Wireless Technology For Use In Process Control Systems

Wayne W. Manges, Director
Extreme Measurement Communications Center
Oak Ridge National Laboratory
October 27, 2005
PCS Forum
Chicago, IL

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

OAK RIDGE NATIONAL LABORATORY
U. S. DEPARTMENT OF ENERGY

UT-BATTELLE

Is Wireless Security An Oxymoron?

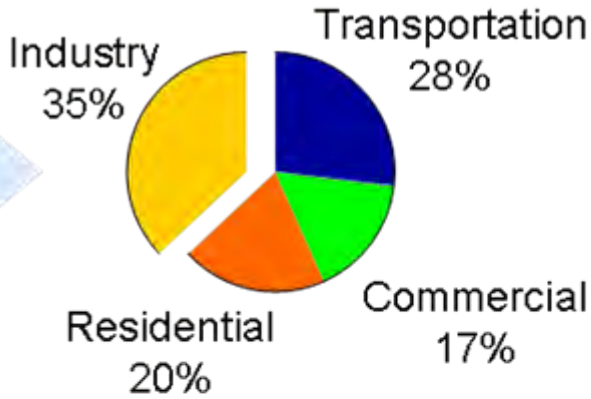
- How we got here
- Why we're here now
- What's happening today
- What coming
- Why it's a good thing
- How we get there together

A key player in the wireless business! Guess Who?

DOE Program Primarily Targets Industry

Industry is the largest single energy-consuming sector in the Nation.

2001 Energy Use

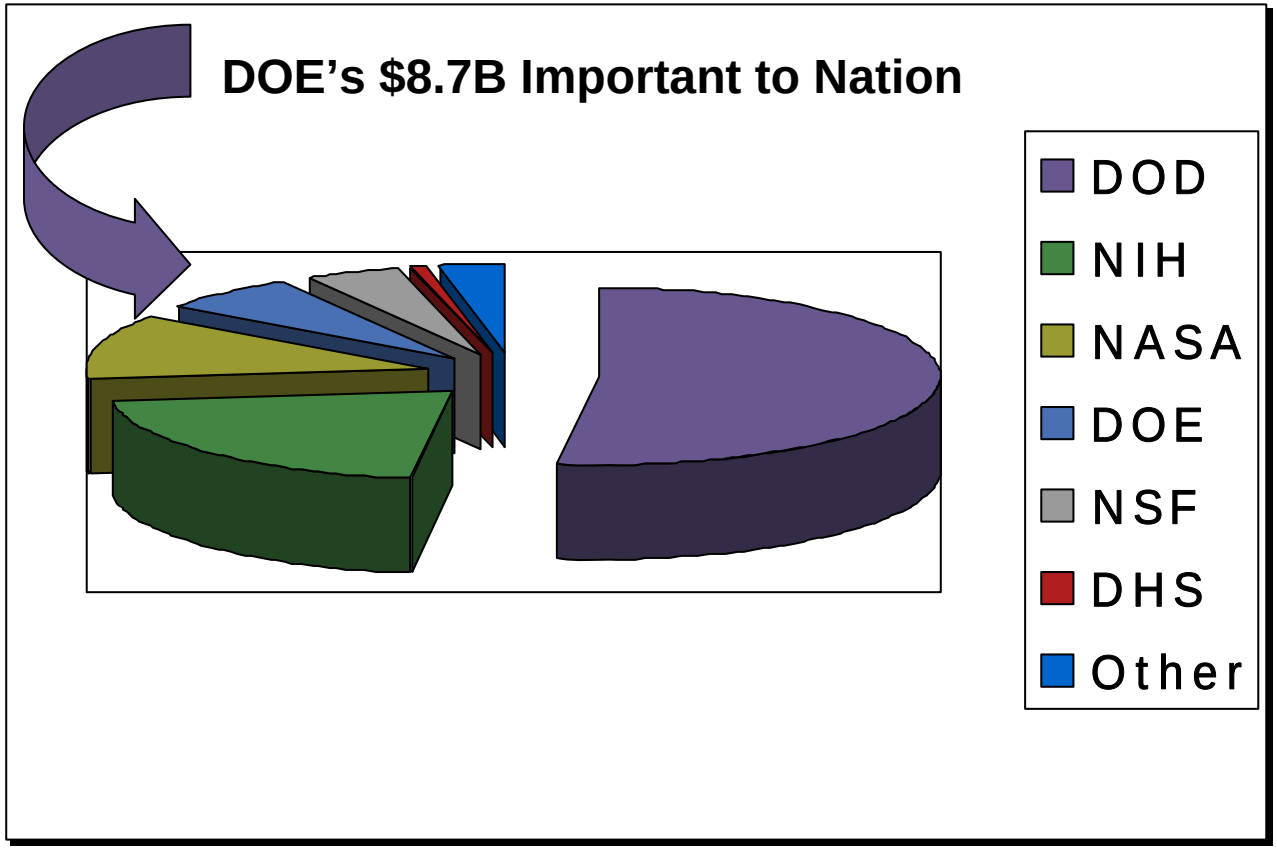


Energy Savings Benefits

- Lower production costs
- Environmental compliance
- Reduced waste
- Increased productivity
- Improved competitiveness

- Economic Strength
- Environmental Quality
- National Security

Department of Energy – A Major Player in US R&D Landscape



National Research Council (NAS) Identified Wireless Research Needs

- **Interference Rejection – self-interference from metal surfaces, lots of sparks and other sources**
- **Integrated Intelligence – reduces need for host communication**
- **Reliable Networks – ad hoc routing, security**
- **Power – harvesting and new batteries**
- **Standards – communication, interfaces, and protocols**

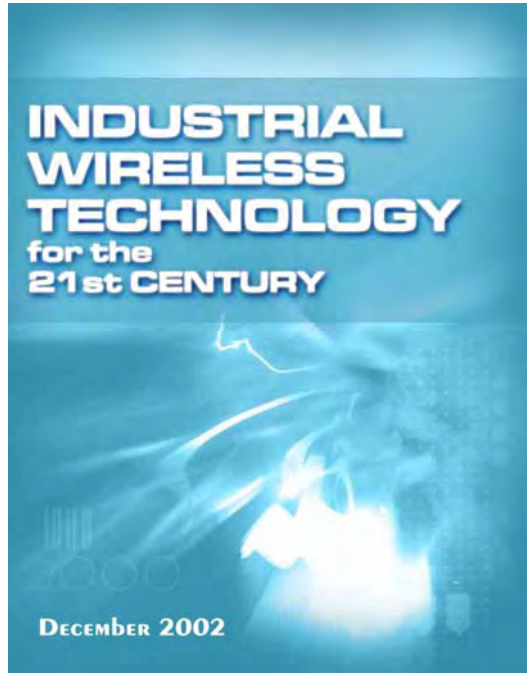
Manufacturing Process Controls for the Industries of the Future - Free PDF version at NAS

Presidential Advisory Committee report identifies industrial wireless with potential for 10% energy reduction and 15% emission reduction.

Vision: Industrial Wireless – Moving Forward

Industrial wireless technology will be

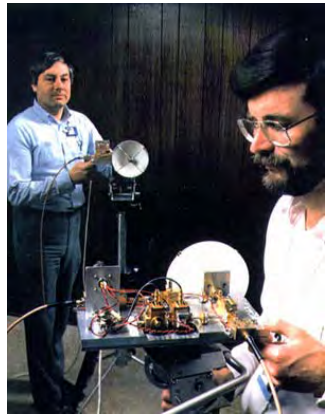
- **robust,**
- **reliable**
- **cost-efficient**
- **totally secure**
- **often integral to the measurement device**
- **the *obvious choice* for monitoring and controlling industrial processes to optimize resource efficiency and productivity.**



Get pdf at WINA web site

ORNL's History of Harsh Environment Wireless and Microsystems

- Robust Communications in Extreme Environments
  - **Markets: Energy, National Security, and Transportation**
- Tagging and Tracking Systems
  - **Markets: Energy, National Security, and Transportation**
- RF and Microwave Measurements
  - **Markets: Energy, National Security, and Science**
- Microsensors
  - **Microcantilevers**
  - **Ultra-low power electronics**



94 GHz Reflective-Environment Communications System

Video Intercept Receiver

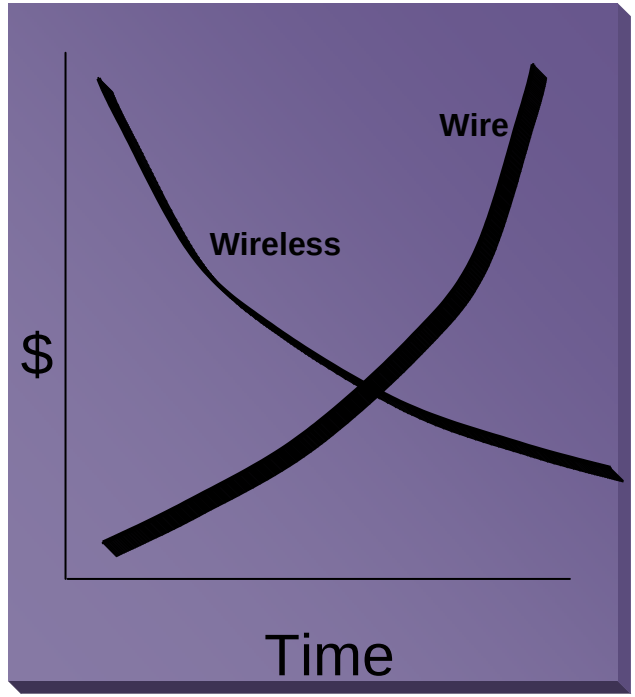
Shipboard Cargo Tracking System

Innovative Technology Base

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

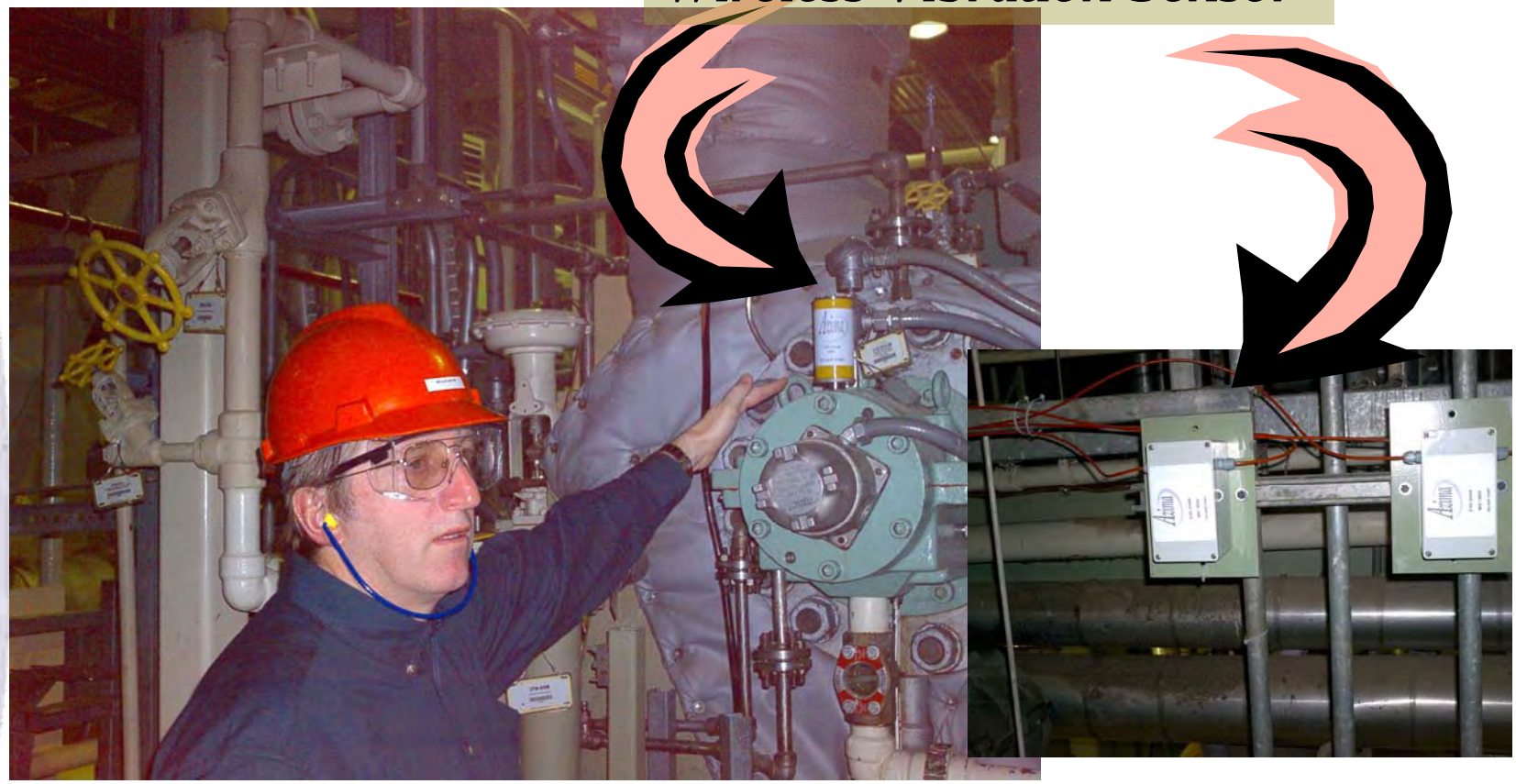
The Genie is Out of the Bottle

- Wire continues to get more expensive – over $2,000 per foot!
- Wireless continues to get cheaper
- $14M installation a hit today
- Market is ready
- Technology is ready
- Matching application to technology is all that remains



Wireless Is Now – In Nuclear!

Wireless Vibration Sensor



Two Guys Making It Happen!

***"CBM is the next killer app for wireless"* – Dr. Jay Lee at the Center for Intelligent Maintenance, University of Wisconsin, Milwaukee – Fortune Magazine, April 2002**

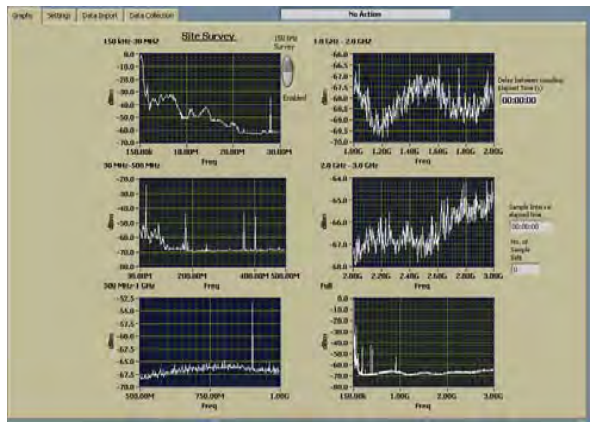
Ramesh Shankar of EPRI & Clinton Carter of TXU Energy

Wave Relay™ Secure Channel Solution

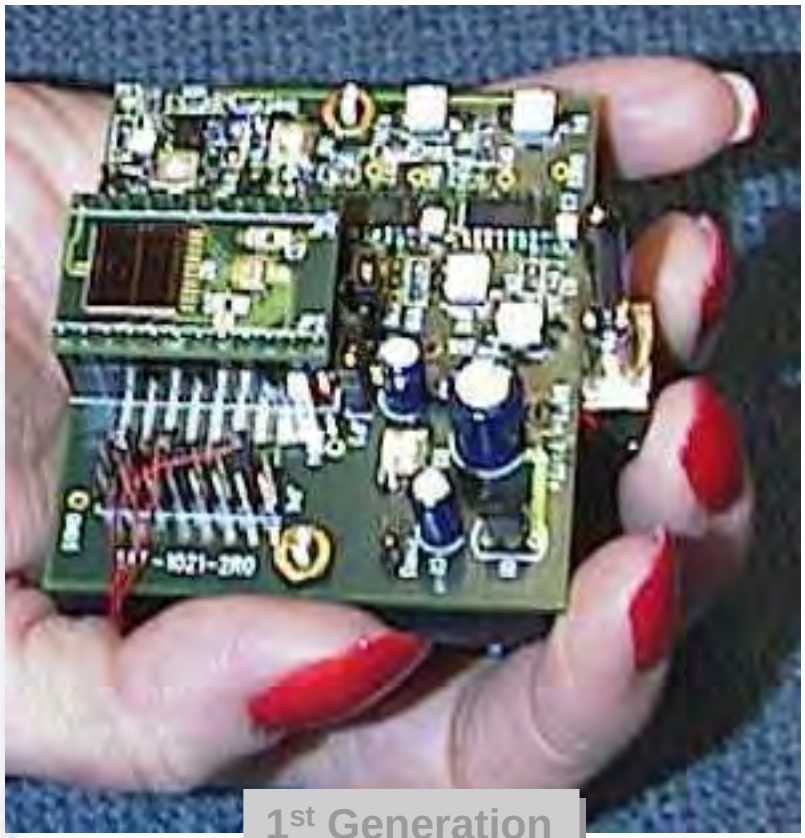
- *Wave Relay* (tm) is a Layer 2 network switch designed for 802.11 a/b/g which provides an ability to secure data and control packets over multiple hops on an end-to-end basis.
- The architecture provides scalable, high performance network capabilities through the use of secure virtual circuits over a wired and/or wireless network.
  - William J. Miller
    President
    Maximum Control Technologies
    a MILLER W J & ASSOCIATES Company
    mact-usa@att.net
    www.mact-usa.com

DOE Strategy Focuses on Supporting Wireless Vision For Industrial Wireless

- **WINA –**
  - Self-sufficient – paying members, end users
  - Standards-based – de facto and de jure
  - Ubiquitous sensing business models – low cost, extensible
- **DOE Projects –**
  - Eaton - Refinery
  - Honeywell – chemicals processing
  - GE – material processing
  - **ORNL's Extreme Measurement Communications Center (EMC²)**
- **Users' Expectations –**
  - Characterizations – RF, environmental
  - Simulation – playback of combinations
  - Qualification – standards and proprietary



Electronic Readout/Telemetry Miniaturization For Wireless Sensors

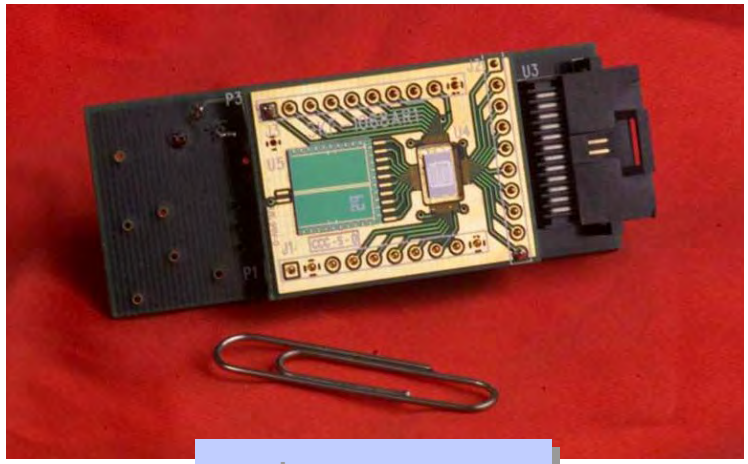


1st Generation

MEMS Readout Telemetry

Present Chip Set

(enlarged)



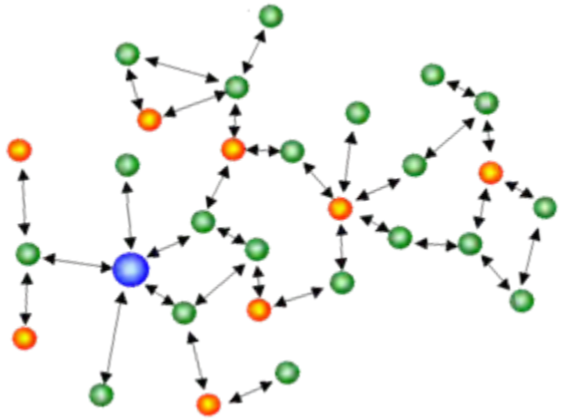
2nd Generation

PROCESS CONTROL SYSTEMS FORUM

Collaborating to Advance Control System Security

Exploiting Defense and Commercial Wireless For Industrial Applications

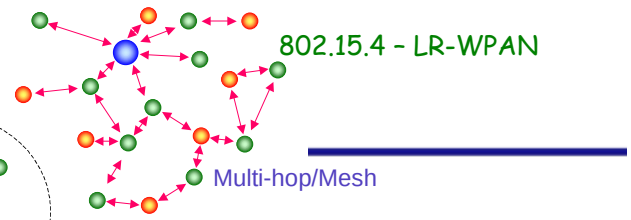
- **Reliability -**
  - Mesh – Billions of $ from DOD
  - Spread Spectrum – FHSS, DSSS, Ultra-Wideband

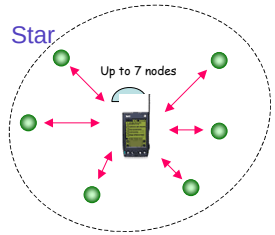


- **Power**
  - Harvesting – vibration, RF, PV
  - Low-power Designs – ASICs, FPGAs, DSP
  - Protocols – Low-duty cycle - ZigBee

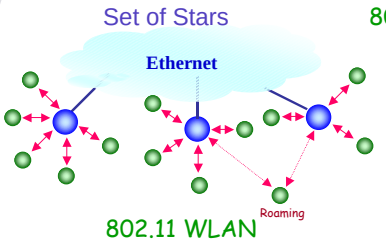
- **Security**
  - Encryption – WEP, AES, WPA
  - Physical – RF layer, FIPS 140-2
  - Integrated – impacts on throughput, latency, reliability

Standard WSN Technology Comparison

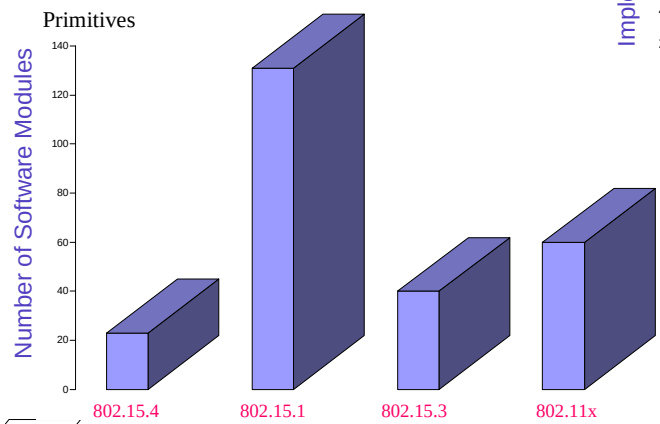


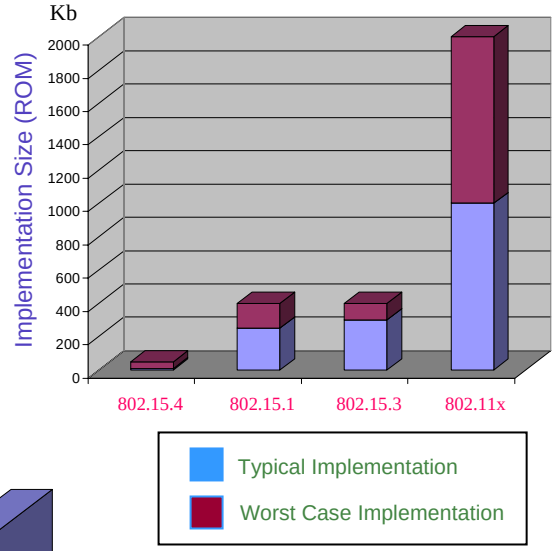


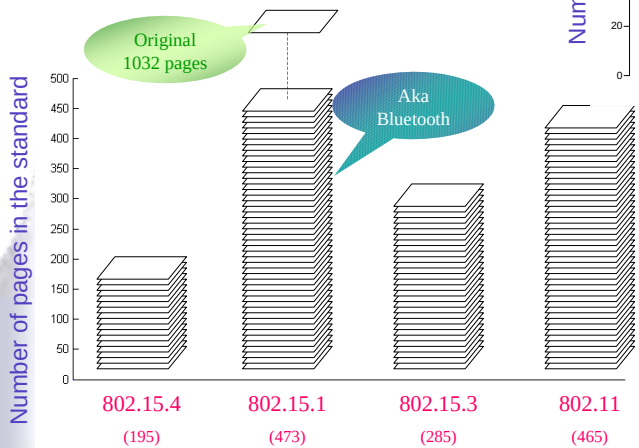
802.15.1 WPAN
(Bluetooth)



802.11 WLAN







	LR-WPAN	Bluetooth ™	WLAN
Range	~100 m	~100 m	~100 m
Data Throughput	0.25 Mb/s 0.04 Mb/s	1 Mb/s	~2-11 Mb/s
Power Consumption	1	1000	5000
Size	Smallest	Smaller	Larger
Cost	1	10	20

Eaton a leader in development of standard wireless technologies for the industrial application space

INNOVATION CENTER

EATON

Partnerships ➡ Solutions in the Field

- **WINA - 19 dues-paying members - approaching self-sufficiency**
- **SP100 – 72 members, end-user co-chair**
- **Sensors Magazine – wireless supplements, website, and Sensors Expo sessions**
- **EMC^2 Facility/Capabilities - $0.75M instruments characterizing sites and components – paid services for non-ITP industries.**

EMC2 Extreme Measurement Communications Center

EATON

Honeywell

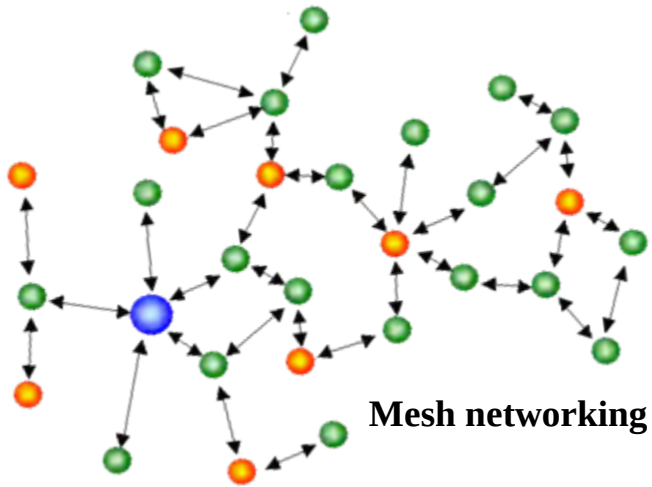
imagination at work

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

DOE Project Next Steps – Deployment Support

- **SP100 – First Draft in 2006**
- **WINA – book, paper, standards – late 2006**
- **Partners – characterization of environments, components, systems**
- **Simulations – improving likelihood of successful deployments – early 2006**

- **Standardized methodology to**
  - Assess environment – light to harsh, RF and other
  - Assess application – latency, throughput, etc.
  - Assess options – technologies, products, standards
  - Assess deployment – initial stability, ease
  - Assess performance – against requirements
  - Maintain – tools, costs, upgrades



Mesh networking topology

WINA

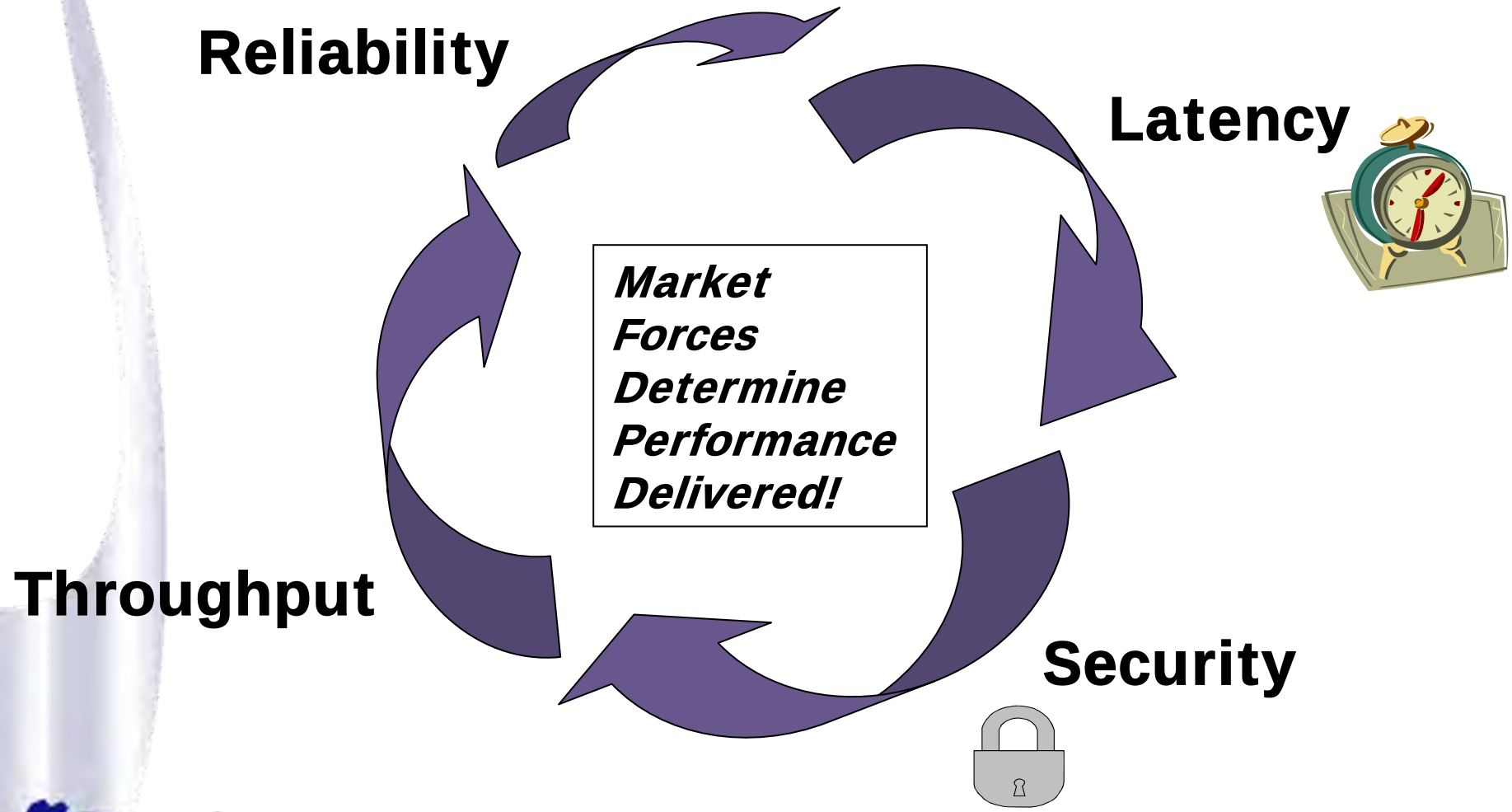
PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Usage classes of wireless data networks

Safety	Class 0 : Emergency action	***(always critical)***	**Importance of message timeliness increases** ↑
Control	Class 1: Closed loop regulatory control	***(often critical)***	
	Class 2: Closed loop supervisory control	***(usually non-critical)***	
	Class 3: Open loop control	***(human in the loop)***	
	NOTE: Batch levels 3 & 4 could be class 2, class 1 or even class 0, depending on function* **Batch levels as defined by ISA S88; where L3 = "unit" and L4 = "process cell"*		
Monitoring	Class 4: Alerting ***Short-term operational consequence (e.g., event-based maintenance)***		
	Class 5: Logging & downloading/uploading ***No immediate operational consequence (e.g., history collection, SOE, preventive maintenance)***		

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Technologies Exploding – Balance Required



PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Encryption Goes Way Back

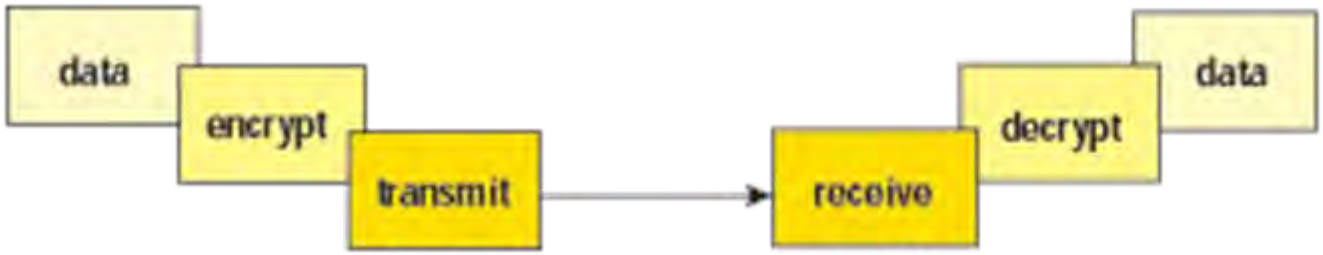


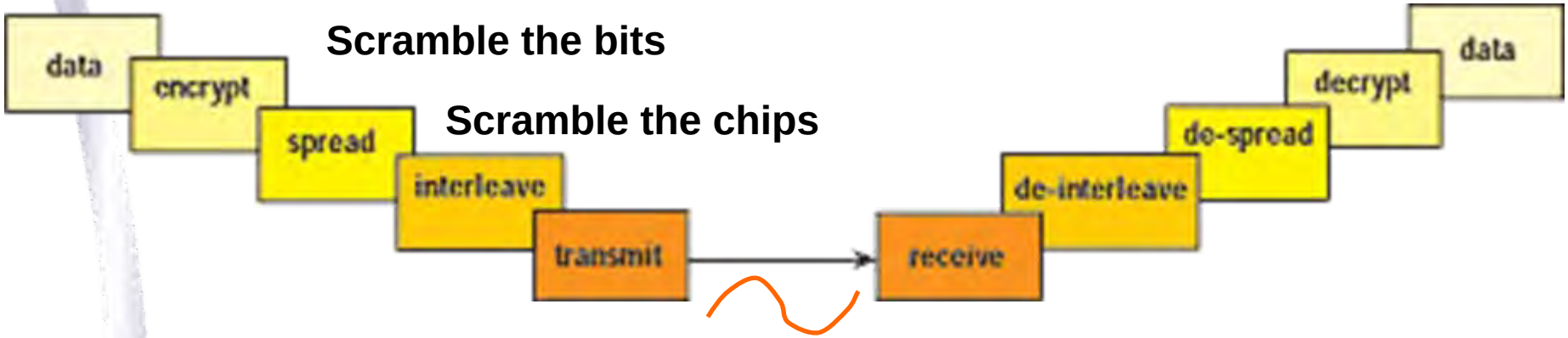
Figure 1. Wired networks normally use encryption as the only weapon against clandestine attacks. This has been effective for many years, but recent attacks are showing that encryption may not be enough.

Wireless Data Security: Encryption, Spreading, Interleaving – 1 for 4 Today

Scramble the data

Scramble the bits

Scramble the chips

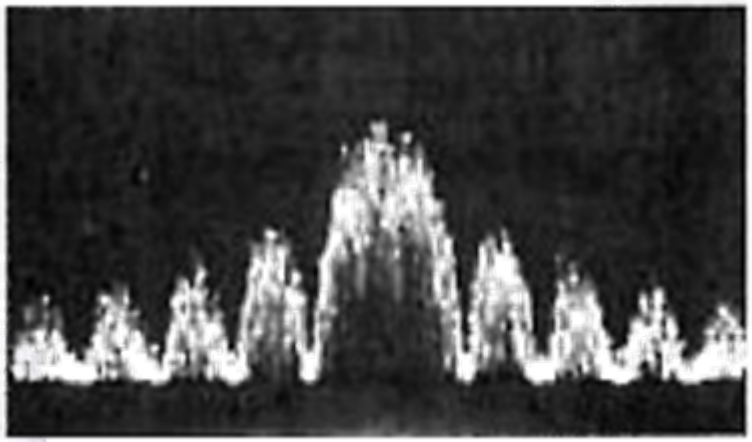


Scramble the radio – Must be present to win; no storage technology available for bad guys.

Wireless networks use a variety of techniques to enhance security, such as spreading and interleaving. These techniques can make the signal virtually undetectable without prior knowledge about the network. This can improve the security of the network by orders of magnitude.

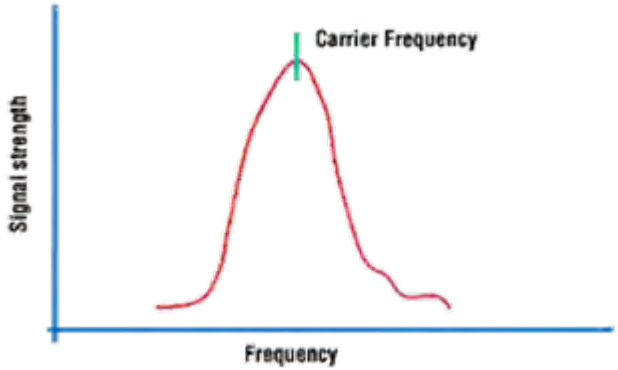
PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Narrowband? Spread Spectrum (what flavor) ?



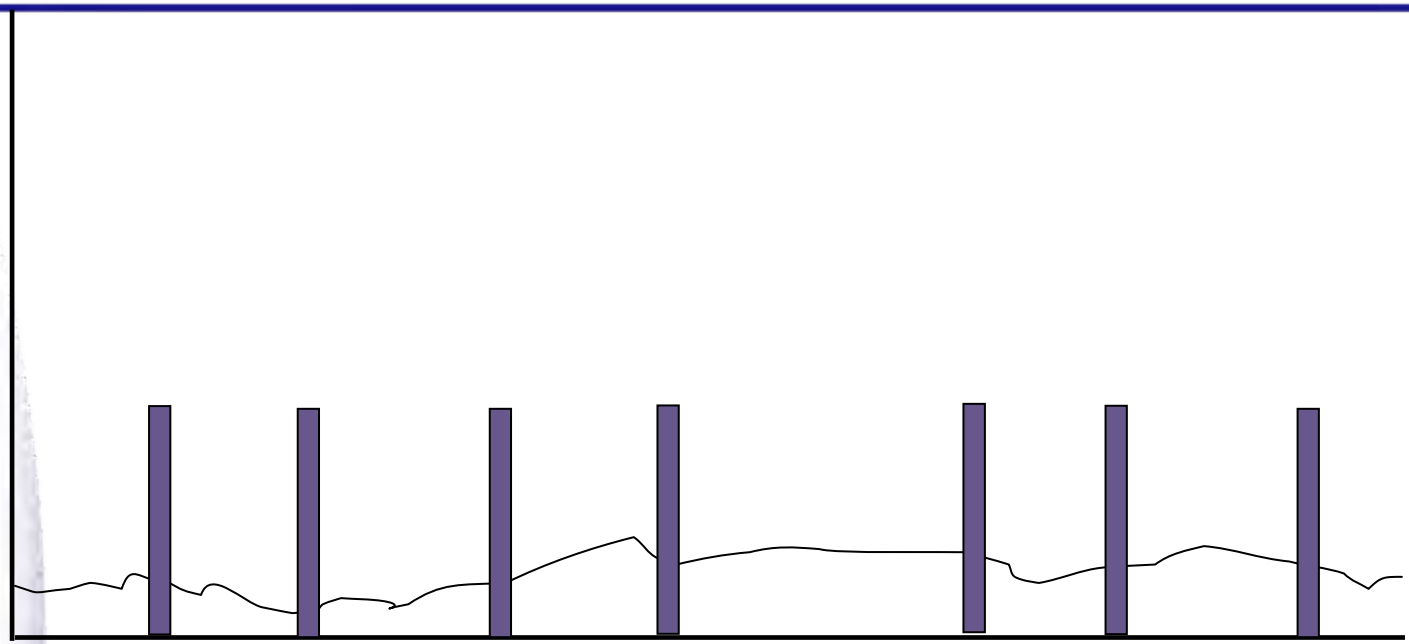
DSSS

FHSS



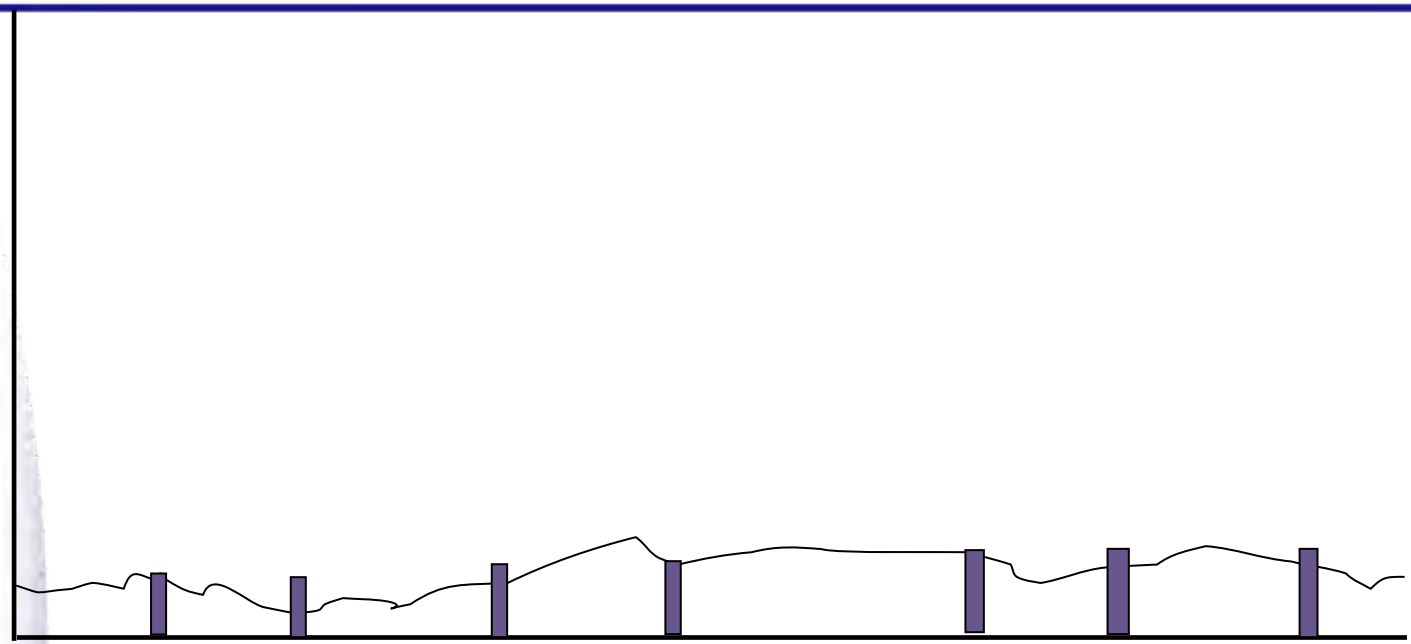
NarrowBand

Secure Wireless – In the Noise!



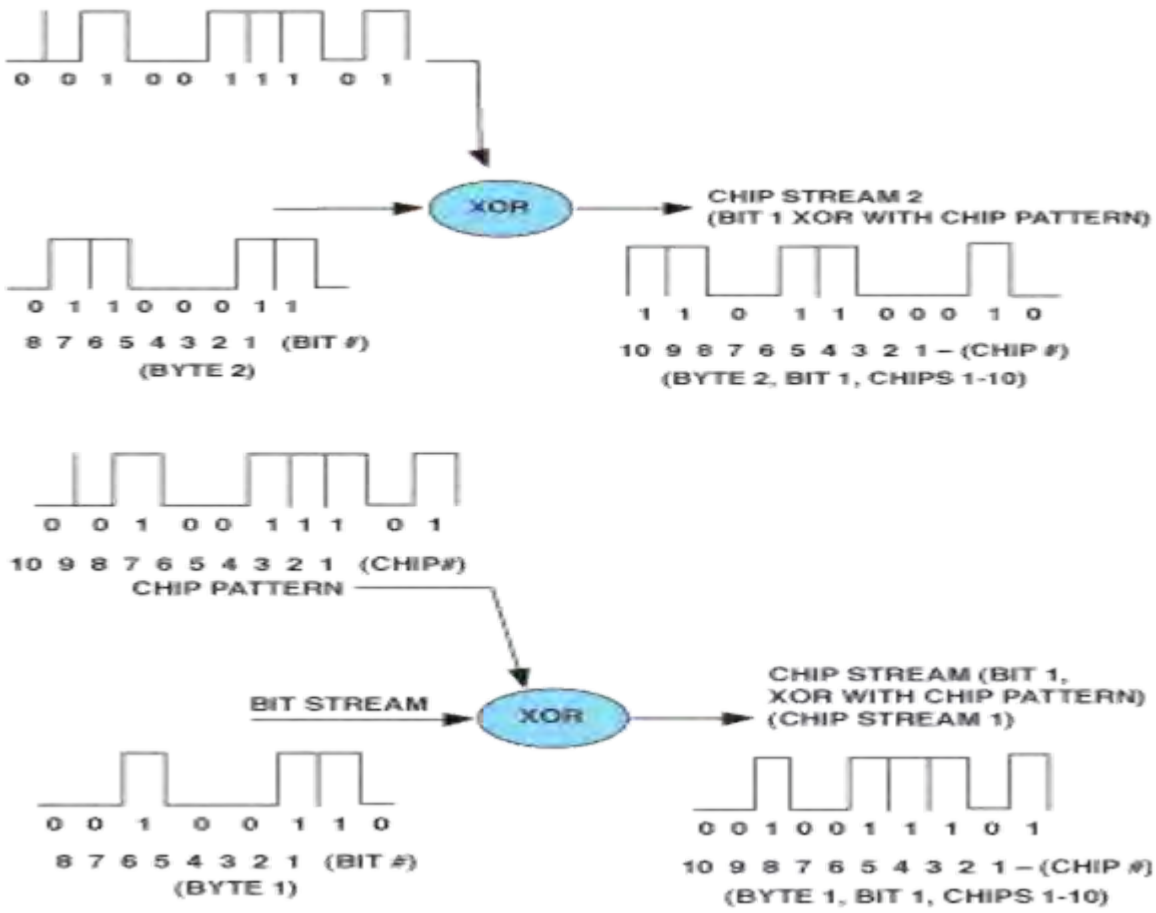
- Chips Visible in Frequency Domain but not Time Domain on Spectrum Analyzer

Secure Wireless – In the Noise!

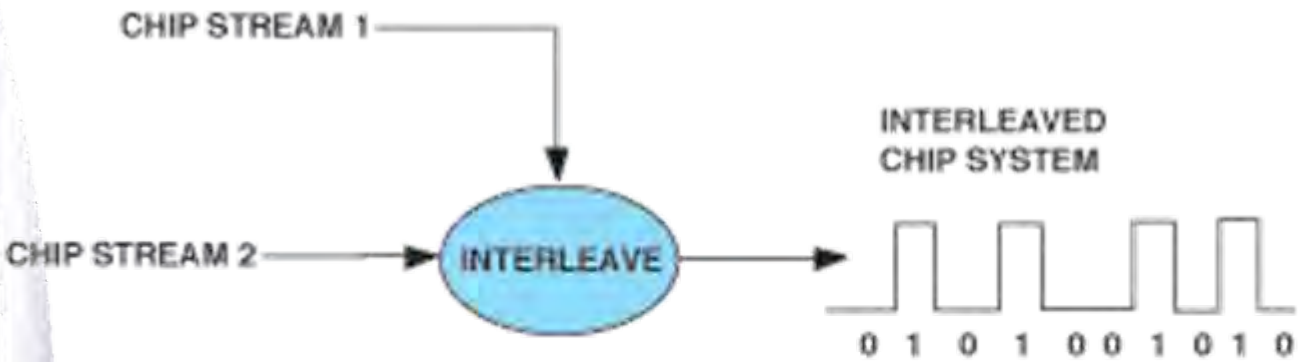


- If each chip represents a fraction of a bit – the bit will pop up when energy summed. – Spectrum analyzer sees just noise!

Base Band Processing Options Improve Security



Interleaving – More Security



2-1-3, 1-1-5, 2-1-1, 1-1-3, 1-1-7, 2-1-8, 2-1-10, 1-1-10, 1-1-1, 2-1-1

INTERLEAVED CHIP SYSTEM = (BYTE # -BIT #-CHIP#)

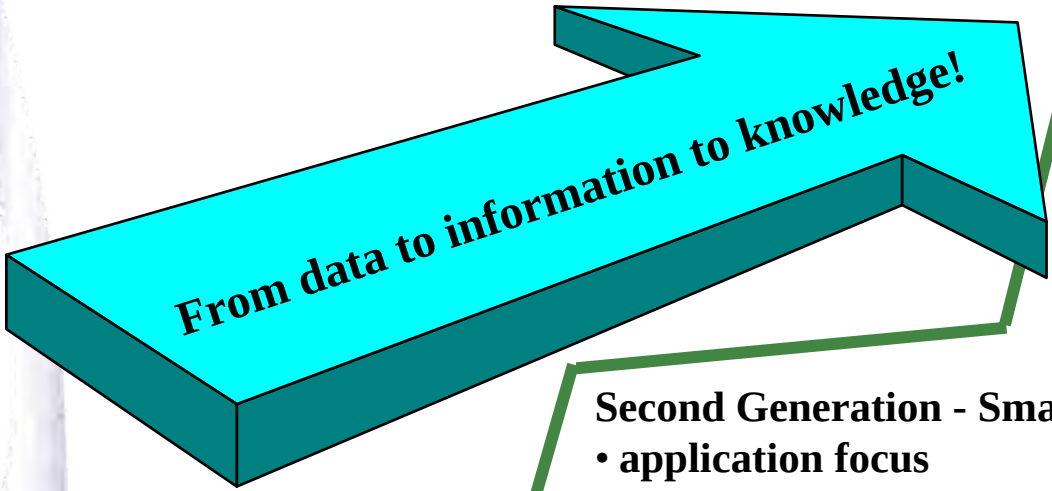
Figure 3. Interleaving improves wireless sensor network robustness and security. The complexity of interleaving discourages its widespread use, but new integrated circuits are making this a more viable alternative.

Wireless Enables Ubiquitous Sensing!

- A Completely New Paradigm!
  - **Efficiency**
  - **Safety**
  - **Asset Management**
  - **Hostless architectures**

The Sensor IS the Network!

What Is The Next Generation?



Third Generation - Sensor Agents
- goal focus
- dynamic architecture
- network intelligence

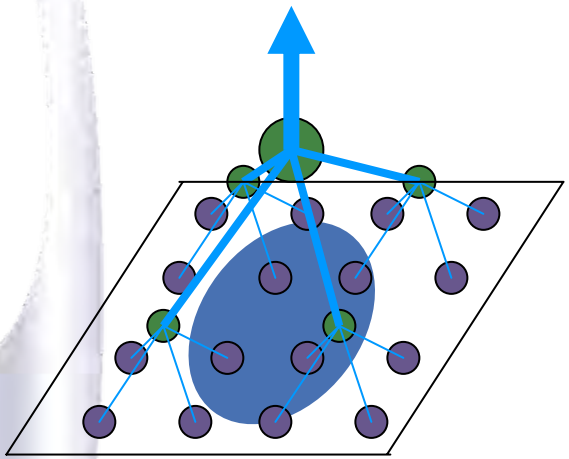
Second Generation - Smart Sensors
- application focus
- hierarchical architecture
- local intelligence

First Generation - Dumb Sensors
- data focus
- flat architecture
- no intelligence

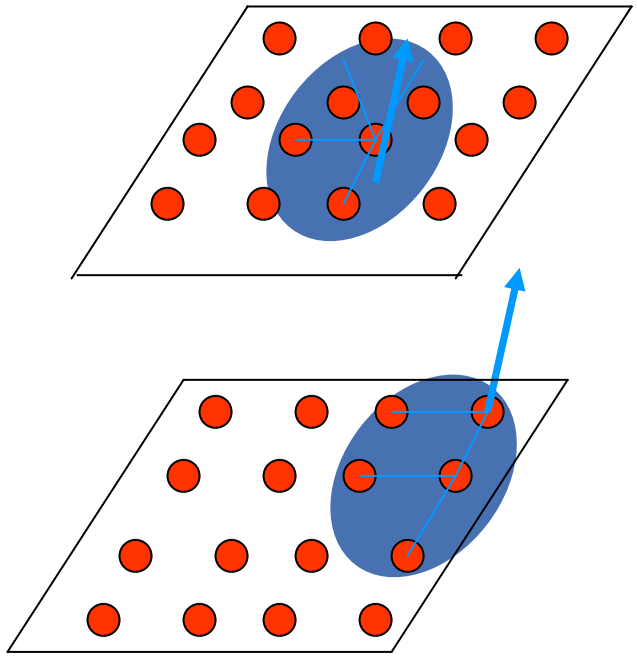
PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

How Will You Know It When You See It?

Present-day systems have fixed hierarchy

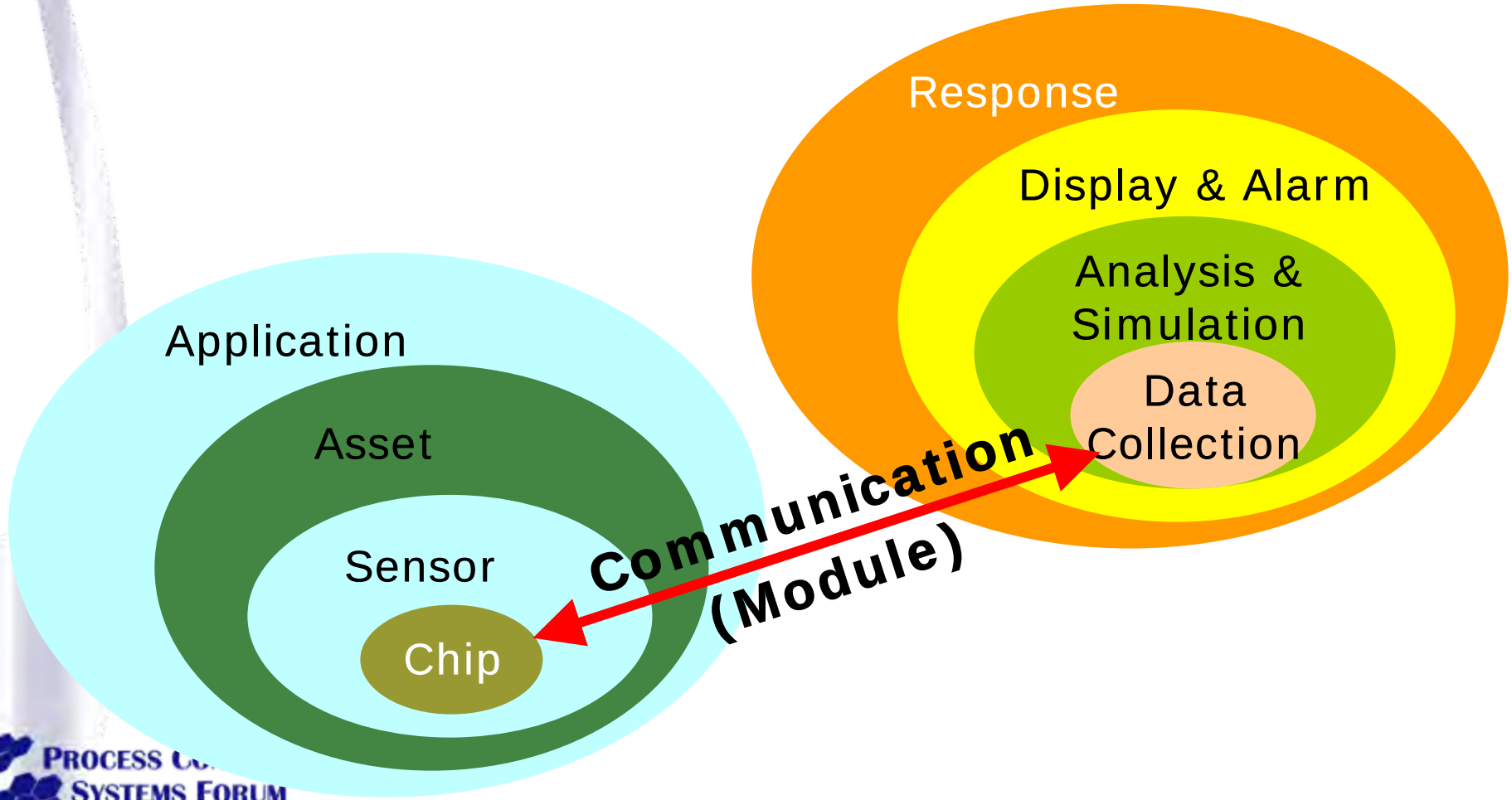


Next generation network will self-organize in response to specific events



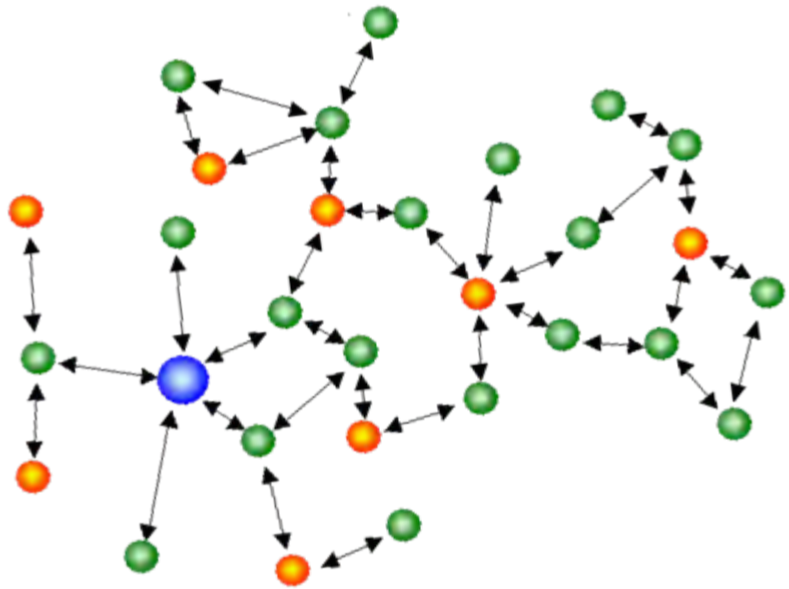
PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Replacing the Wire is Only the First Step!



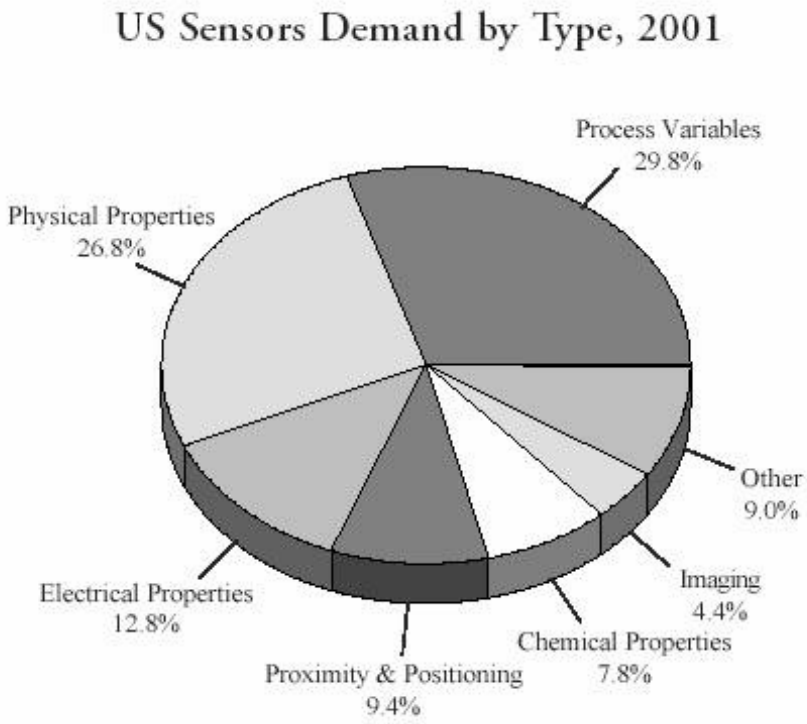
The Sensor Is The Network? – Not Yet

- Cell phones are not mesh-based
- IEEE 802.11b is not mesh-based
- ZibBee (based on 802.15.4) is mesh-based



Why Not Just Let the Market Decide?

- Beta Vs VHS – I still have Beta HiFi on my set top and it's still better!
- Ethernet on the factory floor – Took 20 Years to get the performance required!
- Fragmented Market not Appealing – We hang together or we hang separately?



Freedonia Group report on Sensors, April 2002

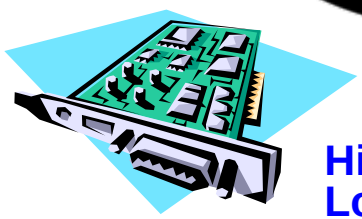
Can Commercial Grade Cut It?

Wireless
Sensor Network

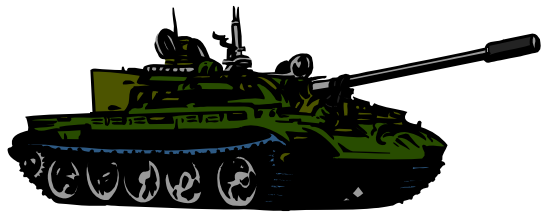
Government Labs
Academia
Industry/Consortia

Consumer Market
High Quality
High Volume
Low Cost
Low Integrity

Manufacturing/ Industrial Markets
High Quality
Low Cost
High Volume
High Integrity



National Defense
High Cost
Low Volume
High Quality
High Integrity



Wireless
Warrior

Strong Relationships with ISA & Sensors

SIGNALS SIGNALS SIGNALS SIGNALS SIGNALS

Home | Directory | Calendar | Discussion Forums | ISA Home | Login | Logout

Home
Conference
Calls
Meetings
Resources
Drafts

Print this Page

List of Standards for Committee

ISA-SP100, Wireless Systems for Automation

A Word from the Chairman

In working to assure confidence in, and the integrity of, wireless technology, and to provide criteria for implementation in manufacturing automation and control systems, the ISA-SP100 Committee recently launched four project teams. Each team's goal is to develop documents that will help users make the right decision on industrial wireless implementations.

The first project team will develop an educational technical report that covers the basic concepts of radio transmission—the physics of radio. The report will cover free space communication of a transmitter and receiver under ideal conditions; address real earth propagation effects such as moving objects or multiple path communication; and deal with issues such as interference related to sharing the license-free band spectrum with others. This technical report will provide new users with a better understanding of the choices and tradeoffs offered with wireless applications in industrial environments. For more information on this activity or to volunteer, please contact Ake Severinson, (800) 663-8806, ake@omnexcontrols.com.

To address the many levels of industrial environments, ranging from the benign to the extremely harsh, the second project team will develop an industrial wireless requirements document. Based on a USDoE-funded program involving Eaton, General Electric, and Honeywell that collected data on customer wireless requirements, this document will cover wireless applications, such as monitoring and control, and will develop a taxonomy of wireless automation networks. The team's objective is to provide end users with a better feel for where their application fits in the overall industrial environment hierarchy. For more information on this activity or to volunteer, please contact Tom Phinney, (602) 313-5989, tom.phinney@honeywell.com.

The third project team will develop a technical report that covers interoperability issues and how sensor networks should interact in an industrial environment. While some of these issues will be addressed in the requirements document, this report will examine co-existence and performance in greater depth. Work is currently underway within this project team to develop a matrix identifying levels of interoperability and providing the rationale for their use. For more information on this activity or to volunteer, please contact Bill Drake, (301) 944-1300, bluelynxwireless@yahoo.com, or Peter Fuhr, (831) 588-7558, peter.fuhr@apprion.com.

The fourth project team will create a "User Guide," providing sufficient guidance to allow users to deploy and use wireless networks in an industrial environment. The guide is intended to be comprehensive, not only helping users achieve a wireless solution but also assisting them in making the right decision on their wireless implementation through tools such as a "buyers' checklist." For more information on this activity or to volunteer, please contact Wayne Manges, (865) 574-8529, mangesww@ornl.gov, or Anoop Mathur, (612) 951-7734, anoop.mathur@honeywell.com.

Wayne Manges
ISA-SP100 Committee Chair

Growth Forecasts

New Capabilities

New Positioning

sensors online

sensors expo & conference

Sensors magazine
Current Issue
Past Issue Index
Wireless Sensors
Subscriber Services

Problem Solvers
Sensors Express
Sensors Buyer's Guide
Wish List
SpecSearch®

Other Resources
Industry Links
Events Calendar

Vendors
Reader Service
Literature Showcase
Product Mart

Inside Sensors
Advertising
Contact Us
Home

SEARCH
GO
Entire Site

See who won!
BEST OF sensors expo DETROIT 2004

Best of the Web

Biodetection Technologies 2005 Baltimore, MD

DATAFORTH Isolated Signal Conditioning Quick Shipment-Modular or Din Package

Wireless Sensors

The publishers of *Sensors* launch *Wireless Sensors* in 2005!

For a **free subscription** to *Wireless Sensors*, click here.

For advertising opportunities please click here.

Wireless for Industry

In 2004, *Sensors* published two Wireless for Industry supplements. Sponsored by the Wireless Industrial Networking Alliance (WINA), the publications focus on wireless sensor networks of all stripes for industrial use. For 2005, we expand our coverage of wireless sensor networks beyond industrial applications to include medical, asset tracking, and more.

Sensors Covers Wireless

Here's a sampling of articles *Sensors* has done on wireless data communications. We hope you find them helpful. Need further assistance? Contact us: sensorswireless@advanstar.com.

- Wireless Sensors—Buyer Beware
- Standards-Based Wireless Networking Alternatives
- Is Wireless Ethernet Safe to Use?
- Using Wireless Sensors to Measure Gaps Efficiently
- Wireless Sensor Network Topologies
- Secure, Low-Power Operation of Wireless Sensor Networks
- Reducing Scrap with Wireless Data and Power
- How Secure Is Secure?
- Meet the ZigBee Standard
- Power Considerations for Wireless Sensor Networks
- The Sensor Web: A Distributed, Wireless Monitoring System
- Battery Power for Remote Wireless Sensors
- MICA: The Commercialization of Microsensor Motes

Wireless Sensors
1st Quarter 2005

Wireless for Industry
Special Supplements
Fall 2004
Summer 2004

SENSORS The News You Choose EXPRESS
NEW PRODUCT INFO
- Select -

May 30, 2005

Industry News
Updated Twice Weekly

- Carbon Nanotubes Already Impacting Sensing
- HART Plant Of The Year Nominations Due June 30
- Sypris Offers Uncertainty Measurement Training
- Center for Electro-Optic Sensors Being Investigated
- New Launch Part of PerkinElmer's Home/Car Strategy
- Phoenix Contact Unveils New Infomobile
- more news ...

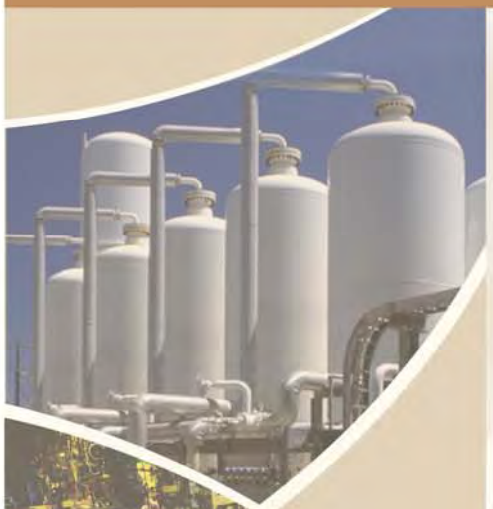
TechWow! Special Issue

Resources
- Business Sense
- Online Exclusives
- Sensors Express
- Web Picks
- Wish List

CELEBRATING 20

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Accelerating the adoption of wireless technologies in industry



WINA

WIRELESS INDUSTRIAL NETWORKING ALLIANCE

ISM frequencies

ZigBee™ 802.11 a/b/g

802.15.4

spread spectrum

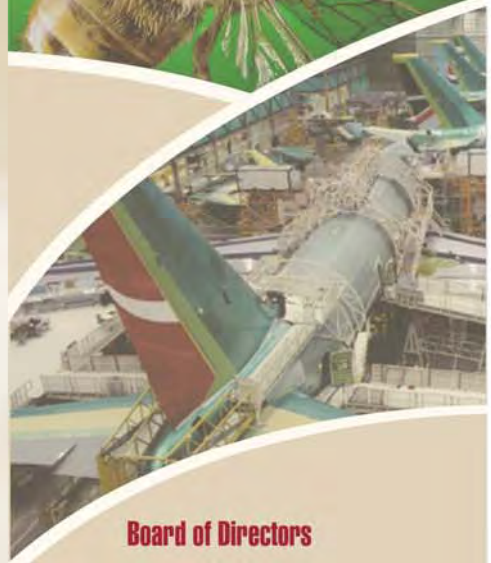
UWB

1451.5

cyber-security

Bluetooth®

WWW.WINA.ORG



Board of Directors

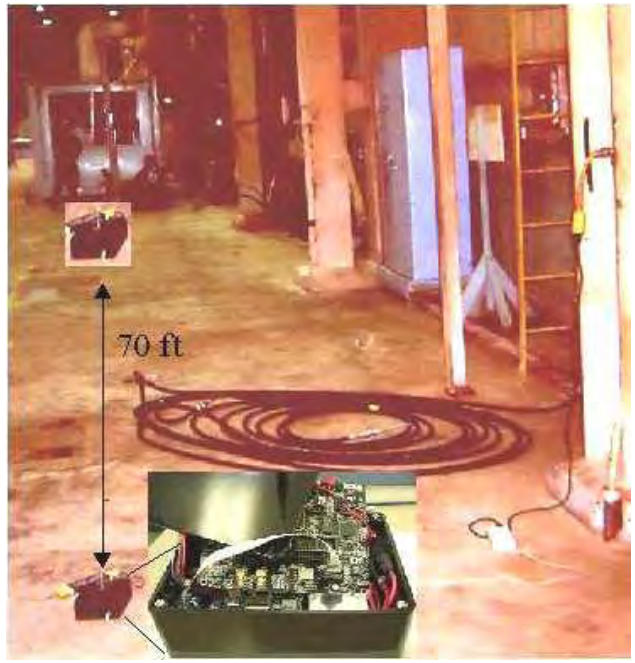
- 3e Technologies International
- Eaton Corporation
- Ember Corporation
- Honeywell International
- Invensys
- Oak Ridge National Laboratory
- Omnex Controls
- RAE Systems
- ZigBee Alliance

Risks Remaining – Be Careful!

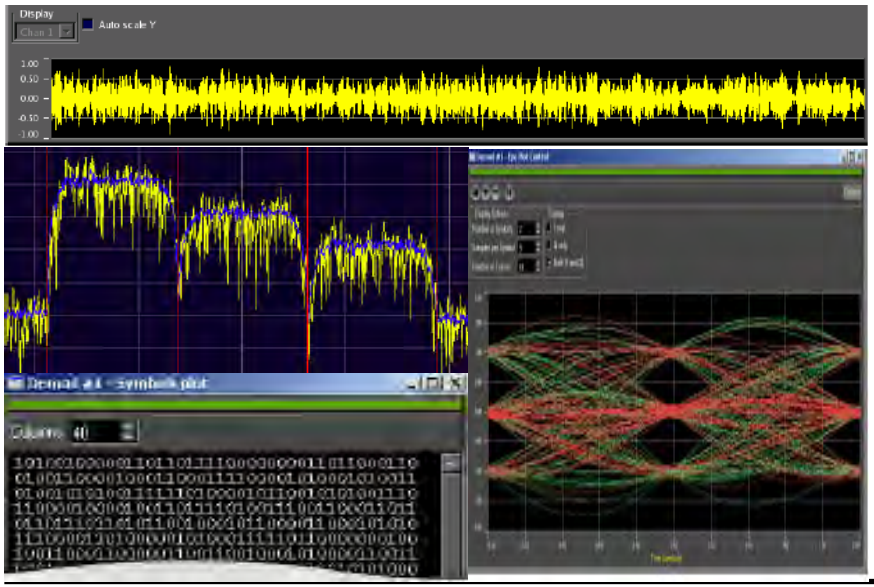
- Technical – security, latency, reliability
- Commercial – acceptance, cost, marketing
- Political – assumptions of either too hard or too easy

Solving a multi-disciplinary problem!

- Wireless – radio, packaging, antenna
- Industrial – harsh environment, fault tolerant, safety related, cost
- Sensor – filters, sampling, sensitivity, interferers, controls
- Networks – real-time, latency, throughput, security, integrity, vertical integration



Extreme Measurement Communications Center (EMC²)



Operational Capability

The DoE EMC² provides modeling, simulation and characterization support for industrial wireless networks.

This facility is equipped with parallel computing resources as well as state-of-the-art measurement equipment for high performance wireless and wired network characterization from the physical layer to the application layer

Broadband RF record and playback instrument can simulate and generate characteristic waveforms to help in-lab study of the wireless device's behavior in harsh industrial environments

EMC² Program Benefits:

- EMC² formalizes the testing of industrial wireless networks to quantify the latency, throughput, security and fault-tolerance (Interference and Noise)
- Wireless Industrial Networking Alliance (WINA) has accepted EMC² as its product testing and characterizing center to member companies
- Currently supports exhaustive modeling and simulation of the communication infrastructure for future electric grid
- Help develop or improve existing standards in industrial wireless networks to include measurement, verification and reliability of network and device parameters
- The center is being developed both as a user facility and an on-site testing provider using portable test equipment

Milestones, Deliverables, & Contact:

Key Milestones: Alliance with WINA and member companies for technology assessment and characterization; Provides modeling and simulation support for developing fault-tolerant electric-grid communication infrastructure

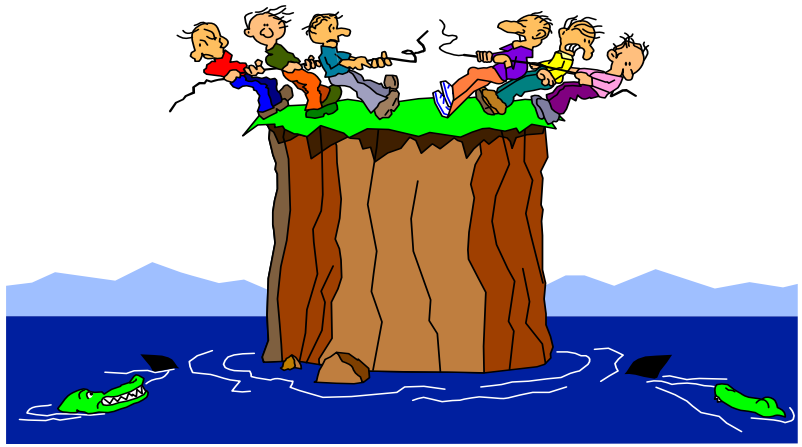
Deliverables: Standards-based report generation for different wireless devices and network layouts; Software development for characteristic network testing;

Contact Information:

Wayne Manges
mangesww@ornl.gov, 865-574-8529

Can We Get There From Here?

- **Standards – for industrial applications**
- **Markets - attractive**
- **Confidence - successes**
- **Tools – easy, handy**
- **Information – broad-based, clear to users**



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