APRIL 2015

PHOENIX CONTACT
INSPIRING INNOVATIONS

So Many Wireless Technologies … Which Is the Right One for My Application?

Don P. Dickinson
Senior Business Development Manager – Water Sector
Phoenix Contact USA

Abstract

Wireless technology has transformed our world. The demand for mobile communications and computing continues its dramatic growth, driven by the proliferation of smartphones and tablets. The use of wireless in industry continues to grow as well.

Wireless technology has been used in industry for many years and has provided reliable communications for monitoring and controlling remote processes, including mission-critical applications. However, license-free wireless technologies are giving industry even more options for solving application needs, such as wireless networking for the mobile worker and wireless sensor networks for process optimization and asset management. But which is the right technology for your application? Understanding the capabilities and limitations of the various technologies will allow users to realize the benefits of wireless while avoiding the problems resulting from misapplication. This paper provides an overview of the various license-free, spread-spectrum technologies and their appropriate use for industrial applications.

TABLE OF CONTENTS

Introduction

Wireless technology has come a long way since the development of wireless signaling techniques in the late 1800s. Today, wireless technologies of many |types are used in a variety of applications, ranging from garage door openers to satellite communications. There are many types of wireless technologies, and many questions arise when considering which wireless technology to use. How far does it go? How fast can data be transmitted? Is it secure? Is it reliable? How much does it cost? The answers to these questions vary greatly, depending on the wireless technology being considered. Generally speaking, there is no one technology that does everything you may want it to do. A particular wireless technology is chosen for a given application because the performance characteristics of that technology best align with the application requirements.

There are many types of wireless technologies used by the general public today. These technologies differ from one another in their modulation techniques, data transmission rates, transmission distance, security, cost, complexity and power consumption. Some wireless technologies may be quite familiar to and widely used by the general public, such as Wi-Fi (short for Wireless-Fidelity), Bluetooth and cellular. Other technologies may be unfamiliar. Some technologies are proprietary — intended for specialized applications not addressed by other technologies.

Wireless has been used in industrial applications for many years, primarily in industry market segments that have a decentralized infrastructure, such as water or oil and gas. Traditionally, the use of wireless in industry has been driven by the need to monitor and control operations over long distances. However, wireless increasingly provides new ways to address a wide variety of needs in all industry segments.

Licensed and Unlicensed Wireless

The Federal Communications Commission (FCC) regulates the airwaves in the United States and oversees many types of wireless transmissions. Most wireless transmissions require a license, issued by the FCC, that authorizes transmission at a particular frequency and power level. If another transmission interferes with a licensed transmission, the licensee has legal recourse to terminate the interfering transmission. Similarly, a licensee's transmission cannot interfere with a transmission on another frequency.

Licensed radio transmissions have been used in industry for many years and will continue to be used when a signal is transmitted over long distances (many miles). However, there has been dramatic growth in the use of license-free wireless technologies by the general public and industry. These technologies have greatly expanded the range of needs addressed by wireless and offer many new benefits for users.

Industrial, Scientific and Medical Bands

In 1985, the FCC allocated segments in the radio spectrum for license-free transmission. These segments are known as the Industrial, Scientific and Medical (ISM) bands. Many devices that we use daily, such as cordless phones and wireless routers, operate in the ISM bands. These devices are not limited to communication devices. Even microwave ovens make use of the ISM bands by cooking food with electromagnetic waves in the 2.4 GHz band. Although an FCC license is not needed to operate these devices, there are specific requirements for frequency, power and technology used. Additionally, the manufacturer of a wireless device must meet provisions of FCC Part 15, which ensures that unlicensed transmissions do not interfere with licensed transmissions.

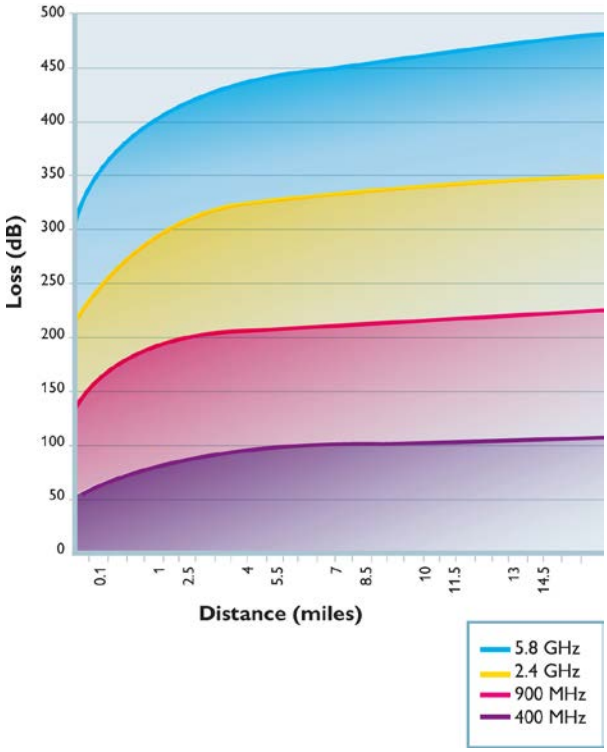
License-free transmissions are allowed in three bandwidths: 900 MHz, 2.4 GHz and 5.8 GHz. These are shorthand designations for the bands. Table 1 lists the specific range of frequencies for each band. It is important to note that other countries may not recognize these same bands for license-free transmissions. All three bands can be used in the United States. License-free transmissions in the 900 MHz band are not permitted in many countries; however, the 2.4 GHz band is considered license-free throughout most of the world. Confirm suitability before selecting a wireless device that will be used outside the United States.

Band	Frequency Range
900 MHz	902 – 928 MHz
2.4 GHz	2.400 – 2.500 GHz
5.8 GHz	5.725 – 5.875 GHz

Table 1: The ISM Bands

The performance of a wireless device is influenced greatly by the frequency band in which it operates. The lower the frequency, the farther the signal will travel and the better it will penetrate solid objects. Figure 1 shows signal loss (attenuation) in free space for different frequencies. Differences in attenuation are even greater when objects are introduced into the signal path.

Figure 1: Free Space Radio Frequency Attenuation



PHOENIX CONTACT
INSPIRING INNOVATIONS

Industrial, Scientific and Medical Bands (*continued*)

Although transmissions in the 900 MHz band go farther, the 2.4 and 5.8 GHz bands offer greater bandwidth and higher data transmission rates. Which band is best depends on the application. A wireless link sending network data needs as much bandwidth as possible, whereas a wireless device controlling a pump two miles away has to contend with the challenges of distance more than the speed or amount of data being sent. The choice of which band to use is not determined by the user. Public wireless standards such as IEEE 802.11 (wireless Ethernet, commonly known as Wi-Fi) specify the frequency band to be used. The band for a proprietary device is selected by the manufacturer for the intended application.

A key difference between the 2.4 and 5.8 GHz bands is channel allocation. For example, when used for Wi-Fi, the bands are segmented into channels. In the United States, there are eleven channels in the 2.4 GHz band. Of the eleven, only three are non-overlapping. Communications on overlapping channels can interfere with one another and diminish the performance of wireless transmissions.

The 5.8 GHz band has eight channels. All are non-overlapping. The 5.8 GHz band offers the flexibility of having multiple networks that do not interfere with each other. However, there is greater attenuation in the 5.8 GHz band, resulting in potentially shorter transmission distances than in the 2.4 GHz band.

As stated previously, the 2.4 GHz band generally is allocated for license-free transmissions throughout the world. There are many wireless devices operating in this band. As a result, congestion could be a potential issue for new or future installations. Regardless of the frequency band being used, high concentrations of RF energy occurring in that band can translate into possible interference for wireless devices. Different wireless technologies deal with interference in different ways. As a result, certain wireless "engines" that tolerate or suppress interference may be better suited for industrial applications that require robustness and reliability.

Spread Spectrum

License-free, wireless transmissions in the ISM bands require the use of one of the spread-spectrum technologies. "Spread spectrum" refers to a method of transmitting a signal by "spreading" it over a broad range of frequencies, one much wider than the minimum bandwidth needed to transmit. Spread-spectrum technologies offer many benefits:

- Increased transmission speed for faster throughput
- Ability to operate multiple networks in the same area for greater flexibility in system layout and expansion
- Minimized impact on performance from interference
- Reduced power consumption for battery or solar-powered installations

There are three wireless technologies that fall under the spread-spectrum umbrella. They are frequency-hopping spread spectrum (FHSS), direct-sequencing spread spectrum (DSSS) and orthogonal frequency division multiplexing (OFDM). Each technology offers advantages and limitations. FHSS sends data as it "hops" from one frequency to another and has the greatest tolerance for interference. The disadvantage to FHSS is low data rates. DHSS uses a "spreading and de-spreading" technique that offers higher data rates while suppressing interference, but not to the same degree as FHSS. OFDM offers the highest data rates but is much less tolerant of interference than FHSS and DSSS.

As with frequency, the wireless engine is specified by the wireless standard or determined by the manufacturer for proprietary devices.

Power Limitations

As noted, the FCC authorizes license-free transmissions in any of the three ISM bands using one of the three spread-spectrum technologies. The third restriction for unlicensed transmissions is power. Unlicensed radio transmitters are limited to one-watt power output. Additional limitations are placed on the gain of antenna systems; these vary according to the type of transmission. Some wireless standards may specify or recommend a power output below the FCC's one-watt requirement in order to reduce transmission distance, minimizing interference between systems in close proximity.

Public versus Proprietary

Wireless transmissions fall into one of two categories: public standard or proprietary system. A wireless public standard involves a governing body that creates a specification guaranteeing performance and interoperability between devices from different manufacturers. Interoperability gives consumers choices in product selection. A particular manufacturer's product may offer more features, benefits, or cost advantages than another's. Standards-based components can evolve, protecting investments in earlier technology, if backward compatibility is part of the standard. An example of a wireless standard is wireless Ethernet, or Wi-Fi.

The standards for wireless Ethernet were developed and are managed by the Institute of Electrical and Electronics Engineers (IEEE). The original standard was developed in the late 1990s and has evolved over time as technology and needs have changed. Public standards provide interoperability but also lead to concerns about security. With a public wireless standard, everyone knows the radio "language," and everyone has access to equipment that can receive and transmit signals. Therefore, sensitive information transmitted using a public standard must be protected. The primary means of protecting wireless data is through encryption.

Other than the standards recently developed for wireless sensor networks, there are no wireless standards developed specifically for industrial applications. However, there have been numerous proprietary wireless products in the market for many years, serving a wide range of industrial needs. With proprietary wireless systems, the manufacturer controls the design and determines which products work together and how they work together.

The word *proprietary* can have negative connotations; however, when considering wireless technology, it may be helpful to think of "proprietary" simply as referring to the application of available technology to meet a need where no public standard exists. Proprietary technology can provide a significant benefit in terms of security. Although the wireless engine and the frequency range for a wireless device may be known (e.g., FHSS, 900 MHz), it would be extremely difficult for an outsider to discover how that device works. Proprietary technology can provide a significant barrier to intrusion. Adding encryption further increases the difficulty of intercepting or manipulating a wireless transmission.

License-Free Wireless for Industry

The use of license-free wireless in industry has increased dramatically in the past few years. In addition to displacing licensed technology for some short- to medium-distance applications (several miles), many new uses for wireless have been discovered. Both standards-based and proprietary technologies are being used in a variety of applications.

There is no one wireless technology that satisfies all the needs of industry. As a result, numerous wireless technologies are being used in a variety of applications. There are five segments of license-free wireless used in industry. They are: unlicensed proprietary, 802.11 (Wi-Fi), Bluetooth, wireless sensor networks based on the IEEE 802.15.4 standard and cellular. Each wireless technology has its advantages and limitations.

License-Free Proprietary

License-free proprietary wireless already has a proven track record for reliable performance in industrial applications. Although product packaging and functionality vary widely between manufacturers, most of the products in this segment use FHSS and operate in the 900 MHz band. For maximum application flexibility, most proprietary wireless products use the full one watt available for license-free transmissions. This technology is well suited for use in applications such as wireless I/O (replacing wired connections between discrete and analog devices) or data radios (replacing wired serial connections between intelligent devices) for transmission distances from a few thousand feet to several miles. Depending on the manufacturer, system architecture can be point-to-point, point-to-multipoint or multipoint-to-point.

When end-to-end transmissions over long distances are not possible, the store-and-forward function is useful. With store-and-forward, data is sent to an intermediate device (repeater) that relays data to a final destination.

Some manufacturers offer unique proprietary products, such as a 900 MHz Ethernet radio. Data rates may be much lower than an 802.11 radio, and because it does not comply with IEEE 802.11 standards, it does not provide interoperability with other manufacturers' 802.11 radios. However, a one-watt, 900 MHz Ethernet radio transmits Ethernet data frames over the greatest distance possible without a license.

Wireless Ethernet

Ethernet is the worldwide standard for local area network (LAN) technology. It is not surprising that wireless Ethernet is widely used for wireless local area network (WLAN) technology. Although Ethernet communications can extend to the device level, the most common use for Wi-Fi in industry is for wireless networking. Ethernet has become an integral part of industrial control networks and is well suited for communications between personal computers, programmable logic controllers (PLCs), and a variety of other devices used in control systems. Wireless Ethernet extends the reach of wired networks to in-plant, near-plant and remote functions. Additionally, Ethernet has simplified the integration of control networks and business networks. Wireless can be useful when implementing other technologies used in the plant, such as radio frequency identification (RFID), voice over Internet protocol (VoIP) and wireless security devices.

Wi-Fi is based on the IEEE 802.11 standard that defines four sub-standards: 802.11a, b, g and n. Each sub-standard defines which ISM band and spread-spectrum technology to use. Table 2 lists the 802.11 standards and key attributes for each. IEEE established and maintains the standards that ensure products from different vendors are compatible. The Wi-Fi Alliance tests adherence to the standards and certifies that a product meets the standards. A product that is certified by the Wi-Fi Alliance can display the Wi-Fi logo. Each sub-standard has advantages and limitations.

	802.11a	802.11b	802.11g	802.11n
ISM Band	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz
Speed (theoretical)	54 Mbps	11 Mbps	54 Mbps	54/300 Mbps
Compatibility	802.11a	802.11b	Backward compatible to 802.11b	Backward compatible to 802.11a/b/g
SS Technology	OFDM	DSSS	OFDM, DSSS	OFDM

Table 2: IEEE 802.11 Standards

PHOENIX CONTACT
INSPIRING INNOVATIONS

Wireless Ethernet (*continued*)

802.11a operates in the 5.8 GHz band. It is unaffected by 2.4 GHz transmissions, so it can coexist with 2.4 GHz networks in the same area. An additional performance benefit for devices in the 5.8 GHz band is that it has eight non-overlapping channels, providing flexibility when operating multiple networks in an area. However, the higher frequency means more signal attenuation. As a general rule, 802.11a has not been widely deployed in industrial applications.

The 802.11b standard was the first to be widely deployed, but 802.11g became more commonly used due to the demand for higher data rates needed for network communications. A key advantage to 802.11g is that it is backward compatible to 802.11b. A limitation of 802.11g is a shorter transmission distance than 802.11b at the same frequency. Again, overlapping channels in the 2.4 GHz band may limit network layout for 802.11g.

802.11n is the latest standard to be ratified and offers key advantages over the previous 802.11 standards. 802.11n provides significantly higher data rates and greater range and can operate in both the 2.4 and 5.8 GHz bands. A key provision for 802.11n is backward compatibility with 802.11a/b/g, although there are performance limits when mixing devices on a network. Industrial-grade 802.11n components are now readily available and are being deployed to take advantage of higher bandwidths and increased range.

Regardless of the 802.11 standard used, it is important to note that Ethernet-based industrial protocols may not function as required on a wireless LAN as they do on a wired LAN. Consideration must be given to the suitability of a given industrial protocol for use over a wireless media. There may be limits on performance or specialized configurations required to ensure proper operation.

Ethernet radios can be used three ways: wireless access point (WAP), bridge and client. A WAP connects client devices to a wired Ethernet network via a wireless link. Client devices, such as laptops, use an internal wireless network interface card (NIC) to communicate with a WAP. If a client device such as a PLC does not have a NIC, an Ethernet radio in client mode provides the connection to a WAP. Some manufacturers may offer specialized functions for Wi-Fi radios, such as a bridge mode, which allows a number of radios to form a wireless mesh LAN. In bridge mode, an Ethernet radio communicates with other Ethernet radios that are in the same bridge network. Only the radios designated as part of a specific bridge network can communicate with one another, adding a degree of security. A WAP can be added if client devices are to have access to the bridge WLAN.

Wi-Fi Security

Because Wi-Fi is a public standard, the security and integrity of wireless transmissions are important concerns. There are a number of measures that can be taken to make transmissions secure, but encryption techniques are the most common. Wired Equivalent Privacy (WEP) was the first encryption technique but now can be compromised with limited know-how. Wi-Fi Protected Access (WPA) was introduced to improve upon WEP. WPA provides better security than WEP but still is vulnerable to attacks. Today, WPA2 provides the highest level of security for wireless Ethernet networks.

Bluetooth

Bluetooth is based on a public standard (IEEE 802.15.1) intended for short-range, low-power wireless transmissions. Originally conceived for connecting consumer electronics such as a wireless keyboard or mouse to a PC, Bluetooth is being used in industry for close-proximity, machine-to-machine (M2M) communications and other short-range wireless applications. Bluetooth is useful for replacing slip rings or festooned cables between a fixed component on a machine and a component that is moving or rotating. Also, replacing a serial cable with Bluetooth eliminates the tether for a wide range of intelligent devices used in an industrial facility.

The Bluetooth Special Interest Group (SIG) certifies that products meet the standard ensuring interoperability of products from different manufacturers. Bluetooth uses FHSS and operates in the 2.4 GHz band, the same as 802.11b/g. When channels become overloaded, the latest versions of Bluetooth use "adaptive frequency hopping" to remove overloaded channels from the hop sequence. This is one example of how wireless standards evolve to minimize interference between unlicensed technologies.

Bluetooth is considered a very-short-range wireless technology. The standard identifies three classes of devices based on transmission power and approximate range. Class 3 devices (1 mW max) have an approximate range of one meter, Class 2 devices (2.5 mW max) 10 meters and Class 1 devices (up to 100 mW max) 100 meters. However, some Bluetooth installations with line-of-sight can greatly exceed 100 meters.

Because most Bluetooth applications are very short range with limited data exchange, security may not be a critical concern. Regardless, as with any public standard, security is important. Bluetooth uses a number of techniques to ensure secure transmission of data. Password protection ensures that only devices with identical passwords can participate in the protected data communication. Additional security comes from controlling the pairing process to determine which products can communicate. Also, devices can be made "invisible," so other devices cannot discover them.

Wireless Sensor Networks

The IEEE 802.15.4 standard defines the fundamental provisions of a low-power, wireless, mesh network that is the basis for several wireless standards, including WirelessHART and ISA100.11a (part of the ISA100 family of standards for wireless). Unlike other wireless standards, WirelessHART and ISA100.11a were specifically developed for the industrial automation environment, where reliability, robustness and security are critical. Both are low-rate, low-power mesh networks operating in the 2.4 GHz band. Both employ FHSS and DSSS for communication between the nodes and the gateway that connect the Wireless Sensor Network (WSN) to the plant network or host system.

Although the two standards differ in scope and implementation, because they are based on IEEE 802.15.4, there are commonalities in their general application relating to wireless field devices and the establishment of a WSN. A WSN typically consists of nodes that are able to discover and communicate with neighboring nodes, forming a mesh network that communicates to a host system via a gateway. Although a star topology is possible, a mesh network allows devices to connect and reconnect in any number of ways. This creates multiple redundant paths that increase the reliability and range of the network. Another benefit of a mesh network is that nodes do not have to communicate directly with the gateway, only to nodes in close proximity. Shorter transmission distances translate into lower power requirements and enable the use of battery-powered field devices. Truly wireless devices can be relocated as needed or used as a portable device.

Although a mesh network has many advantages, there are limits in its application within an industrial process. As the mesh network increases in size so do the number of hops to get data from a node to the gateway. As the number of hops increases so does the latency of the system. This is not an issue when used for non-critical monitoring and control functions. A WSN can provide valuable information for asset management and process optimization that might have been difficult or impossible to obtain otherwise.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Wireless Sensor Networks (*continued*)

A WSN is best suited for the process industries, where there are many instruments in close proximity; however, because WirelessHART and ISA100.11a are true industrial wireless standards, both are expected to be widely deployed over time and further enhanced as the standards evolve. As a result, a more thorough understanding of performance and application considerations is warranted. For more information on the WirelessHART and ISA100 standards, visit www.hartcomm.org or www.isa.org/isa100, respectively.

Cellular Technology

Of all the wireless technologies available to the general public, none has had a greater impact than cellular. Cellular has empowered smartphone technology and provides instant global connectivity. Cellular is proving useful for industry as well, especially for the supervisory control and data acquisition (SCADA) industries, which often require communication with geographically dispersed assets. Traditionally, telemetry has relied on a variety of connection types for remote communications such as analog phone lines, wired network connections (DSL, cable, etc.) and wireless telemetry systems that can be costly and difficult to maintain. Users of cellular technology can leverage a highly capitalized wireless infrastructure, providing global connectivity that would be cost-prohibitive or impossible with traditional telemetry systems.

In industry, many applications are well suited for cellular technology, such as remote monitoring and control, data logging and M2M applications. Consideration must be given to the suitability of cellular for time-critical or mission-critical functions. Although cellular networks have very high uptime, when loss of communications would result in loss of critical functions, cellular may not be appropriate, unless it is the only means of communication.

It is hard to imagine anyone who doesn't already have a good understanding of cell phone technology, at least in terms of personal communications and mobile web access. Regardless, even experienced users can be confused by the cellular jargon commonly heard on TV commercials for cellular providers.

Since its inception, there have been several major advances in cellular technology, beginning with the second generation, or 2G, which was widely deployed in the 1990s, followed by 3G in the mid-2000s and now, 4G, which has been widely deployed throughout the U.S. It's important to note that the designation of a "generation" is a generic term that does not specify a particular technology. Generally, a new-generation implies a significant increase in data transmission rates without backward compatibility to the previous generation.

A generation label can represent multiple technologies. Common 2G technologies are Global Services for Mobile Communications (GSM) and Code Division Multiple Access (CDMA). GSM is the dominant cellular technology used globally; however, in the U.S. CDMA is as common as GSM, if not more so. Major providers in the United States that deploy GSM are AT&T and T-Mobile. Verizon is the major provider deploying CDMA.

Currently 2G, 3G and increasingly, 4G technologies are being used for SCADA and telemetry applications. The most common application is the transmission of process data between cellular modems via the cellular data network. Cellular also is enabling new options for monitoring and controlling remote assets. One example is cloud-based SCADA where data from remote sites is sent to web servers via the cellular network and accessed via the internet. Information can be easily accessed and operations monitored from any location with an internet connection. As noted previously, the benefits and risks of applying cellular in mission-critical applications must be fully considered to ensure cellular technology is used in an appropriate manner.

Cellular Technology (*continued*)

A very useful benefit of cellular is the ability to send alarm and status notifications to mobile devices such as smartphones. Short message service (SMS) messages, also known as text messages, provide a cost-effective and simple means of monitoring remote assets and alerting personnel of a problem. Timely notification of a situation requiring action can greatly minimize the potential impact of a problem on the process or on operations. Figure 2 illustrates how text messages could be used to monitor, and if appropriate, control plant processes.

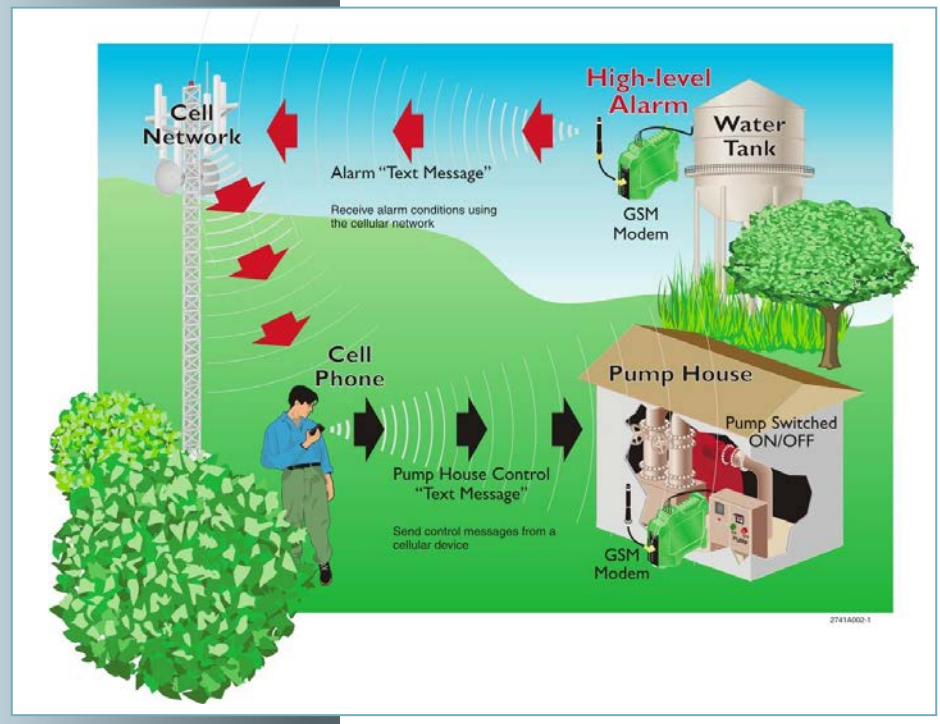


Figure 2: Alarm and status notifications sent to mobile devices alert operators to potential problems.

A major development with cellular technology is AT&T's 2012 announcement that it will shut down its 2G–GSM networks by early 2017 to free up spectrum for 4G technology. The process of reallocating spectrum has already begun and as a result, some markets have already lost 2G coverage. This process will continue until all of AT&T's 2G networks are shutdown in 2017. Additionally, T-Mobile is planning to "sunset" most of its 2G networks as well at some point in the near future. Shutting down the GSM networks will have little impact, if any, on consumers because most smartphones and mobile devices already use 3G or 4G technology. However, current users of GSM technology for M2M and SCADA applications will have to transition to newer technology which will have a significant impact on installed systems. Current users of GSM technology for industrial applications must assess their situation and plan accordingly.

A key issue with cellular is the recurring costs for monthly service. Depending on the provider, there are a variety of call plan options. Data plan charges are based on the amount of data sent each month. Unlimited text and data plans that may be available for mobile devices typically do not apply for SCADA applications. However, it is likely a major provider will offer plan options to utilities that would not be available to individual consumers. Further, adding to or expanding existing cellular data plans is a common option. Additionally, suppliers of industrial equipment containing cellular devices may offer their own plans as well as options for hosting data. It is recommended that a comprehensive review of cellular call plans be conducted before finalizing contracts for service to ensure the most economical use of cellular technology for SCADA and telemetry installations.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Relative Transmission Distances

Transmission differences are influenced by many factors and can vary greatly even for the same wireless technology due to differences in transmission paths, antenna systems and application performance requirements. Table 3 shows the relative transmission distances for the wireless technologies discussed in this paper.

Relative distances for typical applications		0' - 300"	1,000' - 3,000'	3,000' - 1 mile	1 - 2 miles	2 - 5 miles	5 - 8 miles	Around the world*
Max distance with line of sight (LOS)		1,000'	1 mile	2 miles	15 miles	20 miles	40 miles	*contingent on availability of cellular service
Minor obstructions		150'	500'	1,000'	1.5 miles	3 miles	7 miles	
Heavy obstructions		100'	250'	500'	1 mile	2 miles	5 miles	
Applications	Wireless Technology							
I/O to I/O	Bluetooth	■						
	900 MHz Proprietary	■	■	■	■	■		
I/O to BUS System	Bluetooth	■						
	WLAN (100 mW)	■	■					
	WLAN (400 mW)	■	■	■	■			
	900 MHz Proprietary - Serial	■	■	■	■	■		
	900 MHz Proprietary - Ethernet	■	■	■	■	■		
Low data rates < 9.6 kbps; e.g., PLC-to-PLC I/O collection	Bluetooth	■						
	WLAN (100 mW)	■	■					
	WLAN (400 mW)	■	■	■	■			
	900 MHz Proprietary - Serial	■	■	■	■	■		
	Licensed Proprietary	■	■	■	■	■	■	
	900 MHz Proprietary - Ethernet	■	■	■	■	■		
	Cellular (GSM/GPRS)	■	■	■	■	■	■	■
Medium data rates < 500 kbps; e.g., PLC-to-PLC communication and programming	Bluetooth	■						
	WLAN (100 mW)	■	■					
	WLAN (400 mW)	■	■	■	■			
	900 MHz Proprietary - Ethernet	■	■	■	■	■		
	Licensed Proprietary	■	■	■	■	■	■	
	Cellular (GSM/GPRS)	■	■	■	■	■	■	■
Heavy data rates < 54/300 Mbps* *802.11n theoretical data transmission; e.g., video surveillance	WLAN (100 mW)	■	■					
	WLAN (400 mW)	■	■	■	■			

Table 3: Relative transmission distances for license-free wireless technology.

Conclusion

Wireless has a well-established role in industry today, and its use will continue to grow in the coming years as wireless technologies find mainstream acceptance and standards intended for industrial applications are further developed and deployed. Understanding the advantages and limitations of the various wireless technologies will allow users to realize the benefits of wireless, while avoiding unnecessary costs and lost time resulting from its misapplication.

List of Acronyms

CDMA - Code Division Multiple Access

DSSS – Direct-Sequencing Spread Spectrum

EMI – Electromagnetic Interference

FCC – Federal Communications Commission

FHSS – Frequency-Hopping Spread Spectrum

GSM - Global Services for Mobile Communications

IEEE – Institute of Electrical and Electronics Engineers

I/O – Inputs/Outputs

ISA – International Society of Automation

ISM – Industrial, Scientific and Medical

LAN – Local Area Network

M2M – Machine-to-Machine

NIC - Network Interface Card

OFDM – Orthogonal Frequency Division Multiplexing

PLC – Programmable Logic Controller

RF – Radio Frequency

RFI – Radio Frequency Interference

RFID – Radio Frequency Identification

SCADA – Supervisory Control and Data Acquisition

SIG – Special Interest Group

SMS - Short Message Service

UHF – Ultra High Frequencies

VHF – Very High Frequencies

VoIP – Voice Over Internet Protocol

WAP – Wireless Access Point

WEP – Wired Equivalent Privacy

WLAN – Wireless Local Area Network

WPA – Wi-Fi Protected Access

WSN – Wireless Sensor Network