

Strategic Implementation of Wireless Technologies

PD-06-121

**By: Brent E. McAdams
FreeWave Technologies**

The evolution in wireless technologies has opened the door to a new class of plant automation architecture that offers adopters a significant strategic advantage. Driven by substantial and measurable cost savings in engineering, installation, and logistics, as well as dramatic improvements in the frequency and reliability of field data collection, automation experts and IT professionals are presented with an opportunity to deliver a major, positive impact to their respective company's bottom line.

In terms of the key drives associated with adopting wireless technologies, the cost benefits are the most intuitive. However, another important consideration is safety. Some of the key drivers include:

- **Installation savings** — Installation of wirelessly connected assets is up to 10 times cheaper than the wired alternative and offers much faster startups and accelerated profits. In addition to the installation savings, engineering costs are dramatically reduced as extensive surveys and planning are no longer required to route wire back to junction boxes or control rooms. The reduced costs in wiring engineering, installation and maintenance combined with the increased data gathering flexibility is the primary driver for wireless migration.
- **Better information** — Replacement of manual readings with automated measurement results in information that is more accurate, timely, and consistent.
- **Economy of Scale** — Deployment of additional points in a network is incremental and may include integration into legacy systems.

- **Operational Savings** — The ability to quickly diagnose and troubleshoot plant operations and support predictive maintenance programs by monitoring facility assets. Additionally, identify costly problems leading to excess use of energy or raw materials.
- **Safer Operations** — By reducing human exposure to hazardous environments. Also, more frequent measurements and early detection of issues can help reduce or even prevent incidents or accidents.

Unfortunately, there is no one type of wireless technology that solves all problems. Therefore, in order to maximize the return on industrial wireless networking investments, companies must be able to select the best technology for a given application.

By evaluating the attributes of various wireless technologies, essential technology decisions can be made to guarantee the successful implementation of a wireless architecture solution. These attributes include the RF technology itself, security, interference rejection, sensitivity, power management and the ability to embed wireless into existing OEM technologies. Furthermore, the determination needs to be made whether new systems may interface with existing systems for the purpose of preserving investments in existing infrastructure. Determination might also be made with respect to the radio providers' commitment to backward compatibility to extend the life of the system and drive down the overall lifetime cost of implementation.

Licensed vs. Unlicensed

In 1985 the Federal Communications Commission (FCC) issued rules permitting use in the Industrial, Scientific and Medical (ISM) Bands (902-928MHz, 2.4-2.4835 GHz, 5.725-5.85 GHz) at power levels of up to one Watt without end-user licenses. There are two very common spread

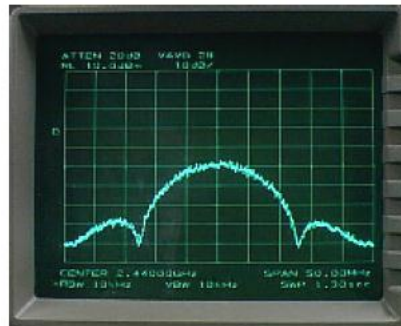
spectrum modulation methods used in these bands: Frequency Hopping (FHSS) and Direct Sequence (DSSS).

FHSS

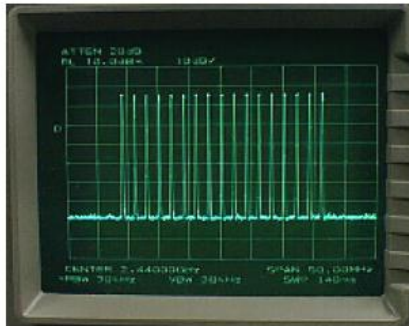
Rather than transmitting over a static spectral segment, FHSS radios pseudo-randomly vary carrier frequency, quickly hopping through multiple channels while sending data. Interference is avoided by hopping over different frequencies, each of which has a different interference effect or characteristic. This provides FHSS with collision-free access by allocating a specific time slot and frequency for its transmission. A frequency-hopping scheme, combined with error detection and Automatic Repeat requests ensures that the data is reliably delivered. Further, with FHSS systems, it is anticipated that there will be competition for the airwaves, so interference avoidance and management are designed into the system. Other modulations are more susceptible to interference because they do not anticipate interference by design.

DSSS

Direct Sequence spreads a narrow-band source signal by multiplying it with a pseudo-random noise signal. The resulting signal is then spread over a large range of continuous frequencies. This introduces redundancy into the transmission, enabling a receiver to recover the original data even if parts of it are damaged during transmission.



DSSS



FHSS

Licensed

In addition to the unlicensed ISM Band, licensed radios operate in the UHF and VHF bands, and as the name indicates, users must purchase a site license to operate radios in a specific area. Consequently, these systems can be expensive to setup, and offer slow data rates (i.e. typically ≤ 9600 kbps), which are not likely to support industrial data communication requirements in the future. However, UHF/VHF radios are allowed higher transmit power which increase the range and because they operate at lower frequencies, they typically have better propagation characteristics. However, one of the draw backs of a licensed system is that only one system can operate at that location. Therefore, overlapping networks and other communication capabilities using the same frequency band is not possible.

Spread Spectrum Advantages

Spread Spectrum has two significant advantages over fixed frequency licensed radio transmissions. The first is that no FCC license is required by the user. Even though licensed spectrum is available, the user must go through the process of obtaining the license. Once obtained, they are good for a single site and have a defined term.

The second advantage Spread Spectrum, specifically FHSS, has over fixed frequency transmission is that Spread Spectrum radio transmissions are far less susceptible to interference. In an industrial plant environment, machinery and other equipment generates interference over a very broad spectrum of frequencies. Therefore, if one frequency is affected in a FHSS system, for example, the data is quickly transmitted over another, clear channel. This gives the technique greater coverage, channel utilization, and resistance to noise than comparable direct sequence systems. A licensed solution has no such capability.

FHSS Characteristics

FHSS technology has immediate advantages in terms of security, immunity to interference, robustness, and network reliability.

Security

FHSS systems were originally designed for military applications during World War II. The very impetus for these systems was data security and interference avoidance that existing fixed frequency systems could not reliably provide. Concerns about the integrity of signal transmission and reception are prevalent amongst adopters who are worried about leaving their control and business networks vulnerable to hacking or denial of service attacks. In fact, the issue of security is widely seen as the most significant barrier to industrial wireless adoption. FHSS technology has inherent advantages in terms of security, immunity to interference, robustness, and network reliability.

Since, as the radios communicate, their communication frequency is changing rapidly (as much as 1000 times per second), FHSS provides an additional layer of security and makes

transmissions very difficult to detect. To outside listeners, transmissions simply look like noise spread over the spectrum, with only a small signal at any one given frequency.

This technique assures the integrity of the data, because without the hopping sequence, no outside sources can listen to a communication. This technique also allows communications to continue even if a number of the frequencies in the 26MHz band are blocked. The devices simply hop to another frequency.

Additional data security is gained through 128bit and 256bit Advanced Encryption Standard (AES). The AES algorithm uses an encryption key (password). Each encryption key size causes the algorithm to behave slightly differently, so the increasing key sizes not only offer a larger number of bits with which you can scramble the data, but also increase the complexity of the cipher algorithm.

Data Integrity

As with existing data transmission over wire, Packet Protocol Acknowledgment is supported by error checking. Error checking is designed to insure that the data received by any spread spectrum radio is not forwarded from its buffer until it is acknowledged as a correct transmission, guaranteeing that what is received is identical to what is sent. In order to accomplish this, a CRC or Cyclic Redundancy Check is generated giving the packet a unique digital signature.



Data Packet

The probability of detecting any random error increases as the width of the checksum increases. Specifically, a 16-bit checksum will detect 99.9985% of all errors. This is far better than the 99.6094% detection rate of an eight-bit checksum, but not nearly as good as the 99.9999%

detection rate of a 32-bit checksum. With a 32-bit CRC there are over 4 billion possible CRC values. To be exact that's 2^{32} or 4,294,967,296. By comparison, the commonly used 16-bit CRC offers a chance data error in one in 65,536 transmissions (2¹⁶), a relatively small number of transmissions in a work cycle especially given that many radios transmits packets as often as 50 to 100 times per second.

Sensitivity

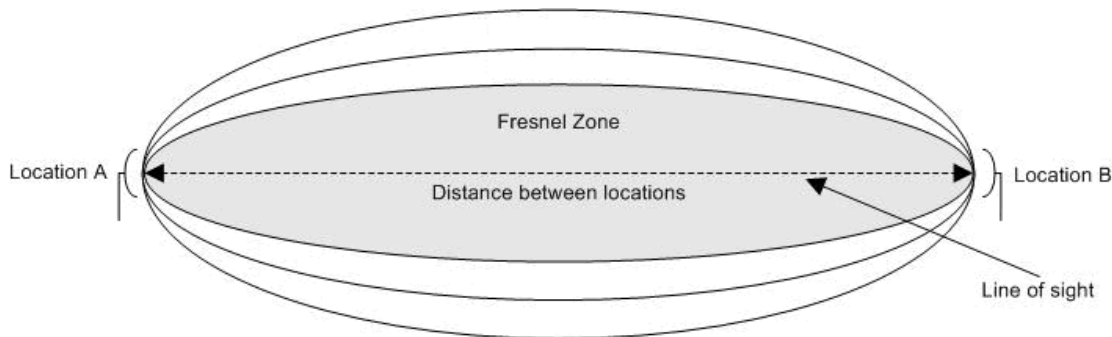
Receiver sensitivity is an important specification to consider. The more sensitive the receiver, the weaker the transmitted signal can be yet still get through. In other words, the distance and obstructions between a transmitter and receiver can be greater.

One reason that receive sensitivity may be confusing is that it is expressed in a unit of measure known as a decibel (dB). A decibel is a ratio expressed on a logarithmic (exponential) scale. A 10:1 ratio is 10 dB and a 2:1 ratio is 3 dB. A 1:1 ratio is 0 dB, while ratios of less than 1:1 are expressed as negative numbers. For example, a 1:2 ratio equals -3 dB.

Because receive sensitivity indicates how faint a signal can be successfully received by the radio, the lower power level, the better. This means that the larger the absolute value of the negative number, the better the receive sensitivity. For example, a receive sensitivity of -110 dBm is better than a receive sensitivity of -107 dBm by 3 dB, or a factor of two. In other words, at a specified data rate, a receiver with a -110 dBm sensitivity can hear signals that are half as strong as a receiver with a -107 dBm receive sensitivity.

Fresnel Zone & Antennas

For the shorter range installations in industrial facilities, a common question is, "Is line of sight required for all radio links? The answer is often, no, but radio waves can travel through a variety of objects with different levels of attenuation. The area over which the radio waves propagate from the antenna is known as the Fresnel Zone. Like the waves created by throwing a rock into a pool of water, radio waves are affected by the presence of obstructions and may be reflected, refracted, diffracted, or scattered, depending on the properties of the obstruction and its interaction with the radio waves. This is often how the signal gets to the receiver when there is no line of sight. However, this effect attenuates the signal, and affects how a radio will operate without line of sight.



Proper use of antennas and the ability to adjust output power provide a great degree of assistance in overcoming these issues and getting messages through. Industrial quality directional and high-gain omni-directional antenna allow the radio communications at long distances through a crowded industrial facility. At the same time, the use of low-gain antennas can be used to keep radio signals from straying unwanted distances or directions.

Flexibility

With many existing wired networks, the user is locked into using only one particular protocol simultaneously. Alternatively, by using wireless architecture, several protocols operating over the same communications layer is possible given the user greater flexibility.

Any wireless device needs to tie into existing control systems. Getting information into the myriad of existing control systems is not a small task. The 4-20mA signal and switch closures are universally translatable. Digital input allows more data flow at significantly lower cost, but generally adds a level of complexity to any system. Modbus and OPC servers offer degrees of acceptance where large data flows are required.

Temperature Range

Products intended for industrial applications should use industrial-rated components and therefore reliably operate over industrial temperature ranges (i.e. -40° to +75° C). Temperature extremes are commonplace in many applications. In addition, these products are generally better constructed than consumer devices, and continue reliable operation under shock and vibration conditions.

Operation in Hazardous Environments

Industrial wireless modems typically carry some form of UL certification. Most commonly this UL certification is for Class 1, Division 2 environments which permits radio operation in the presence of flammable or explosive gases, fluids, or vapors. Having this certification is also beneficial because a company can standardize on a single type of device, and use it for many applications, regardless of the environment.

Applications

- **Wireless I/O** - Asset information is available from applied and embedded sensory points enabling sophisticated diagnostics, remote monitoring and control, and plant optimization. The form factor of wireless devices allow for easy integration into existing

OEM technologies and housings.

- **Safety** - Environmental alarms and personnel management allows for greater safety and compliance with OSHA regulations, especially in dangerous environments and in locations where the plant is in close proximity to residential areas. Also, completely unmanned first response systems are now available limiting human exposure in the event of a release or catastrophic incident.
- **Security** - Detect intrusions, control access, report smoke/fire, or perform video surveillance within the facility.
- **Workforce Mobility** - Wireless connectivity allows mobile workers to access their application and perform their job where they work. Whether it is logging data or managing operations, worker mobility impacts productivity and efficiency.
- **Mobile asset and Material Tracking** - Tracking asset location allows for better use of assets as well as regulatory compliance for the use, storage, and transport of hazardous chemicals.
- **Integrated Technologies** - Wireless sensor networks, or Mesh Networks, represent an emerging technology that has great potential for widespread applications. These networks consist of a large number of simple nodes with limited power sources and functionality, but they offer greater utility than the sum of those individual nodes. Greater flexibility and connectivity may be achieved by integrating these networks with other wireless technologies.

Summary

Information is power. As such, the ability to gather time-critical information, digest it, and react upon it is the key to continuously adapting to change with increasing reliability and profitability. No one type of wireless technology solves all problems. Therefore, it becomes very important that the necessary monitoring, management, and security capabilities be evaluated to ensure the wireless architecture selected maximizes limited resources, while at the same time allowing the disparate applications to share the spectrum within the context of their importance, time sensitivity and mission criticality.