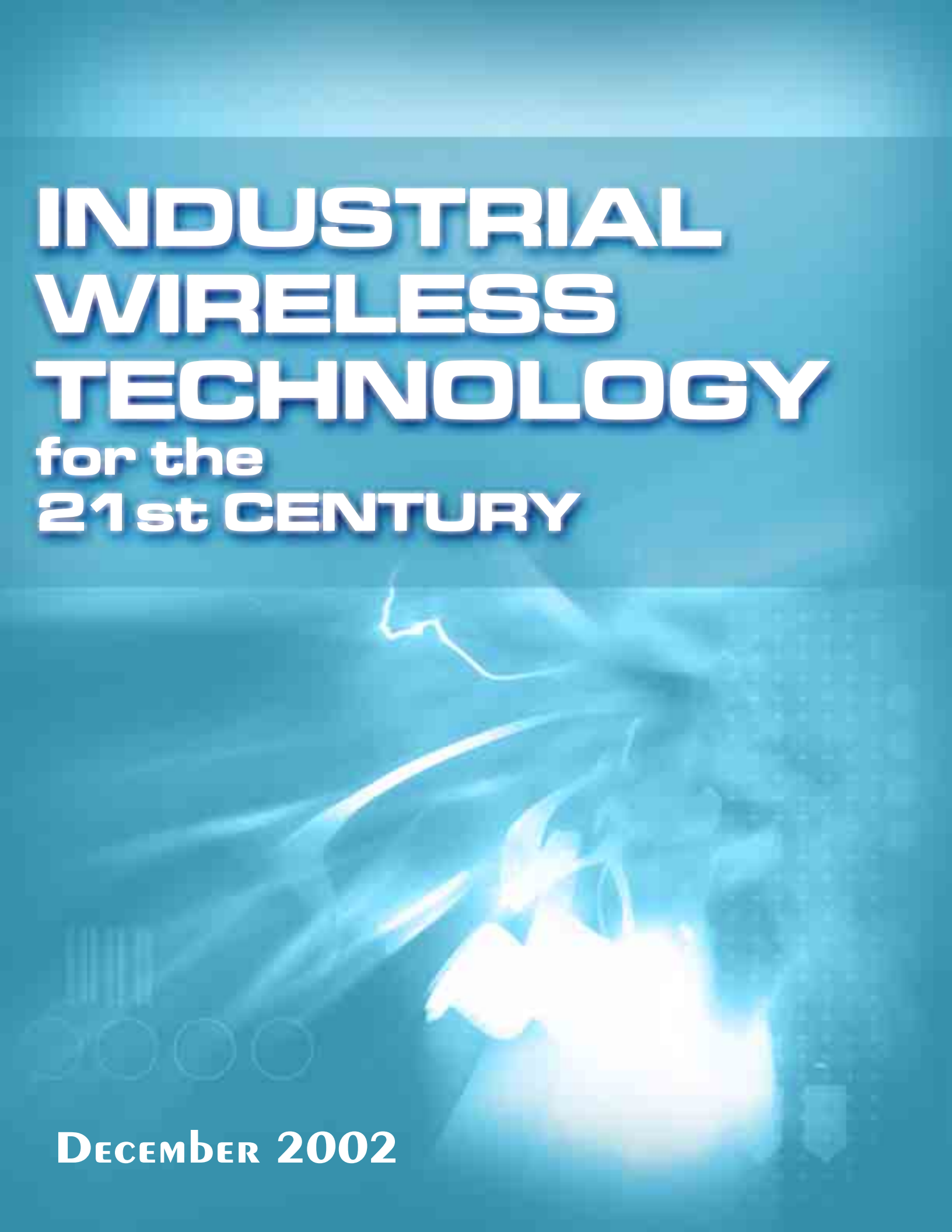
# INDUSTRIAL WIRELESS TECHNOLOGY for the 21st CENTURY



December 2002

# Industrial Wireless Technology
## for the 21st Century

December 2002

Based on the views of the

Industrial wireless community

In collaboration with the

U.S. Department of Energy
Office of Energy Efficiency and Renewable Energy

# Foreword

Wireless sensor systems hold the potential to help U.S. industry use energy and materials more efficiently, lower production costs, and increase productivity. Although wireless technology has taken a major leap forward with the boom in wireless personal communications, applications to industrial sensor systems must meet some distinctly different challenges. Some of the technology development needed to expand industrial applications and markets will require coordinated efforts in multiple disciplines and would benefit from a clear identification of industrial requirements and goals.

In July 2002, the U.S. Department of Energy's Industrial Technologies Program sponsored the Industrial Wireless Workshop as a forum for articulating some long-term goals that may help guide the development of industrial wireless sensor systems. Over 30 individuals, representing manufacturers and suppliers, end users, universities, and national laboratories, attended the workshop in San Francisco and participated in a series of facilitated sessions.

The workshop participants cooperatively developed a unified vision for the future and defined specific goals and challenges. This document presents the results of the workshop as well as some context for non-experts. Discussions of today's technology are intended to serve as a rough baseline for decision makers and government funding agencies; descriptions necessarily represent a "snapshot" in time as new developments emerge almost daily. Energetics, Inc. of Columbia, Maryland, facilitated the workshop and prepared this summary of the proceedings. Wayne Manges of Oak Ridge National Laboratory and Dr. Peter Fuhr of San Jose State University provided valuable technical information and advice. 3e Technologies International and L3/Celerity sponsored a reception for the participants prior to the workshop.

Special thanks go to the workshop participants who kindly contributed their time and expertise to make this document possible. These individuals and the companies or organizations they represent are listed on the following page.

## Industrial Wireless Workshop Participants
### San Francisco, California
### July 30, 2002

William Burke
ChevronTexaco

Steven Chen
3eTI

John Coates
Coates Consulting

Chris Davis
Konarka
Technologies, Inc.

Donald Doan
TXU Energy

Peter Fuhr
San Jose State
University

Jeff Griffin
Pacific Northwest
National Laboratory

Leslie Hamilton
3e Technologies
International,
Incorporated

William Harms
Spirax Sarco,
Incorporated

Gerard Hill
Axonn

Ron Hofmann
RHC

Kurt Kelty
Panasonic
Technologies

Thomas Kevan
Advanstar
Communications

Pramod Kulkarni
California Energy
Commission

Ron Kyker
Sandia National
Laboratory

Kang Lee
National Institutes of
Standards and
Technology

Wayne Manges
Oak Ridge National
Laboratory

Daniel Maxwell
Walden Technology
Source, Incorporated

Rick Nozel
Microwave Data
Systems

Sanjay Parthasarathy
Honeywell

Robert Poor
Ember Corporation

Mark Prichard
Celerity, L3
Communications

Debbie Reid
Celerity, L3
Communications

E. Tom Rosenbury
Lawrence Livermore
National Laboratory

Richard Sanders
ExxonMobil Research
and Engineering

Ake Severinson
Omnex Control
Systems, Incorporated

Daniel Sexton
General Electric

Ramesh Shankar
Electrical Power
Research Institute

David Shepherd
Strategic Analysis,
Incorporated

Stephen Smith
Oak Ridge National
Laboratory

Denise Swink
U.S. Department of
Energy

James Taylor
Venture Development
Corporation

Moira Young
Microwave Data
Systems

Bary Wilson
Pacific Northwest
National Laboratory

# Contents

1. Why Wireless? ..... 1

2. Wireless Today ..... 5

3. The Future of Wireless ..... 13

4. Challenges ..... 19

Appendices

A. Results of Facilitated Sessions

B. Presentations

# Why Wireless?

## *Revolutionary Potential*

In today's industrial environment, systems and equipment must perform at levels thought impossible a decade ago. Global competition is forcing U.S. industry to continuously improve process operations, product quality, and productivity with fewer people than ever before. Production equipment must deliver unprecedented levels of reliability, availability, and maintainability as plant managers seek ways to reduce operational and support costs and to eliminate or minimize capital investments. In short, industry must invoke new measures to improve production performance and safety while minimizing costs and extending the operational life of new and aging equipment.[1]

**The New Industrial Paradigm**

- Improved product quality
- Minimized capital costs
- Extended equipment life
- Streamlined operations
- Lower operating costs
- Increased equipment availability

Wireless sensor systems can revolutionize industrial processing and help industry meet the demands of increased competitiveness. Intelligent wireless sensors built for ubiquitous use in industrial environments will enable real-time data sharing throughout a facility to increase industrial efficiency and productivity. Wireless sensor technology offers reliable, autonomous process control to improve product quality, increase yield, and reduce costs. In 1997, the President's advisers on science and technology asserted that the development of wireless sensors could improve production efficiency by 10 percent and reduce emissions by more than 25 percent.[2]

**What's Wrong with Wires?**

- High installation costs
- High maintenance costs
- Constantly increasing costs
- High failure rate of connectors
- Difficulty in troubleshooting connectors

### Wireless Systems Provide a Competitive Edge

By using electromagnetic waves as their transmission medium, wireless systems avoid the limitations of wired networks and offer competitive advantages in terms of cost, flexibility, and ease of use. Forward-thinking companies are looking beyond mere replacement of existing wired networks to comprehend the greater potential and envision completely new capabilities offered by industrial wireless

sensor systems. According to Forrester Research in Cambridge, Massachusetts, some 15 percent of industrial companies now have wireless networks in their plants, up from 6 percent a year ago.[3]

**Why Wireless?**

- Lower installation and maintenance costs
- Ease of replacement and upgrading
- Reduced connector failure
- Greater physical mobility and freedom
- Practical deployment of micro-electromechanical systems (MEMS) technology
- Faster commissioning

***Lower Costs.*** The costs associated with installing, maintaining, troubleshooting, and upgrading wiring have escalated while costs for wireless technology have continued to drop, particularly in the areas of installation and maintenance.[4] A market study by the Venture Development Corporation found that users of wireless technology cite lower cost as a major reason for adoption. Most non-users who cited cost as a deterrent focused solely on comparative hardware and software costs, neglecting the savings discovered in full cost analyses.[5]

*Installation.* Wireless systems could ultimately eliminate tens of thousands of feet of wiring from the average industrial site. Such wiring can cost $50 to $100 per foot including labor. Specialized wiring for harsh environments can cost as much as $2,000 per foot.

*Maintenance*. As wires age, they can crack or fail. Inspecting, testing, troubleshooting, repairing, and replacing wires require time, labor, and materials. If wiring faults cause a production stoppage, costs escalate rapidly. Wireless systems obviate any costs associated with running new wires and eliminate associated downtime.

***Reduced Connector Failure***. Most failures in any network occur at the connectors; wireless sensors eliminate this problem.

***Improved Flexibility.*** Without the constraint of wires, plant managers can better track materials and more easily reconfigure assembly lines to meet changing customer demands. Freedom from wires also allows greater flexibility in sensor placement—particularly in the case of mobile equipment (e.g., cranes and ladles).

***Exploitation of MEMS.*** Micro-electromechanical systems (MEMS) offer a rapidly expanding wealth of sensing capabilities. Integrated wireless sensors with built-in communications capabilities can avoid the failure modes introduced by attaching bulky wires to these miniature devices. This advantage will increase in significance as sensors continue to shrink.

***Rapid Commissioning***. Simple wireless sensor systems can rapidly organize and configure themselves into an effective communications network. Self-calibration and verification are on the horizon, opening the possibility of deploying ad hoc systems to explore a range of production scenarios.

## Wireless Systems Create Value

Significant technological advances exist at bench-scale in labs across the country. These technologies need to be brought forward and integrated with other emerging technologies to realize the full potential of wireless systems. As these systems move into wider use, industrial end-users will gain greater flexibility and discover new possibilities. Low-cost, high-performance, easily deployed wireless devices will change the way end-users view sensors and sensor systems.

***Reliability.*** Some industrial applications require absolute reliability in systems control to avoid serious consequences such as injury, explosions, and material losses. Emerging wireless sensor systems can offer built-in redundancy and capabilities for anticipatory system maintenance and failure recovery. Demonstration of reliability will pave the way for deployment in these applications.

***Ease of Use.*** Integrated wireless sensor systems with distributed intelligence can enable operator-independent control of industrial processes. Sensor nodes can dynamically adapt to and compensate for device failure or degradation, manage movement of sensor nodes, and react to changes in task and network requirements. They can locate themselves in 3-D space and correlate their positions with on-line plant maps to assure correct placement. Continuous, high-resolution, ubiquitous sensing systems have the potential to autonomously monitor and control industrial processes. Based on the application, such systems will be capable of maximizing product quality and yield while minimizing waste, emissions, and cost.

***Security.*** Manufacturers and industrial companies have become increasingly concerned about threats of industrial espionage and cyberterrorism. New strategies for encrypting and even hiding wireless data transmissions promise a level of security that equals or surpasses that of wired systems. Upgradeability is essential to maintain security as technologies evolve and new threats emerge.

***Robust Design.*** Recent advances in materials technology should enable integrated wireless sensor systems to meet durability and reliability requirements in harsh industrial environments. Integrated sensor nodes encased in advanced materials should be able to endure repeated exposure to caustic gases and high temperatures. Some applications may require components designed to withstand highly specific environmental challenges.

***Open Architecture.*** With the wide range of potential applications and broad diversity of physical devices, the software components will need to be highly modular and efficient. A generic development architecture should allow specialized applications from a wide spectrum of devices without requiring cumbersome interfaces. This will also enable connection to existing sensors and easy upgrades to incorporate more advanced modules in the future.

## The Time Is Right

Advances in a number of technologies at the beginning of the 21st century are collectively paving the way for the growth of wireless industrial sensor systems. The phenomenal explosion of the personal communications market has dramatically reduced costs and increased the quality of the underlying radio components and technologies. Continued reductions in the costs of computational capabilities also support a distributed architecture for these systems. Embedded intelligence reduces the bandwidth requirements for communications and lowers power requirements—both critical issues for wireless sensors. The technology will also benefit from continuing progress in sophisticated modulation techniques, emerging standards, miniaturization of sensors, and enhanced system reliability and robustness.

Integrated wireless sensor systems promise exciting prospects for U.S. manufacturing and industrial competitiveness. In line with the increasingly interdisciplinary nature of technology, many of the advances described in this document both build on and apply toward the development of sensors, controls, and communications systems in other application areas, such as automobile assembly, building management, power generation, and transportation systems. Continued technology development and the use of a collaborative, multidisciplinary approach to solving common challenges in a cooperative environment can signal a new era in productivity.

---

[1] Manges, W. W., Allgood, G. O., and Smith, S. F. (May 1999). It's time for sensors to go wireless; Part 2: Take a good technology and make it an economic success, *Sensors: The Journal of Applied Sensing Technology* 16(5), 70-80.

[2] President's Committee of Advisors on Science and Technology, Energy Research and Development Panel (November 1997). Federal energy research and development for the challenges of the 21st century, 3-16.

[3] Koudsi, S. and Bylinsky, G (June 24, 2002). Hot technologies, *Fortune*. Retrieved October 29, 2002, from http://www.fortune.com/indext.jhtml?channel=print_article.jhtml&doc_id=208250

[4] Manges, W.W., Allgood, G. O., and Smith, S. F. (April 1999). It's time for sensors to go wireless; Part 1: Technological underpinnings, *Sensors: The Journal of Applied Sensing Technology*, 16(4), 10-20.

[5] Venture Development Corporation (2002). *The North American market for wireless monitoring & control in discrete and process manufacturing applications.*

# Wireless Today:

## *Orientation in Wireless Technology*

To gain a competitive advantage, many industrial companies are demanding greater amounts of information, faster methods of processing it, and the means to distribute it to more locations. They seek more devices to collect better information on the physical world, assess its meaning, and communicate it—often over longer distances. Increasingly, industry is turning to systems composed of distributed intelligent devices that communicate via digitized data streams. These systems can move the human-machine interface, monitoring, and control functions closer to the production process, enhancing performance while reducing wiring and cable costs.

Wireless sensor technology is now moving rapidly into niche applications in plants and other industrial environments where it can deliver cost advantages and increase flexibility. The cost factor is critical; industry will invest in these systems only if the resulting performance improvements exceed the cost to communicate. Wiring and cable have traditionally dominated the cost of industrial communications, but a new dynamic is now in effect—high-speed, license-free, low-cost wireless devices have dramatically altered the equation.

Industrial wireless systems must transmit information over distances that can range from six inches to fifty miles, depending upon the application. Not surprisingly, distance exerts a strong influence on the choice of communications technology. Key industrial wireless markets can be grouped into the following three areas according to their typical distance requirements (from shortest to longest): factory automation, process automation, and supervisory control and data acquisition (SCADA) or telemetry.

Most of the industrial applications currently in use perform monitoring rather than control due to remaining security and performance issues.[1] Improvements in these areas will greatly expand monitoring and control applications throughout U.S. industry. Hurdles to wider use of wireless systems currently include a range of limitations imposed by both the industrial environment and the state of the technology. Industrial end-users must feel confident in the solutions to these issues before they will entrust control functionality to a wireless system supporting mission-critical industrial system requirements.

## Interoperability

A key issue currently limiting wireless deployment in industry involves compatibility among wireless components from different suppliers, generally referred to as *interoperability*. Some industrial end-users are wary of becoming locked into a proprietary system that might later hinder system upgrades as technology advances. Full compatibility among components would also provide end users with the flexibility to connect highly specialized, high-end sensors with best-in-class wireless interface devices.

**What Is Interoperability?**

State achieved when software and hardware (from any source) work together without user attention (true "plug & play") and without interfering with each other.

The issue becomes how to guide the development of interoperability in the least restrictive manner to encourage creative and unbound solutions. As a framework, the International Standards Organization (ISO) has developed a network model composed of seven different levels or layers. By standardizing these layers and the interfaces between them, portions of communications protocols can be adjusted as needed to accommodate new technologies or altered system requirements.[2] The seven layers are as follows:

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data link
1. Physical

Attainment of the long-sought goal of interoperability will depend upon how wireless suppliers implement interfaces among the seven layers of the ISO model. Numerous standards now exist or are under development to promote the compatibility of these interfaces.

## Standards

The move toward networking of industrial wireless applications is relatively recent. Most of the millions of wireless devices currently used in industrial applications are neither networked nor standards-based. Instead, they pass digitized data transparently and are either FCC-licensed solutions or solutions using the license-free bands.

Today's networking standards typically address the physical layer and the lower portion of the data link layer (also known as the medium access controller, or MAC, sublayer). The physical layer addresses modulation (encoding data onto an electromagnetic waveform), frequency use, and transmission. The MAC layer refers to access points and maintains the order of signal flow to avoid signal collision and cancellation.

Two of the most widely used standards today were originally designed for office or in-building wireless systems. They are known as **802.11b**, issued by the Institute of Electrical and Electronics Engineers (IEEE), and **Bluetooth**, which was developed by a group of commercial companies (www.bluetooth.org). Both of these standards use the unlicensed 2.4 gigahertz (GHz or billions of cycles per second) band, the same band used for microwave ovens and industrial heating. This band spans 2.4 to 2.4835 GHz in the United States, and the Federal Communications Commission (FCC) has classified it as an Industrial, Scientific, and Medical (ISM) band. Other popular ISM bands include 5.8 GHz and 900 megahertz (MHz) (see table of ISM Bands). The 60 GHz unlicensed band has also recently become available and holds promise for reducing interference in short-range applications.

ISM Bands

| Frequency Band | Characteristics | Products That Use It |
|---|---|---|
| 900 MHz (902-928 MHz) | Lower throughput, better wall penetration and range<br>Available only in the U.S., Canada, and Australia | Proprietary protocols |
| 2.4 GHz (2.4-2.4835 GHz) | Slots of this frequency are available throughout most of the world | Bluetooth<br>802.11b<br>Industrial heating equipment |
| 5.8 GHz (5.725-5.850 GHz) | Highest available throughput, better noise immunity, stricter line-of-sight constraints, smaller antennas possible | No products yet developed; greater technical challenges at higher frequency |

The FCC set aside these ISM bands for license-free, low-power radio transmission over short to medium distances. In these bands, the FCC requires that the signal be distributed over a wide swath of bandwidth using a spread spectrum technology—originally developed by the military for anti-jamming applications.[3] Wireless devices that operate in these license-free bands can allow immediate, real-time commissioning of a network, avoiding the delays associated with installing wiring or cables.

| | IEEE 802.11b | Bluetooth |
|---|---|---|
| Effective distance | 500 meters | 10 meters |
| Spread Spectrum Technique | Direct Sequence (DHSS) | Frequency Hopping (FHSS) |
| Data Rate | 11 Mbps | 721 kbps |

By spreading data transmissions across the available frequency band in a prearranged scheme, spread spectrum encoding technology makes the signal less vulnerable to noise, interference, and snooping. The significant amount of metal often found in industrial settings can cause signals sent over a single frequency to bounce and cancel other signals arriving at the same time. Spread-spectrum technology helps overcome this problem and allows multiple users to share a frequency band with minimal interference from other users.[4]

Although there are three spread-spectrum schemes suitable for industrial wireless systems, the two most common are frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). Bluetooth uses

FHSS, in which the transmission hops in pre-defined patterns from channel to channel across the entire 83.5 MHz spectrum. 802.11b uses DSSS, which divides the spectrum into overlapping 22-MHz channels and sends all the information through those swaths.[5] The popularity of both of these standards has increased interoperability among wireless products from different vendors, but the two standards have the potential for spectrum conflict.

The third spread-spectrum technique, Ultra-Wideband (UWB), broadcasts on many frequencies simultaneously, distributing its signal across a vast bandwidth. The idea is that the signal is spread so thinly that interference will be negligible in any one frequency, but many have expressed concern about potential interference.

## Spread-Spectrum Encoding Techniques

| Technique | Approach | Characteristics |
|---|---|---|
| Frequency Hopping Spread Spectrum (FHSS) | Transmission jumps from frequency to frequency at a predefined rate and pseudo-random sequence | Reduces interference |
| Direct Sequence Spread Spectrum (DSSS) | Signal is sent over a range of frequencies by sub-sampling each bit in the data stream with a high-rate, pseudo-random spreading code | Implementations with a 63-bit spreading code provide a robust interface and process gain (power savings) |
| Ultra-Wideband (UWB) | Spreads signal over a very large frequency range at low power | High throughput; good in areas with physical obstacles; used for live video feeds |

Each technique offers advantages and disadvantages under the various conditions that might be encountered in a typical sensor application.

The newer 802.11a and 802.11g standards support speeds as high as 54 Mbps (million bits per second). Instead of spread spectrum, both of these recently ratified standards employ the relatively power-intensive, wideband orthogonal frequency division multiplexing (OFDM) signaling technique. OFDM, which was not originally designed for industrial applications, offers higher throughput in areas without intervening walls or other obstructions, but is less power-efficient than most other data-transmission schemes due to its requirement for high radio frequency linearity. Unlike FHSS, it uses all channels at once, boosting throughput but increasing the likelihood of interference with other wireless devices in the area. Both standards also use the unlicensed ISM and national information infrastructure (U-NII) frequency bands (802.11a at 5 GHz and 802.11g at 2.4 GHz). The U-NII bands are just beginning to be exploited by wireless networking applications.[6] If these standards achieve widespread commercial acceptance that results in lower costs, they are likely to find numerous niche applications in industrial operations.

Other bands now available in the U-NII category include 100-MHz bands beginning at about 5.1 and 5.2 GHz. Although some commercial, off-the-shelf products are now available for use in these bands, few have been implemented in industrial applications to date.

As the speed of data transmission (throughput) increases, radio frequency signals supply less energy per bit, adversely affecting reliability. Suppliers to the commercial market for personal communications devices tend to value throughput over reliability (generally higher frequencies), and they exert a strong influence on emerging standards. Developers of wireless industrial sensor systems, on the other hand, tend to value reliability over throughput (generally lower frequencies). Greater flexibility is needed in making these tradeoffs as appropriate to the application.

## Bandwidth Availability/Regulation

Data throughput is adversely affected by distance and the amount of "noise" or interference in the area. If too many wireless devices are operating in the same vicinity, they can interfere with each other, restricting network capacity. If insufficient spectrum is available for interfaces among the wireless devices, communication can become difficult or impossible.[7]

Many of today's wireless systems contain provisions for collision avoidance and packet retransmission in the event a signal is blocked by interference. Users can also block out frequencies that experience continuous interference, thereby "sidestepping" offending signals. These techniques, combined with the use of maximum permissible transmit power and highly sensitive receivers, can yield a reliable transmission even over longer distances. On the down side, these solutions are energy-intensive and can generate interference for other systems.

In terms of protection from interference, users of FCC-licensed, narrow-band systems have a regulatory edge and an avenue of redress if interference does occur. Spread-spectrum technology is based on interference avoidance techniques, but if outside transmission does disrupt communications, users can only switch to another frequency[8] or block out channels occupied by the interferer. In short, users of license-free bands are responsible for reestablishing communications—they cannot complain to the FCC. Rapid growth of wireless devices has generated increasing concern about future overcrowding of the ISM bandwidth.

## Power

Since industrial applications increasingly employ miniaturization and require longer intervals between scheduled maintenance, the power source and power conservation strategies are key issues for wireless sensor systems.

Some of today's wireless systems rely on solar panels, but many require batteries that require periodic replacement. Although this is an important power source issue, maintenance requirements have been greatly reduced by today's more power-efficient wireless devices and recent gains in battery performance.


More devices operating in a bandwidth can cause more transmission repeats and higher power requirements.

Many current wireless systems require regular attention to the power source, necessitating a scheduled outage every 3 to 18 months. Techniques such as exception reporting and power management can extend battery life for multiple years. Even when maintenance is required, shutting down a networked wireless site need not cause disruption to the remainder of the network. Auto-discovery techniques will recognize the site when it is brought back online, and operation will continue.

Frequency hopping (FHSS) provides greater range by transmitting short signal bursts, but this uses higher peak power. In contrast, direct sequencing (DSSS) uses available power to spread the signal thinly over multiple channels, resulting in a wider signal with less peak power. Transmitting over longer distances and overcoming interference increase the power demand. Bi-directionality and the need to transmit waveforms similarly drive up power requirements.

One power conservation strategy is to minimize the duty cycle—the interval between measurements. This strategy can be applied only when the measured process parameter changes relatively slowly. In applications where power consumption must be kept to a minimum, many of today's networks report "by exception" rather than the traditional "polling" scheme used in multiple address systems. Rather than requiring the wireless device to transmit at regular intervals (whether it has new data to report or not), transmissions are made only when a user-definable condition is met. One potential problem with this approach is that the network may be flooded with reports if the process suddenly goes awry.

Another power conservation strategy is to use process gain, an encoding technique that involves spreading the signal over a wider bandwidth than is strictly necessary to recover the signal from background noise or interference. DSSS, for example, can sample every bit 63 times, which has the same effect as amplifying the signal without actually using power to do so. Process gain can increase the reliability of transmission and avoid the need for retransmission or use of higher power to overcome interference (in effect, reducing power demands without sacrificing reliability).

## Manageability

When a network experiences drop-outs, outages, or reduced throughput, end-users need tools that can help locate the problem and prevent recurrences. Some of today's systems include tools that allow early detection of problems before they pose a threat to network operations. In distributed networks, these

tools can also help minimize or eliminate trips to wireless sites to change configuration parameters.

## Functionality

Most of today's wireless systems incorporate sensors and communications interface components that are physically separate devices, and the systems require configuration by the installer or the user. In the future, however, system developers envision networks of integrated components that configure themselves and perform a host of other functions that will make for rapid system commissioning and unprecedented ease of use. The technology is progressing rapidly.

In August 2001, researchers from the University of California-Berkeley and the Intel Berkeley Research Lab demonstrated a self-organizing wireless sensor network with more than 800 low-power sensor nodes. Today, several developers of industrial wireless sensors are advertising self-organizing, self-healing, wireless networks. Some feature intelligent, mesh-based topology (allowing every node to communicate with every other node) designed for scalability into the tens of thousands of nodes.

## Cost

Today's wireless sensors currently cost an estimated $500 to $5,000 installed, with the median installed cost being about $1,000. The life-cycle cost is believed to be at least three times the installed cost.

## Security

Spread-spectrum technology presents unintended receivers with challenges: they must know the specific frequency band, modulation technique, and spreading code. Well-designed wireless networks also provide encryption tools to keep transmissions secure.

Many of today's systems have 128-bit encryption with dynamically generated, rotating encryption keys, that are also password-protected and have mechanisms in place to prevent eavesdropping and unauthorized access. These systems also provide report generation for network activity, including logins/logouts and attempted access by "rogue" users.

For maximum security, internal network precautions—separate from those implemented in the wireless layer—are strongly recommended, including firewalls and virtual private networks- VPNs. These are essential to maintaining a secure network, whether wired or wireless.

### Challenged by Industrial Environments

Some wireless systems will perform in certain challenging environments:

- High and low operating temperatures (-40˚ to 70˚ C or -40˚ to 158˚ F)
- High humidity levels (95% at 40˚ C or 104˚ F, non-condensing)
- Potentially explosive situations (intrinsically safe for use in UL Class 1, Division 2 installations)
- Mobile and stationary metal equipment affecting transmission pathways (reject interference from "noise," signal overload, inter-modulation distortion, and co-channel desensitization)

## Reliability

Many of today's standards-based solutions offer a "consumer-grade" mean time between failures (MTBF), which may not be adequate for industrial applications. Harsh industrial environments, in particular, can adversely affect reliability. Some of today's systems can operate within some industrial environments, but not others (see inset). Reliability also includes avoidance of interference or noise from other devices and the ability to receive weak signals reliably in the presence of such interference. Consequences of failure are not trivial. Industrial applications entail the risk of substantial losses through equipment damage, personnel injuries, loss of raw materials, and environmental pollution. In most industrial applications, reliability is far more important than throughput.

---

[1] McEldowney, Doug, and Ken Hall (n. d.). The progression of wireless Ethernet in industrial environments, *A-B Journal.* Retrieved October 12, 2002, from ab.com/abjournal/june 2002/departments/todays_tutorial

[2] Retrieved October 14, 2002, from www.zoomtel.com/bigglossary.html

[3] Hedy Kiesler Markey (a.k.a. Hedy Lamarr) and George Antheil, U.S. 2,292,387, Secret communication system.

[4] Dell Online (April 2001). Deploying 802.11b in the enterprise network, Vectors white paper. Retrieved from http://www.dell.com/us/en/gen/topics/vectors_2001-wireless_deployment.htm

[5] 802.11b Networking News, filed *4/5/01 by Glenn Fleishman,* http://80211b.weblogger.com/coexistence.html

[6] Kapp, Steve, Cisco Systems (January-February 2002). 802.11: Leaving the wire behind, IEEE Internet Computing Online. Retrieved December 3, 2002, from www.computer.org/ internet/v6n1/w102wire2.htm

[7] McEldowney and Hall, *A-B Journal*, 2002.

[8] AIM Network, Association for Automatic Identification and Data Capture Technologies, Data basics, http://www.aimglobal.org/technologies/datacom/dcbasics.htm

# The Future of Wireless:

## *Workshop Results*

Wireless sensor networks will become ubiquitous in U.S. industry as they deliver an easy and cost-effective way to improve processing performance and productivity. Highly reliable and secure wireless systems with distributed intelligence will enable industry to exploit powerful new sensor capabilities and reliably exercise closer control of critical production processes.

### Industry-Defined Goals

To achieve their vision of the future (inset), the industrial wireless sensor community will need to achieve a series of ambitious goals and performance targets. As discussed below, attainment of these industry-defined goals will require key advances in power, reliability, integration, cost, functionality, and bandwidth efficiency.

**Industrial Wireless Sensor Vision**

Industrial wireless technology will be robust, reliable, cost-efficient, totally secure, and in many cases, integral to the measurement device. It will be the obvious choice for monitoring and controlling industrial processes to optimize resource efficiency and productivity.

### Power

Through design improvements, wireless sensor systems of the future will require less power and therefore less maintenance (e.g., battery replacement) than today's systems. By **2010**, costs associated with operating and maintaining these systems (sensing and transmission) will decrease by 90 percent. In the **long term**, systems will be self-powering, capturing energy (e.g., thermal, solar, or vibrational energy) from the industrial environment and virtually eliminating power maintenance activities and related costs.

Wireless systems will use "embedded intelligence" to process sensor data and minimize power use. These "smart" sensor systems will use a reporting system that minimizes transmissions to simultaneously reduce power usage and avoid transmission interference.

Prior to 2010, new system topologies (the physical layout of nodes) may minimize power demands as a function of the distance of transmission, amount of data, and radio frequency. For example, selected data may be transmitted across short distances (node to node) in a series of low-energy transmissions until reaching the receiver for the control system or until a transmitter with a stronger energy source is engaged to pass on the message.

## Reliability/Maintainability/Availability

Wireless systems of the future will reliably perform mission-critical monitoring and control functions. Maintenance requirements for these systems will be minimal, whether for battery replacement, verification of sensor calibration, or any other activity necessary to sustain system performance. The mean time between attention (MTBA) will at least equal the period between scheduled downtimes for the maintenance of other production equipment. In short, wireless systems will not upset production or cause a shutdown.

### Tailored to Industrial Environments

Robust wireless systems will reliably perform mission-critical tasks in harsh industrial environments:

- Extremely high and low operating temperatures
- Strong vibrations
- Airborne contaminants
- Excessive electromagnetic noise caused by large motors or conductors
- Exposure to harsh, corrosive chemicals
- High humidity levels
- Potentially explosive situations
- Mobile and stationary metal equipment affecting transmission pathways

Wireless systems and components will be built to withstand the extreme temperatures, vibrations, and other harsh environments typical of industrial operations (see inset). They will also be immune to nearby radio frequency generators and multipath interference from reflected signals.

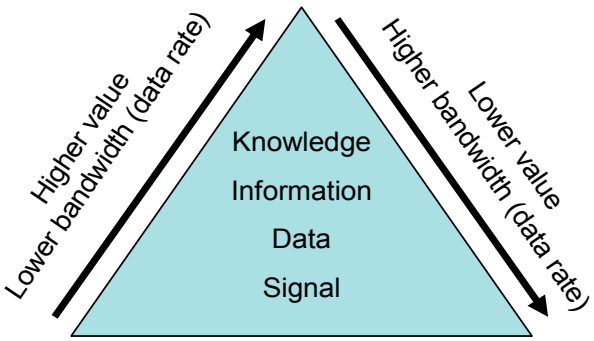
The performance reliability of future systems will be sufficiently high that they can be depended upon to perform essential functions. This high level of reliability is necessary to avoid the consequences of non-performance, which in some industrial applications may include personnel injury, off-spec production, damage to costly capital equipment, environmental pollution, or material losses.

The **2010** goal is a tenfold increase in today's required attention interval (from 3-18 months to at least 3 years). The stretch goal for these systems over the **long term** is zero maintenance for the intended mission life of the wireless system.

## Integration/Compatibility

Future wireless systems will operate with a non-proprietary open architecture infrastructure that will facilitate processing and transmission of data to and from sensors and controllers produced by different companies. Systems will be capable of handling output from sensors of all types, including new and already-in-place (legacy) sensors. By **2010**, these systems should provide interoperability (see page 6) at the data level. In the **long term**, these systems

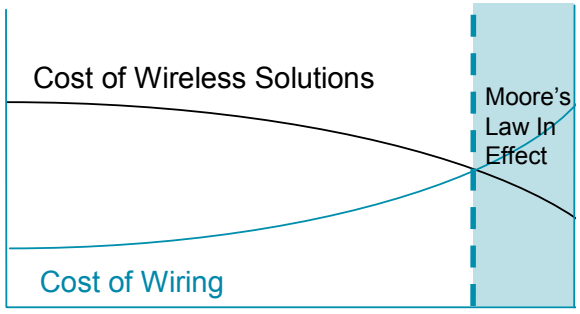
should provide interoperability at the knowledge level, such that the system can analyze and act on the information.




Achieving true interoperability will require an overarching open architecture, within which various standards may apply. One approach may be to move from hardware-based to software-based systems. An established reference design, for example, could cover every type of wireless sensor and the devices with which they might need to interact in 2010. All these devices would have the capability to change their communications protocols and apply them through software. Such open standards and open protocols would also allow for some proprietary solutions. These proprietary components would be encapsulated and isolated from the open system infrastructure, yet would allow new and extremely innovative solutions.

## Cost

Over the next decade, technological advances and economic drivers will move wireless sensor systems onto a track of steadily increasing performance and declining costs. Inexpensive, disposable, "peel and stick" sensors with "plug and play" compatibility will lead the way for sensor networks to operate on "Moore's Law" for the first time. Continued advances will gradually open the door for sensors further up the complexity continuum to migrate toward this model.



Y-scales are application-dependent.

Competitive pressures continue to force industrial end-users to seek new strategies for streamlining operations. Integrated wireless sensor systems represent a promising tool as their costs continue to drop. By **2010**, the installed cost of a wireless system should be only one-tenth of today's installed cost. In the **long term**, many sensors will be integral components of the production equipment, and their costs will be incorporated into equipment costs. Sensors at either end of the complexity spectrum, however, will continue to be offered separately on the market.

Integration costs provide a convenient measure of progress in compatibility. By 2010, the addition of individual sensors to a system should increase the cost in a linear rather than compounded fashion as is now the case. Linear cost escalation is far easier to justify in an industrial environment than the current exponential (or worse) cost increases associated with network expansion.

The true cost of wireless sensors includes the cost of the devices, calibration, integration, maintenance, operation, information abstraction, and security. By 2010, these life-cycle costs should be only half of current costs. As in any business, the key to the cost issue is return on investment. As wireless sensor systems improve resource productivity on the plant floor, industrial companies will readily invest in wireless sensor networks.

## Functionality

Wireless system components of the future should be able to recognize each other and organize themselves to carry out effective, efficient, and secure communications, even on an ad hoc basis. These smart, distributed, heterogeneous computing devices should be nearly self-sustaining. Demands on the user will be minimal as the systems become self-configuring, self-calibrating, self-identifying, and self-reorganizing for optimal network performance and fault recovery. Sensor nodes will also be designed to be self-locating to ease bookkeeping requirements and associated costs.

Individual components will be capable of performing different functions as required in response to dynamic industrial environments and system conditions. Multi-functional devices, for example, may redistribute tasks to assume the functions of a node temporarily blocked from performing.

The primary metric for gauging progress in functionality is ease of use. The **2010** goal is to provide wireless sensor networks that are self-configuring. For the **long term**, the goal is to create self-commissioning systems with advanced, embedded computing and communications solutions. These advanced systems will increase ease of use to the point that they perform autonomously.

The security function is a significant concern in a growing number of industrial applications. Network security and integrity must be protected against insider curiosity and outsider eavesdropping or attack; industrial espionage and cyberterrorism are growing concerns among industry. Levels of protection should be scalable and set according to the potential ramifications of access.

Network managers should assume that all attackers are hostile insiders—as that is the worst-case scenario. Security can be strengthened by using advanced modulation, encoding, encryption, and interleaving technologies. One approach is to make the network signals simulate random noise; they become virtually indistinguishable from the normal background noise of the environment.[1] While precautions can be implemented on both wired and wireless systems, wired network managers often take security for granted. Consequently, spread-spectrum wireless systems may well be more secure than their wired counterparts.

Security goals can be expressed in terms of the amount of time required to gain unauthorized access. By 2010, the time required to breach the security of a

wireless sensor system will be an order of magnitude longer than it is today. The **long-term** goal, of course, is to totally block unauthorized access, no matter how much effort is expended. Security is obviously a moving target, and wireless systems of the future must be extensible to stay ahead of advances in tools and techniques for gaining access. The open architecture infrastructure will facilitate continuous improvement so that security stays ahead of the curve.

## Bandwidth Efficiency

Growing use of industrial wireless technology will place heavy demand on the narrow bandwidth currently available. Efficient use of the bandwidth is imperative to reduce interference and avoid the resulting increase in power use. System developers will need to embrace a strategy of bandwidth conservation to avoid higher power requirements and associated costs. They will use embedded intelligence to reduce transmission loads where feasible and use the minimum amount of power to maintain effective communications.

Industrial end-users need the ability to predict the quality of service they can expect from a wireless sensor system, given the interference factors present in their specific industrial settings. Before 2010, a flexible quality-of-service model will be developed to meet this need. By 2010, developers will have eliminated self-interference as well as interference from external systems (e.g., other wireless systems in the area). For the long term, nanotechnology or another innovative approach will enable devices to operate beyond the realm of existing radio frequencies, relieving or removing the bandwidth constraint.

As wireless technology expands, industrial wireless systems will need to support a growing number of protocols and frequencies, increasing the value and advantages of an open, frequency-agile architecture. Flexibility will also remain essential in related and often interdependent system characteristics. While priorities will change according to application, the following system capabilities are generally desirable:

| Maximize | Minimize |
|---|---|
| Data rate (bits/second/hz ) | Latency (sample rates & updates) |
| Range (distance) | Bit Error Rate (BER) |
| Volume (sensors/area) | Power demand |
| Security (time to access) | Cost ($ per bit per Hertz) |

The goal for **2010** and the long term is continuous improvement in all of these areas.

[1] Manges, W. W., and Allgood, G.O. (February 2002). How secure is secure? *Sensors: The Journal of Applied Sensing Technology,* 14-23.

# Challenges

## *Opportunities for Progress*

Industrial wireless sensor systems face challenges and opportunities in fulfilling their potential for U.S. industry. Even as wireless sensor technology continues to benefit from advances in other commercial wireless products, system developers will need to overcome significant hurdles unique to industrial applications.

In industry, uninterrupted production has always been of paramount importance. Plant managers will not adopt a new technology until they are certain it can deliver real value to their operations. Many manufacturing industries operate on narrow profit margins, so any system downtime can have major consequences for profitability. Industrial facilities require systems that perform quickly, reliably, and cost-effectively.

In some industrial applications, consequences of system faults or failure can be extremely serious, including explosions, personnel injury, toxic releases, or major damage to capital equipment. These plants demand demonstrated operational reliability in similar industrial environments before committing to any investment in new systems or equipment.

Developers of integrated wireless sensor systems will need to work with representatives of the industrial manufacturing community and others to better understand and address concerns. At a minimum, they must resolve the following key issues regarding technology, collaboration, culture, regulation, and cost.

### Technology

**Proven operational reliability**. Wireless sensor systems can gain industry confidence by demonstrating reliability under realistic factory conditions. A test bed facility should be established at a respected agency or organization to make objective measurements and certify the capabilities of candidate systems in various areas. Provisions for additional, long-term demonstrations of wireless sensor systems in some of the most challenging industrial environments would provide valuable proof of reliability.

**Sustained Performance in Harsh Environments.** Some industries may wish to use industrial wireless sensors in processes that expose the sensors to

temperatures of up to 2,600° F. Sensors may also be subject to highly caustic or corrosive environments, high humidity levels, vibrations, dirt and dust, or other conditions that challenge performance. Industrial companies need to know with absolute certainty that a given sensor system can perform reliably in a prescribed range of conditions.

**Fail-soft operation.** Many industrial processes involve dangerous work environments requiring high reliability over defined periods. In many cases, fail-safe operations are too expensive. Many industrial end-users will accept fail-soft systems. These systems are designed so that they will only fail in a predictable, non-catastrophic manner and/or move into a safe state.

**Intrinsic Safety.** For some applications, wireless sensor devices themselves must be intrinsically safe. That is, the devices must not be capable of igniting an explosive gas in the environment, even under fault conditions.

**Invulnerability to Interference.** Wireless sensor systems must demonstrate that they can communicate effectively even in areas with high electromagnetic noise or radio frequency interference. System operations must remain unaffected by such common industrial equipment as moving metal vehicles, storage tanks, arc welders, and banks of variable-speed drives that can affect transmission characteristics. Developers must also be aware of the potential for new devices to interfere in the electromagnetic spectrum. There is a growing need for tools to facilitate complex site surveying and planning. Similarly, end-users would benefit from tools for managing plant spectrum.

**Security.** Industrial end-users have expressed major concerns about the integrity of signal transmission and reception. System developers must be prepared to provide security options with demonstrated success against state-of-the-art attacks. Security designs should assume the worst-case scenario—unauthorized access by someone impersonating an authorized employee.

**Power.** In the near and mid term, wireless developers need the ability to store more power capacity in a given amount of space (increase the energy density and power density of power sources). At the same time, they must find ways to make more efficient use of power conservation strategies such as process gain and power management (e.g., duty cycle controls). This is particularly important to successful deployment of integrated wireless sensors using MEMS technology. For the long term, developers will extend the ability to scavenge or harvest power from the industrial environment.

## Collaboration

**R&D Funding**. The required development and integration work will require substantial research and development (R&D) involving expertise in communications, sensors, industrial applications, and commercial computer systems. Most organizations will be unable to tackle this challenge alone. The

effort will require collaborative R&D by a variety of organizations working in these fields. Sources for funding and mechanisms for facilitating the development of collaborative R&D partnerships or teams must be identified.

**Scale-Up.** A formal process is needed for scaling up many promising technologies now at the bench-scale. Anecdotal information indicates that exciting new developments may be stalled in small laboratories around the country. Initial developers may lack access to funding or channels for finding partners who can help them take the next steps. Mechanisms are needed to foster the development of business partnerships that can advance these technologies.

**Integration of components.** Many system developers today tend to specialize in a single technology area. Successfully integrated wireless sensor systems will develop a multidisciplinary perspective (including sensors, communications, information technology, and end-user applications). System developers need a strategy for fostering cooperation among diverse companies and organizations to achieve their technical objectives.

## Culture

**Work force/corporate attitudes.** Changeover from a wired to wireless sensor system, particularly one that is capable of autonomous operation, may require adjustments in corporate culture. How will maintenance workers react to the system? Will they harbor concerns over job security? Will managers and engineers need to think differently about the operations? Will technical training be required? Many new control systems are subverted by employees who misunderstand the new technology and lack confidence in its ability to improve over earlier operations. Those responsible for risk management are particularly wary of such innovations. Forethought and planning on these issues could avert future problems.

**Societal attitudes**. The general public has limited understanding of complex technologies and their value. While the public has embraced wireless personal communications, will they show the same enthusiasm as the technology moves into industrial manufacturing? Will misperceptions or fringe elements generate resistance? Will the technology raise privacy issues? System developers and industrial end-users should not neglect emerging public attitudes as the technology evolves. Early public outreach can dissolve issues that might otherwise become major impediments to deployment.

## Regulation

**Interoperability**. Development of true interoperability will require an open architecture within which different standards may apply. The industry needs well-written standards that genuinely promote interoperability. Standard developers should seek not to protect their own narrow interests, but to establish a framework that will help the entire industry flourish. In the long run,

broad-minded thinking of this type generates ample dividends for all. The FCC should also be brought into the process, allowing all parties to share information and secure the best outcome.

**Spectrum Policy**. The wireless sensor community may benefit broadly from the formation of an organization that can represent its interests in negotiations with the FCC, particularly as part of efforts to acquire additional bandwidth to serve the growing demand for industrial wireless systems. A proactive posture in this area could help industrial wireless systems gain access to the available bandwidths most conducive to industrial objectives and environments—which differ markedly from those of commercial personal computing systems.

## Cost

**Value Proposition.** Many potential end-users of industrial wireless sensor systems lack a full understanding of the value these systems can bring to their operations. They perceive wireless systems as more expensive than they really are because their analyses stop at the initial software and hardware costs. The industry needs to find compelling ways to communicate to their potential customers the true value of these systems, including

- Scalability
- Ease of Installation and Configuration
- Ability to integrate and allow migration of current network
- Reliability
- Cost of Implementation
- Manageability
- Future-readiness

Once plant engineers have been convinced, they will need material for convincing management.

## The Path Forward

Industrial wireless sensor systems hold tremendous potential to improve U.S. industrial productivity and product quality. As noted above, the challenges to achieving the full potential of these systems will require both technical and non-technical solutions. Technical solutions will require major funding and concerted R&D efforts that tap the expertise and resources of the diverse stakeholders in the technology. Sensor developers, wireless communications suppliers, computer processing specialists, and industrial end-users must work together to develop and demonstrate effective systems that perform successfully in plant operating environments and deliver on the promise.

*All* stakeholders are encouraged to join in this worthwhile endeavor.

# Appendices

A. Results of Facilitated Sessions
B. Presentations

# A. Results of Facilitated Sessions

## Key Characteristics & Capabilities

◆ = Top Priority for End-Users
● = Top Priority for All Others

| Power | Reliability & Maintainability/ Availability | Integration/ Compatibility | Cost | Sensor Functionality |
|---|---|---|---|---|
| ▪ Low power consumption ◆◆◆●●●●●● <br> ▪ Power management ●●●●●●● <br> ▪ Scavenge power from environment ●●●●●● | ▪ Performance assured ●●●●●●●●●●●● <br> ▪ Trustworthy ●●● <br> ▪ Able to survive harsh (hazardous) environments ◆● <br> ▪ EMI compatibility ◆● <br> ▪ Error-free communications ◆ <br> ▪ Self-healing <br> ▪ Zero maintenance | ▪ Open standards ●●●●●●●● <br> ▪ Self-organizing ◆●●●● <br> ▪ Upward compatible, also forward and backward ◆◆ <br> ▪ Able to talk to multiple architectures (multi-lingual) ◆● <br> ▪ Fully vertically integrated ● <br> ▪ "Agnostic" systems (protocol independent) | ▪ Low cost <br> ▪ Cost-effective ◆◆◆●●●●●●●● <br> ▪ Sustainable in the market ●●●● <br> ▪ Asset management | ▪ Self-configuring ●● <br> ▪ Environment-aware devices ● <br> ▪ Enables customer-defined intelligence distribution ● <br> ▪ Multi-mode (multi-functional) ● <br> ▪ Self-identifying <br> ▪ Self-locating <br> ▪ Self-calibrating <br> ▪ Ease of use (would have had a few votes) <br> ▪ Intrinsic safety |
| **Frequency Bandwidth** | **Sensor Physical Properties** | | | |
| ▪ Bandwidth efficiency ◆●●●● <br> ▪ Endless data capacity (bits per second per cubic meter) | ▪ Scalable in quantity, processing power, density, intelligence ◆ <br> ▪ Modular ● <br> ▪ Sensors on inside–organic ● <br> ▪ Small size <br> ▪ Embedded <br> ▪ Mobile <br> ▪ Environmentally friendly | Goal: *Be the "obvious choice"* | | |

| Performance Targets (1 of 2) | | | |
|---|---|---|---|
| **Characteristics**<br>Metrics | **Today's Baseline** | **2010** | **Long-Term** |
| **Power** | ▪ Frequent battery maintenance (3 to ~ 18 months; 10 years for one-way transmission)<br>▪ Power source/batteries that must be replaced (cell phone case) | ▪ Low power use<br>▪ Reduce maintenance (O&M) cost of power by factor of 10 (includes the sensor)<br>▪ Scavenge power from the environment | ▪ Maintenance-free power |
| **Reliability/Maintainability/ Availability**<br><br>Local attention (hands-on)<br>- duration of maintenance attention<br>- mean time between attention | ▪ Sensors and communications are separate systems<br>- treated separately by supply chain, not by end-users<br>▪ 3–18 months between required attention to powered sensors (3 for battery powered, 18 with outside power) | ▪ Not driving force for an outage (scheduled)<br>▪ Increase required attention interval by factor of 10<br>▪ Able to survive harsh environments | ▪ Disposable<br>▪ Zero maintenance for intended mission life |
| **Integration/Compatibility** | ▪ None | ▪ Open architectural standard(s)<br>▪ Interoperability at the data level<br>▪ Linear scalability in terms of cost of adding sensors | ▪ Interoperability at the information/ knowledge level |
| **Cost**<br><br>Total lifecycle: devices, integration, maintenance, operations, information extraction<br>Installed only | ▪ Lifecycle management<br>▪ Lifecycle cost is at least 3 times installed cost<br>▪ $500 to $5,000 per point installed (median ~ $1,000) | ▪ Reduce installed cost by a factor of 10<br>▪ Reduce lifecycle cost by a factor of 2 | ▪ Cost of the sensors is embedded into the equipment being bought (infrastructure)<br>▪ Disposable sensors |

| Performance Targets (2 of 2) | | | |
|---|---|---|---|
| **Characteristics** | **Today's Baseline** | **2010** | **Long-Term** |
| **Sensor Functionality**<br>- Security | ▪ AES CCM<br>▪ External user-configured<br>▪ Unauthorized access requires "X" amount of time | ▪ Self-configuring<br>▪ Unauthorized access requires "X" amount of time | ▪ Self-commissioned<br>▪ No (zero) unauthorized network access over time<br>▪ Increase ease of use to point at which they are autonomous |
| **Frequency Bandwidth**<br>(self-interference, interference from other systems) | | ▪ Flexible quality of service model<br>▪ Increase: $\left(\frac{bps}{M^2\ W}\right)$ (for the channel)<br>▪ Minimum amount of transmitted power to maintain BER (digital) or SNR (analog) for a given range | |

| Barriers to Achieving the Targets | | | | | |
|---|---|---|---|---|---|
| **R&D Funding/ Collaboration** | **System Vulnerability** | **Regulatory Standards** | **Technical** | **Culture** | **Cost** |
| ▪ Lack of formal process for scaling up lab technologies/ addressing key needs<br>▪ Need to foster business partnerships to advance technology<br>▪ Adequate funding for R&D<br>▪ Need greater participation by sensor manufacturers<br>▪ Lack of integrated, dual perspective: technology and application areas<br>- plus IT | ▪ System vulnerability concerns<br>▪ Vulnerability to intentional jamming, industrial espionage, etc. | ▪ Lack of well-written standards that promote inter-operability<br>▪ Spectrum policy—FCC allocation of open spectrum<br>▪ Regulatory agencies | ▪ Increased energy density and power density of power sources<br>▪ Unproven immunity to RF interference<br>▪ Possibility of new devices interfering in broadband<br>▪ Lack of objective measurements for various aspects of systems | ▪ Impacts on maintenance workers (job security)<br>▪ Technical training needed for workforce<br>▪ Requires change of culture/attitude<br>▪ Compatibility with legacy systems (integration)<br>▪ Lack of industry confidence (end-user through supplier)<br>▪ Complexity of the technology<br>▪ Public perception of privacy implications | ▪ Perceived higher cost<br>▪ Need to generate demand among end-users<br>▪ Lack of material to help convince management of value<br>▪ Lack of end-user understanding of value proposition<br>▪ Lack of certification plan or government clearinghouse |

# B. Presentations

1. Gideon Varga, U.S. Department of Energy
2. Dr. Peter Fuhr, San Jose State University
3. Wayne Manges, Oak Ridge National Laboratory

# Welcome To OIT's Industrial Wireless Workshop

San Francisco, California
July 30, 2002

Gideon M. Varga
U. S. Department of Energy

## What is OIT ?

- The U. S. Department of Energy's Office of Industrial Technologies is one of 11 programs within the Office of Energy Efficiency and Renewable Energy
- OIT works in partnership with U.S. industry to develop and deliver advanced technologies that:
  - Increase manufacturing energy efficiency
  - Improve environmental performance
  - Boost industrial productivity

## OIT Focuses on Key Energy-Intensive Industries

**Industries of the Future**


Glass


Forest Products


Metalcasting


Chemicals


Aluminum


Steel


Mining


Petroleum

## Why Is Government Involved with Wireless?

- Share RD&D costs
- Reduce risk of developers, system manufacturers, and users
- Accelerate progress through goal directed partnerships
- Expedite adoption of industrial wireless systems

## OIT's Wireless Activities

- An OIT-sponsored wireless telemetry project generated high-level interest
- OIT Sensors and Process Automation Program will increase wireless emphasis
  - Launch wireless solicitation
  - Want broad industry participation
  - Seeking consensus among researchers, suppliers and users on direction

## What's Wrong With Wires?

- High installation cost
- High maintenance cost
- Constantly increasing costs
- High failure rate of connectors
- Difficulty in troubleshooting connectors
- Old wires never die
- Multiple sensor inputs can create single point of failure

## Why Wireless?

- Enables continuous, high resolution, ubiquitous sensing
- Adds redundancy
- Potentially lower cost, especially installation
- Easier to replace and upgrade
- Makes use of MEMS technology practical
- Boost from cell phone technology: cheaper, easier, provides experience
- Better process control and energy efficiency, improved product quality and yield, lower costs

## What's In What's Out

**IN**

- Movement of industrial data from sensor to control system to actuator
- R&D to deployment
- New and retrofit
- Application to full-scale automated, integrated systems

**OUT**

- Voice
- Cell phones
- Mainframe to mainframe networks
- Building to building networks

## Wouldn't It Be Nice?

- Compatible with harsh industrial environment
- Interference free
- Low cost
- Everlasting power supply
- Nationwide standards and protocols
- Zero response time
- Security
- Total reliability
- Data rate
- Legacy interfaces
- Worker attitudes
- Commercial availability

## Department of Energy
## Industrial Wireless Workshop

# Wireless Systems for ....

**Dr. Peter Fuhr**
**The Institute for Sensors & Wireless Networking**
**San Jose State University**

## The Industrial Applications are seemingly limitless.....

- Just consider potential sensing of these Forms of Energy:
  - Atomic (force between nuclei and electrons)
  - Electrical (E)
  - Gravitational (gravitational attraction between 2 masses)
  - Magnetic (H)
  - Mass (as in E=mc2)
  - Mechanical (pertains to motion, displacement, forces, etc.)
  - Molecular (binding energy in molecules)
  - Nuclear (binding energy between nuclei)
  - Radiant (related to EM waves, UV, IR, Xray, γray)
  - Thermal (related to kinetic energy of atoms and molecules)



## The Frequency world within we work:



Its Just an Electromagnetic Field

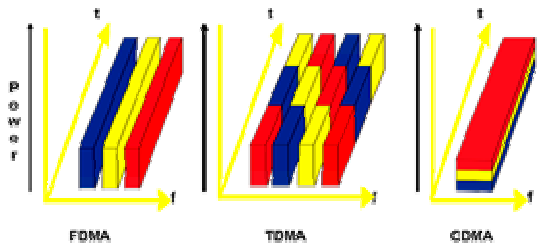
$$E(t) = A(t)\cos[\omega t + \phi(t)]$$

**Contemplate on what the receiver has to do to extract the AM, FM or PM encoded info**

**Amplitude Modulation (AM)**
**info is in A(t)**
**Frequency Modulation (FM)**
**info is in ω**
**Phase Modulation (PM)**
**info is in ϕ(t)**

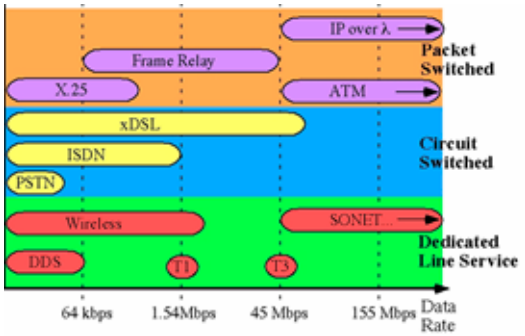


## Details: what multiplexing technique?



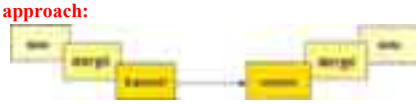



## Details: Protocols and Data Rates?

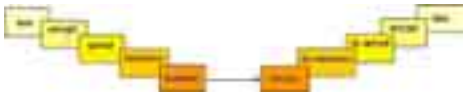


## Details: Data Security?

**the wired approach:**

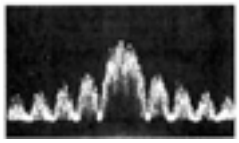


**the wireless approach?**





## Details: Narrowband? DSSS? FHSS?



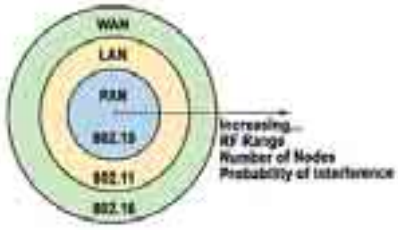


## Details: A "simple" Bluetooth transmission?



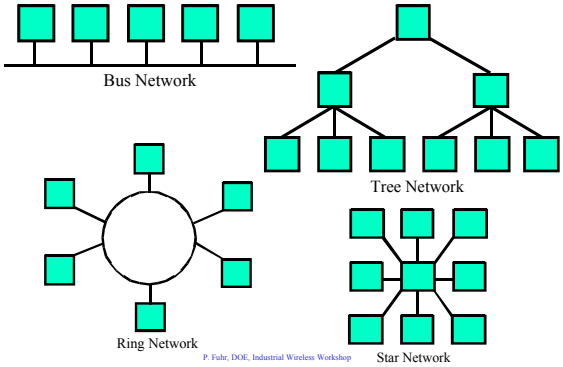
Bluetooth, Feb 2001

## Details: Network cell size? Integration of multiple methods? Cross-platform transmission? Self-Identification?






## Details: Network topologies?

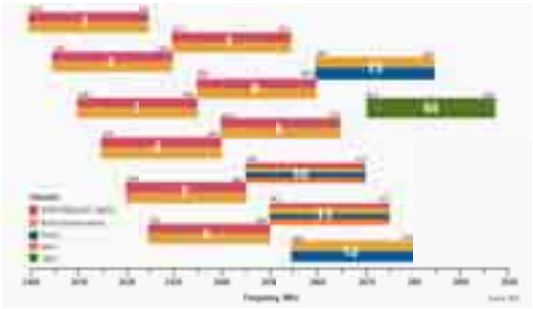





**or does all of this really boil down to a question of power?**

**For a battery powered system, every bit transmitted brings you closer to death!**

## Details: Worldwide implications?



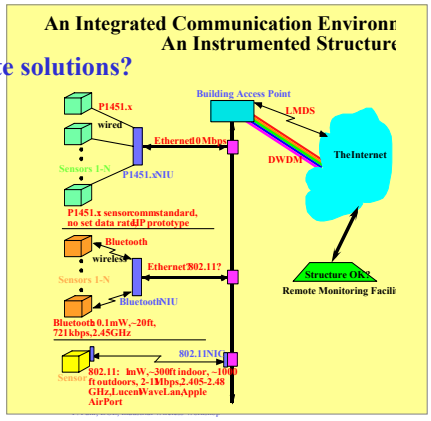


## Details: It's an industrial setting with rampant EMI and attenuation (ambient condition) "conditions".


**Museum Towers. 26 floors. Boston**



## Details: Complete solutions?




## RECOMMENDATIONS

**This is why we are here.**

**So forget about the accountants, let us examine TECHNOLOGY and use our broadbase of talent and experience to attempt to truly examine what it will take for a true penetration of Wireless Technologies into the Industrial Environment.**



## who knows? the final result may be a Monument with all of us standing beside it!

King Bluetooth's Monument



## Questions? Comments?

**Dr. Peter Fuhr**
**San Jose State University**
**Institute for Sensors & Wireless Networking**

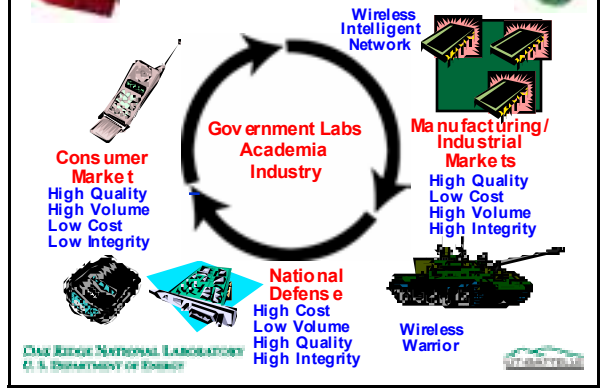
**V: 408-924-3917, f: 408-924-3925, e: pfuhr@email.sjsu.edu**

## The Government Can No Longer Afford to Be the Only Customer

- State of the Art - Commercial vs Government use
- Emerging Trends - Short term, Medium Term
- Enablers and Disablers - Where help is needed to meet government needs

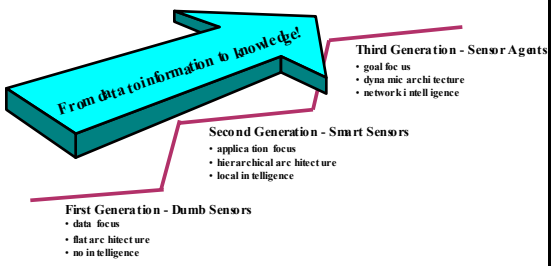


## Everybody Wins






## What Is The Next Generation Sensor System?






## Sensor Agents
## A New Sensor Paradigm

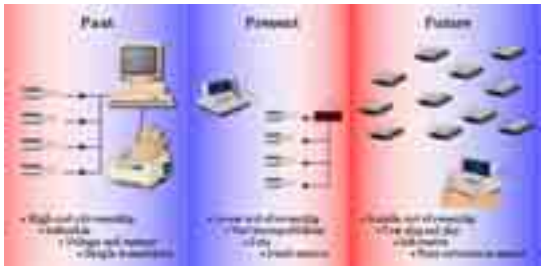
Today's measurement systems are time consuming, lack adequate replication, spatial coverage, and are usually restricted to 'snap shots' during collection period.

*These limitations have a significant impact on understanding the evolution of processes, their dissipative nature, and response to stressors.*

*Sensor agents are goal-directed rather than algorithm directed and can exhibit learned behavior based on metrics, outcomes, and correlation.*



## The Future:
## The Sensor IS the Network






## Emerging Drivers Poised To Impact Deployment

- Moore's Law - increased performance, lower cost… every year
- Agent Technology - goal directed, learn from experience (like Google?)
- Public Acceptance - consumer products go wireless
- MicroElectroMechanical Systems (MEMS) - too small for wires
- Spread Spectrum CDMA - (code division multiple access) - lower power, more channels

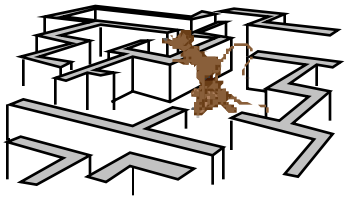
## The Future Must Overcome Roadblocks

- Expertise - shortage of qualified people
- Biases - "been there, done that, bought the tee shirt, didn't like it!"
- Technology - power, architecture, data rates, site planning
- Costs - still can cost more than wire



## Exploiting the Coming Revolution Requires Strategic Partnerships

*Merging science, technology, standards, and marketing*





## Who Will Lead, Who Will Follow, Who Will Whine?

- Technology is ready - driven by cellular personal/business communications
- Market is ready - $2000/ft for wires in some plants
- Are we ready? - partnerships, consortia, standards, and collaborations