an additional set of barriers for a would-be intruder to overcome. Like the single channel very high frequency/ultrahigh frequency radios, each packet is encoded, thereby forcing the intruder to gain knowledge of the protocol, identification, and decoding. Unlike fixed frequency radio, the FHSS data continually hops across a wide range of

frequencies that constantly change in a pseudorandom sequence. To listen to the data, the intruder must know (or establish) the hopping sequence and follow along as the FHSS system jumps around. Data transmissions tightly time themselves to make sure both ends of the system are on the same frequency at the same time. To make a FHSS system efficient, the time required to hop from one frequency to another must be very short. This is one of the design difficulties associated with frequency hopping.

With MCR-RAD or RT systems, the intruder needs technical competence, detailed knowledge of the inner workings of the hardware (frequencies, bandwidths, hop and synchronization sequences, and timing), and software (data packet construction, time tracking, synchronization strategy, etc.) in the device. Although a case can be made that nothing is really safe against a determined intruder, in the case of FHSS wireless interface devices, military-type equipment and experience are needed to “break into” this military-type radio.

Users often compare FHSS to IEEE 802.11b. With FHSS radios, the complexity lies with the hopping synchronization of the narrow data signal that remains unaltered. Data remains narrow from transmitter to receiver. The FHSS radio is a narrow band fixed frequency radio—but only for an instant—before it hops to another fixed frequency radio on another channel, and then another, and another, and so on. And it has plenty of room to hop. The 902–928 megahertz ISM frequency band is wide enough to hold approximately 1,000 licensed narrow-band radios.

Small packets of data go to the receiver with hops in a pseudorandom pattern to more than 50 different frequencies around the band before repeating the hopping sequence. Encounters with a significant interfering signal on a frequency generate error detection, and the packet is discarded.

The hopping sequence continues and data updates resume. Interfering signals can knock one packet out of a FHSS radio’s hop pattern, but the rest of the updates get through, no matter how powerful the narrowband interference.

This is very different from IEEE 802.11, which frequency hops until data needs to be sent, then sends a long transmission on a single frequency—not appropriate for mission critical industrial I/O.

FHSS radios do not “avoid” interference; they “tolerate” it. Simply put, the process checks each packet and when it encounters interference, it does not process the bad packet. As the hopping pattern continues, the radio moves along its sequence looking for the next packet to get through cleanly, at which time it outputs the good data. Slow and steady, FHSS radios are the industrial I/O tractors.

FHSS also has the advantage of being a small moving target. Throughput does not cease until the entire ISM frequency band at any one location becomes plugged. This enables the FHSS to reliably get small redundant messages through areas of heavy interference even as interference increases.

802.11b is vulnerable to several direct attacks because it uses the Ron’s code 4 encryption. In addition, 802.11b authentication records one of the authentication procedures, making it at risk for impersonation.

In heavy interference environments the FHSS continues to function until the entire ISM frequency band is jammed (a very unlikely scenario). FHSS is the perfect choice for small packet redundant data—for example, alarm and emergency stop signals—because even though some packets are lost, others get through.

The redundancy of data transmission and small packet size make FHSS the preferable choice for industrial wireless I/O applications such as simple analog and digital signals. The technology provides reliability even in confined environments where many FHSS radios operate. W

Behind the byline

Davis Mathews is a product manager at Harrisburg, Pa.-based Phoenix Contact Inc. His e-mail is dmathews@phoenixcon.com.