

# Remote Condition Monitoring Using Open-System Wireless Technologies

Jeffrey M. Rybak, Oceana Sensor Technologies, Inc., Virginia Beach, Virginia

Condition monitoring involves the use of sensors and data acquisition equipment to assess the quality of a given process by determining the health of its components. Machinery condition monitoring, which affords one the ability to implement condition-based maintenance (as opposed to time-based maintenance or run to failure) assesses the health of critical machinery components to reduce catastrophic process downtime and extend the useful life of machinery. The advent of robust, open-system, spread-spectrum radio technology has brought about the ability to reduce unplanned maintenance by continuously monitoring the condition of critical machinery and processes remotely and affordably via network and computer interfaces. This article looks at the value of continuous condition monitoring through remote data access and the means in which that data can be cost effectively transmitted wirelessly without compromising its integrity. It provides information on available wireless system technologies, addresses the suitability of various applications, and briefly describes product solutions commercially available today.

Rotating machinery is a vital part of virtually every manufacturing process. Motors, gearboxes, pumps, compressors, etc. are relied upon to operate efficiently to maintain a steady stream of production at maximum throughput. This dependency on machinery used in critical operations has prompted the evolution of machinery health monitoring. The lifespan of every piece of machinery is limited by the speed at which it is operating, the load to which it is subjected, the quality of its components, assembly and installation, its environment and the level of maintenance. While all of these factors are extremely important, it's the attention that's placed on the latter that will dictate how efficiently the machinery performs. It's the incorporation of intelligent maintenance practices, which predict impending failure of critical machinery components like bearings that prevent costly downtime, excessive overhead due to inventory and costly capital expenditures.

## Condition-Based Maintenance

Performing maintenance on a piece of machinery relative to its actual condition as opposed to how many hours it has been in service is referred to as condition-based maintenance, or CBM. This practice, which requires accurate machinery health monitoring techniques, allows machinery to operate to its maximum useful life without being subjected to premature component replacement or unplanned downtime. Machinery health monitoring utilizes sensors to monitor 'symptoms' associated with the degradation of rotating machinery. Some of these are temperature, vibration, oil condition, acoustic emission, pressure and electrical current. These parameters are typically gathered and analyzed by specialized "predictive maintenance" systems implemented by the end-user within the factory environment. The data are often gathered with portable data collection equipment by a technician who must physically walk from machine to machine. Vibration signals are obtained using a hand-held data collector and then compared to a vibration signature or baseline associated with that specific data collection point. Symptoms of impending bearing or gear failure due to pitting, fretting, spalling, hairline cracks, corrosion

and improper load often show up as extremely low-level signals across a broad range of frequencies. These indications can then be used to order replacement components in advance without holding excess inventory and to schedule corrective maintenance during off-peak production periods.

A permanent and continuous monitoring system offers several advantages over a periodic route-based collection system. First, by mounting sensors directly on the machinery, consistent and accurate results are provided for valid trending, analysis and decision support. Most importantly, alarm levels can be set so operators can be made aware of potential problems at early stages of development before a condition becomes critical. While data are more readily available in a continuous-monitoring/remote-data access system, which better assures that the data will actually be processed and used, traditional cabling is very expensive. This makes the solution cost prohibitive to most companies interested in monitoring a large number of points.

## Wired vs. Wireless

Cabling necessarily tethers equipment to fixed locations, reducing flexibility in equipment placement and reorganization. Cabling can also be very expensive to install and maintain in terms of both material and labor costs. New runs, moves or upgrades easily disrupt operations while cable is accommodated, and repositioning or upgrading equipment can necessitate completely new runs. Moreover, as the distance between equipment and control or monitoring devices increases, cable run length maximums are quickly exceeded.

Cable installation accounts for roughly two-thirds of the total cost of obtaining a channel of data in an industrial environment. At a modest rate of \$40/ft, a typical two-channel vibration monitoring system would cost more than \$13,000 just to run 100 meters of cable for remote alarm notification, analysis and trending.

Distance and cost limitations associated with wired links surface quickly on sprawling factory floors and in large industrial settings, and running cable to new or relocated equipment can interrupt production. These hard-wiring drawbacks have led many to seek a longer range and more flexible alternative in wireless networks. "Wireless Ethernet," for example, the general descriptor applied to wireless links within an Ethernet network, is any over-the-air connection between Ethernet network nodes or devices. As is often the case with new technology applications, there is a wide range of wireless network implementations on the market, and there is no single wireless standard.

## Wireless Technologies

Wireless network solutions typically fall into one of two classes of over-the-air protocols: those based on open-system standards (like IEEE 802.11 for WLANs and Bluetooth® for WPANs) and those based on proprietary protocols designed specifically for a given application.

The big difference between the two is cost. The ubiquitous nature of open system solutions lend themselves to economies of scale, offering the consumer a more cost-effective solution.

Open-system wireless data acquisition has greatly enabled the continuous monitoring of critical assets. Wireless systems are now available that reduce that \$13,000, two-channel installation noted earlier, to under \$2,000 – a savings of more than 80%. Wireless network deployment issues can be best under-

This article is based on a paper presented at the 59th Meeting of the Society for Machinery Failure Prevention Technology (MFPT), Virginia Beach, VA, April 2005.

stood if placed into the following three service classifications:

- Wireless wide-area networking (WWAN)
- Wireless local-area networking (WLAN)
- Wireless personal-area networking (WPAN)

WWANs use various devices – telephone lines, satellite dishes, and radio waves – to service an area broader than that covered by WLANs and WPANs, although typically with lower bandwidth. Bandwidth refers to the amount of data that can be transmitted in a fixed period of time, typically measured in bits of data per second, or ‘bps.’ WWANs are generally publicly shared data networks designed to provide coverage in metropolitan areas and along traffic corridors. WWANs are owned by a service provider or carrier, where data rates are low and charges are based upon usage. Specialized applications are characteristically designed around short, burst messaging. Examples of WWAN technologies are CDPD, ARDIS, GSM and GPRS, and WWAN technologies are often categorized into ‘generations’ 1G, 2G, 3G and 4G.

While a WWAN system may be practical for mobile phones, pagers, and even open-field sensor data acquisition, they are generally poor choices for industrial applications due to low bandwidth, spotty coverage, and the expense of service contracts. While satellite-based systems can be viewed as an augmentation to WWAN services, the cost value of service is often limited to specific applications, most notably those applications that benefit from one-direction broadcasting of content or communication to locations on the globe not serviced by other means. Bi-directional communication using satellites to support high-speed and/or pervasive connectivity is not a very practical approach. So, the major cellular systems are listed here as being most representative of WWAN technology.

- **GSM** (global system for mobile communications) – variations are used in Europe, Asia, and North America and operate in 900, 1800, and 1900 MHz bands with a typical maximum data rate of 14.4 Kbps.
- **GPRS** (general packet radio service) – digital mobile phone technology enhancement to GSM, providing data rates to 150+ Kbps. GSM and GPRS are considered rivals to CDMA technologies.
- **CDPD** (cellular digital packet data) – data transmission technology developed for use on the 800- to 900-MHz cellular phone frequencies to transmit data in packets at rates up to 19.2 Kbps. Low cost but slow.
- **CDMA** (code division multiple access) – transmission technology that accommodates multiple signals in the same channel (multiplexing). It uses direct-sequence spread spectrum technology to vary the transmission frequency according to a defined code pattern.
- **1xRTT** (1x radio transmission technology) – also known as CDMA2000, this technology increases data transmission rates over existing CDMA networks, providing 144 Kbps of data and voice.

## Wireless Networking

As stated earlier, wireless wide-area networks are not the best choice for continuous monitoring of industrial machinery and processes due to bandwidth limitations, spotty coverage and the monthly cost of service contracts.

The term wireless networking refers to technology that enables two or more computers to communicate using standard network protocols – but without network cabling. Strictly speaking, any technology that does this could be called wireless networking. But the current buzzword generally refers to wireless LANs. This technology, fuelled by the emergence of cross-vendor industry standards such as IEEE 802.11, has produced a number of affordable wireless solutions that are growing in popularity within business and education as well as sophisticated applications where network wiring is impossible, such as in warehousing or point-of-sale hand-held equipment. WLAN systems are designed to supplement and in some cases replace traditional wired-based LANs. The predominant stan-

dards-based WLAN technology being deployed in the United States is based on the IEEE 802.11b standard.

In a basic 802.3 Ethernet LAN, Cat 5 cable connects LAN stations to a hub. In a wireless LAN, Cat 5 cable is replaced by a radio channel, connecting stations to wireless access points (APs). Each wireless station – laptop, desktop, or server – has a radio network interface card (NIC). APs are essentially hubs, outfitted with a radio transceiver, Ethernet uplink, and 802.1d bridging software. Wireless stations transmit to an AP over a shared channel, carved out of the unlicensed 2.4 GHz band. There are two types of wireless networks. An ad-hoc, or peer-to-peer wireless network consists of a number of computers equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless-enabled computers. They can share files and printers this way but may not be able to access wired LAN resources unless one of the computers acts as a bridge to the wired LAN using special software (this is called ‘bridging’).

A wireless network can also use an access point, or base station. In this type of network, the access point acts like a hub, providing connectivity for the wireless computers. It can connect, or ‘bridge,’ the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet connectivity.

There are two types of access points:

- Dedicated hardware access points (HAPs) offer comprehensive support of most wireless features.
- Software access points, which run on a computer equipped with a wireless network interface card as used in an ad-hoc or peer-to-peer wireless network.

Approved in 1997, the original IEEE 802.11 standard uses the 2.4-GHz band to provide shared bandwidth at a maximum rate of 1 to 2 Mbps. In 1999, the IEEE approved the 802.11b high-rate (Wi-Fi) amendment, increasing the rate to 11 Mbps. Together, these standards specify WLAN physical (PHY), media access control (MAC), and logical link control (LLC) layers for fixed wireless broadband access and WLANs.

**802.11** is an IEEE standard for wireless local area networks (WLANs) that covers the wireless LAN media access control (MAC) and physical layer specification. 802.11b and 802.11a are extensions of this standard, also referred to as Wi-Fi (wireless fidelity), which is an interoperability certification.

**802.11b** is a well-accepted standard for WLANs optimized for the unlicensed 2.4-GHz band, with speeds up to 11 Mbps when using DSSS.

**802.11a** is a standard that improves upon 802.11b, with support for speeds up to 54 Mbps in the less-crowded 5-GHz band by using OFDM (orthogonal frequency division multiplexing) which splits a high-speed signal into a number of low-speed signals transmitted in parallel, more efficiently using bandwidth but decreasing wireless range.

**802.11g** is a WLAN standard comparable to 802.11a (uses OFDM for speeds up to 54 Mbps) but operates in the 2.4-GHz spectrum.

## Personal Networks

WPAN systems have evolved from ‘cord’ replacement technologies. Some examples are: cordless communication between your keyboard and computer, cordless communication between your personal digital assistant (PDA) and your computer and cordless communication within your home between your cell phone and your home phone.

Because of their initial function focus, WPAN wireless implementations to date have been low powered and offer limited coverage range. The most hyped of all WPAN wireless technologies today is called ‘Bluetooth,’ which got its unusual name in honor of Harald Bluetooth, king of Denmark in the mid-tenth century. Bluetooth is a product of the telecommunications and computer industry “Bluetooth SIG” and is rapidly gaining wide acceptance throughout the industry. Bluetooth is a telecommunications industry specification that describes how mobile phones, computers, and PDAs can be easily interconnected

using a short-range wireless connection. Using this technology, users of cellular phones, pagers, and personal digital assistants can buy a three-in-one phone that can double as a portable phone at home or in the office, get quickly synchronized with information in a desktop or notebook computer, initiate the sending or receiving of a fax, initiate a print-out, and, in general, have all mobile and fixed computer devices be totally coordinated.

Bluetooth requires that a low-cost transceiver chip be included in each device. The transceiver transmits and receives in a previously unused frequency band of 2.45 GHz that is available globally (with some variation of bandwidth in different countries). In addition to data, up to three voice channels are available, and each device has a unique 48-bit address from the IEEE 802.15 standard. Connections can be point-to-point or multipoint and can lock out other devices selectively, preventing needless interference or unauthorized access to information. The maximum range is typically 10 meters for battery-powered devices, as transmission distance is directly linked to power consumption, and data can be exchanged at a rate of 1 megabit per second (up to 2 Mbps in the second generation of the technology). A frequency-hopping scheme allows devices to communicate even in areas with a great deal of electromagnetic interference, and built-in encryption and verification are provided for security.

There are three classes of Bluetooth radio: Class 1 – 100 meters, Class 2 – 15 meters, Class 3 – 10 meters. The lowest power radio within the network defines the maximum transmission distance allowed.

WLAN and WPAN systems, i.e. IEEE802.11 (otherwise referred to as Wi-Fi or wireless Ethernet) and IEEE802.15.1 (otherwise known as Bluetooth), both utilize spread-spectrum technologies for battling interference and noise, but there are differences in the manner that these two systems attack the problem. Bluetooth uses a frequency-hopping method, while Wi-Fi uses a direct-sequencing method. The proper choice of direct sequence or frequency hopping as a spread-spectrum technique depends on the environment where the system will be deployed. If there are narrow-band interferers of moderate level, then a DSSS system that will completely reject them may be desirable. Should there be any large interfering signals, then a DSSS link may completely fail, while FHSS (frequency hopping, spread spectrum) is likely to continue operating, even though the interference is not completely rejected.

**Direct Sequence (DSSS).** Designed originally by two vendors to increase the available speed on the wireless network. Divides the available 83.5 MHz spectrum (in most countries) into three wide-band 22-MHz channels. It uses an 11-bit spreading code to reduce the possible interference on signals in each wide-band channel. (Figure 1a)

**Frequency Hopping, Spread Spectrum (FHSS).** Derived from military radio technology, where it was designed to be inherently secure and reliable under adverse battle conditions. It divides the available 83.5-MHz spectrum (in most countries) into 79 (or 75) discrete 1-MHz channels (the 4.5 MHz left over provides “guard bands” at either end of the spectrum). The radio then hops around these 1-MHz channels in a “pseudo-random” sequence using a minimum of 75 frequencies every 30 seconds and using any single frequency for a maximum of 400 milliseconds. (Figure 1b)

Wireless communications obviously provide potential security issues, because an intruder does not need physical access to the traditional wired network to gain access to data communications. However, 802.11 wireless communications cannot be received – much less decoded – by simple scanners, short-wave receivers etc. This has led to the common misconception that wireless communications cannot be eavesdropped at all. However, eavesdropping is possible using highly specialized equipment. Note that the traditional virtual private networking (VPN) techniques would work over wireless networks in the same way as traditional wired networks, but additional security measures are rapidly evolving to reduce the threat of

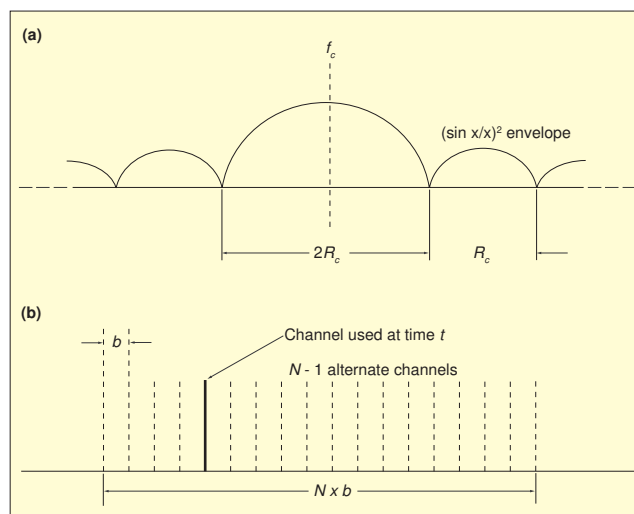


Figure 1. Direct Sequence Spread Spectrum (DSSS) (a) and Frequency Hopping Spread Spectrum (FHSS) (b) schematics.

eavesdropping and data theft.

Bluetooth security utilizes 128-bit encryption, authentication, and authorization schemes. Flaws in security found on mobile phones have undergone software modifications to improve the level of protection from hackers. 802.11 wireless communications initially addressed security in much the same way via a function called WEP (wired equivalent privacy), a form of encryption that provides privacy comparable to that of a traditional wired network. If the wireless network had information that should be secure, then WEP should be used, ensuring the data are protected at traditional wired network levels. In addition to 128-bit encryption, the WEP key also provided authentication when a new client accessed the network. (PROBLEM) The key management structure had two likely outcomes: When WEP was used, keys were rarely updated, leaving the network vulnerable to break-in, and WEP itself was rarely used. Needless to say, neither outcome was desirable from a security standpoint, so the 802.11 committee had formed its ‘i’ subcommittee to explore the problems with and correct the WEP protocol. WPA2 is the second generation of WPA security; providing enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard and is now eligible for FIPS 140-2 compliance.

### Machinery Monitoring Guidelines

So, which system is best suited for continuous monitoring of sensor data in an industrial environment? Bandwidth-rich Wi-Fi, utilizing direct, sequence-spread spectrum, which has some limitations in noisy, interference-ridden environments, or bandwidth-sufficient Bluetooth, utilizing frequency-hopping, spread-spectrum technology, which is very robust and noise immune? In reality, they both have earned their places within a corporate or industrial setting. Many existing infrastructures are suitable for wireless Ethernet interface to sensor data, where the environment may also not be too hostile for Wi-Fi’s direct-sequencing, spread-spectrum limitations. Where the environment is more appropriate for a noise-immune, frequency-hopping, spread-spectrum system, Bluetooth could be used in conjunction with Wi-Fi.

While Bluetooth and wireless LAN were earlier labeled as competing technologies, manufacturers have discovered over time that this is not necessarily the case. Some have even gone so far as to develop products that feature both technologies, such as wireless access points. There is now widespread market acceptance of both Bluetooth and WLAN, which has led to a greater incidence of coexistence between the two, most commonly in computer network environments. But coexistence in the unlicensed 2.4-GHz band comes with a price. Unlicensed



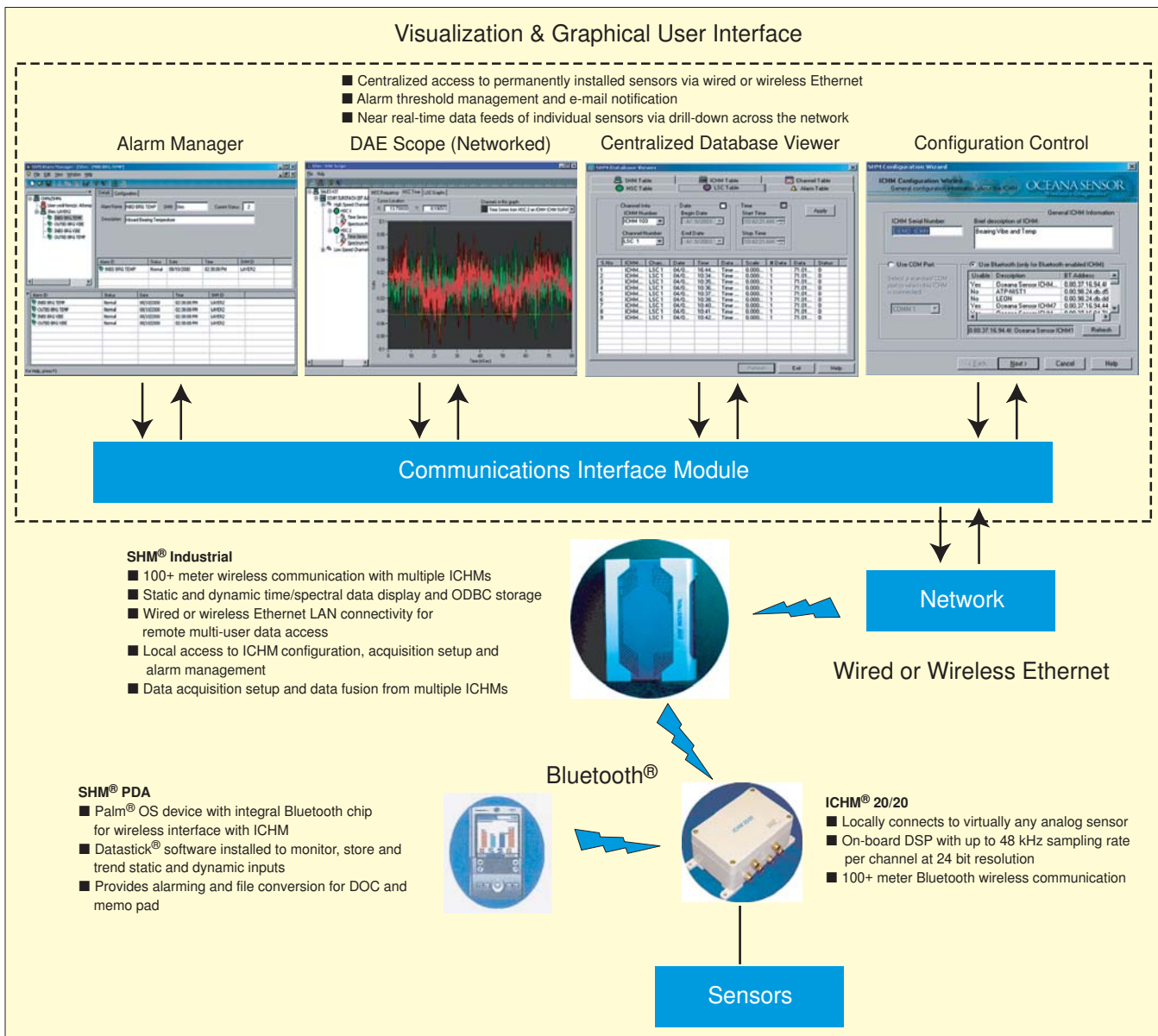


Figure 2. Oceana Sensor Technologies Central Workstation™, PC-based remote sensor interface.

means that competing, or complementary, technologies are free to operate in this frequency band, giving rise to interference that impinges on the quality of communication. To most users, deterioration of quality may be more apparent in voice-centric applications than in data-centric applications. For example, one is more likely to be aware of poor sound quality while using a Bluetooth headset than of the extent to which data packets must be retransmitted between one's notebook PC and a network access point. The Bluetooth industry, through the Bluetooth SIG, has responded by taking measures to reduce interference in environments where multiple wireless technologies coexist.

Version 1.2 of the Bluetooth specification, adopted in 2003, includes adaptive frequency hopping (AFH), a technique proven to be an effective remedy to the problem of interference in WLAN and similar environments.

This technique can be implemented through various methods, each with its own inherent set of advantages and drawbacks. Ericsson, a leader in the field of Bluetooth wireless technology, uses a method well suited for its broad-based Bluetooth design solution sold as intellectual property (IP). Ericsson's implementation of AFH is further enhanced through the use of other standard and proprietary techniques, providing excellent audio quality for voice-centric applications in the presence of multiple wireless technologies.

Note that there are proprietary systems that battle noise and interference problems with proprietary radio solutions. While these systems may solve an immediate application requirement, proprietary solutions will always be more costly than those adopting open-system standards. Vendors ensure considerable repeat business by locking customers into their proprietary systems, which don't allow for interface to cost-competitive, open-system, standard, third-party, hardware and application software.

### Commercially Available Wireless Systems

As for commercially available wireless data acquisition systems, there are several that incorporate proprietary technology, yet very few that use open standards. But, a wireless sensing system offered by Oceana Sensor Technologies (Figure 2) is suitable for industrial applications, employing both open-system Bluetooth and Wi-Fi technology.

The system is based upon the ICHM® 20/20 programmable, wireless data acquisition platform and processing module with on-board diagnostics. The ICHM's digital signal processor executes complex algorithms, Fourier analysis, digital filtering, band-level comparisons, and advanced math calculations and is capable of functioning autonomously and communicating reliably in industrial environments through the use of Bluetooth, 'spread-spectrum technology. Each module is



Figure 3. ICHM<sup>®</sup> 20/20 programmable wireless data acquisition module.

equipped with as many as two dynamic channels (48 kHz sampling per channel at 24-bit resolution) and four static channels (DC to 3 Hz at 12-bit resolution) for local interface to a variety of analog sensors. The ICHM<sup>®</sup> 20/20 is available with a Class 1, 20 dBm (100-meter range) Bluetooth radio system or serial output to interface with other wireless systems, including Wi-Fi.

The ICHM<sup>®</sup> 20/20 (Figure 3) offers remote process and condition monitoring without the enormous expense of running cable and conduit. It is built on open-system architecture for lower installation and life cycle-costs and provides localized health monitoring at the component level. The ICHM 20/20 is a low-power, noise-immune device that incorporates FHSS technology and transmits data continuously or only when needed. ICHMs can communicate directly to Bluetooth-equipped PDAs and PCs, including the system health monitor (SHM<sup>®</sup>) industrial PC for 100+ meter Bluetooth interface to multiple ICHMs.

The SHM industrial is a LAN access point for wired or wireless Ethernet connection to a network gateway that contains logic software for periodically acquiring data from multiple ICHMs. It's ODBC (Open DataBase Connectivity) compliant database provides necessary data for local monitoring or LAN-based access with Central Workstation<sup>™</sup> and third-party software systems.

While Bluetooth offers a robust yet cost effective wireless interface between a multitude of sensors and the SHM industrial, wireless Ethernet can be used for even longer-range communication between stored data and the user. Central Workstation provides LAN-based access to data and features

inherent to the SHM industrial, including alarm monitoring and management, waveform analysis, and a sensor setup function, which allows independent configuration of all static and dynamic inputs.

Alarms are observed as a red/yellow/green status indication, and individual alarm histories can be obtained for historical trending and reporting purposes.

Time-stamped data is stored in Microsoft Access ODBC format for viewing at any time.

### Future Developments

Issues that continue to drive technology forward are:


- Size – self-contained, miniature wireless sensors.
- Power – power-scavenging features for extracting power from the environment.
- OEM integration – incorporation of wireless, remote monitoring systems into machinery at the point of manufacture.
- Open-system architecture – interoperability among system components and data-handling applications.

As for the future of wireless networking standards:

- 802.11e is being developed to help wireless LANs handle interference – by moving away from it – and to provide better support for those big streaming multimedia files by using error correction and better bandwidth management.
- The IEEE P802.15.3 high-rate (HR) task group (TG3) for wireless personal area networks (WPANs) is chartered to draft and publish a new standard for high-rate (20 Mbits or greater) WPANs. Besides a high data rate, the new standard will provide for low-power, low-cost solutions addressing the needs of portable consumer digital imaging applications.
- Zigbee is a standard for wireless personal area networking designed to be simpler and cheaper than other WPANs such as Bluetooth and is aimed at applications with low data rates and low power consumption. It operates in the unlicensed 2.4-GHz, 915-MHz, and 868-MHz bands. The data rate is 20 Kbps per channel, and the transmission range is between 10 meters and 75 meters.
- WiMAX is a marketing name bestowed on a new technology standard that adheres to a certain derivation of the IEEE 802.16 standard, provides wireless broadband Internet connections at speeds similar to Wi-Fi but over distances of up to 30 miles from a central tower.

Once again, open system architecture is at the core of universal acceptance and the economies of scale that offer cost effective industrial wireless solutions.

### Bibliography

1. <http://www.bluetooth.com>
2. <http://www.ieee.org>
3. Erik Strom, Tony Ottosson, Arne Svensson, *An Introduction to Spread Spectrum Systems*, 2002.
4. F. L. Lewis, *Wireless Sensor Networks*, 2004.
5. Earl McCune, *DSSS vs. FHSS Narrowband Interference Performance Issues*, 2004. 

The author can be contacted at: [jrybak@oceanasensor.com](mailto:jrybak@oceanasensor.com).