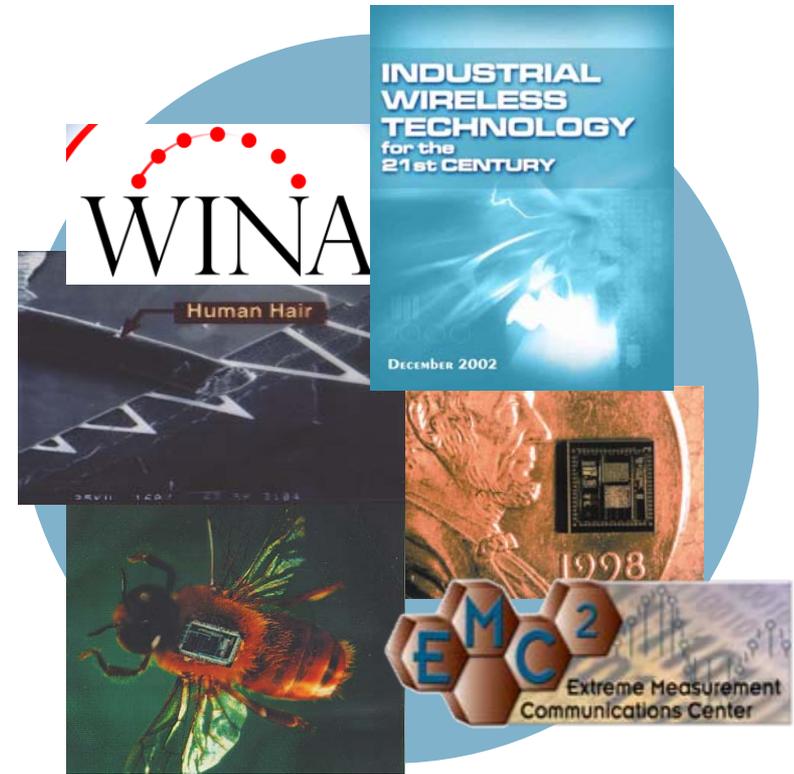


# Wireless Security – An Oxymoron?



## Control Systems Cyber Security Conference August 13 - 16, 2007

Wayne W. Manges

Oak Ridge National Laboratory

Extreme Measurement Communications Center

August 14, 2007

# Early Adopters – Blazing the Wireless Trail!



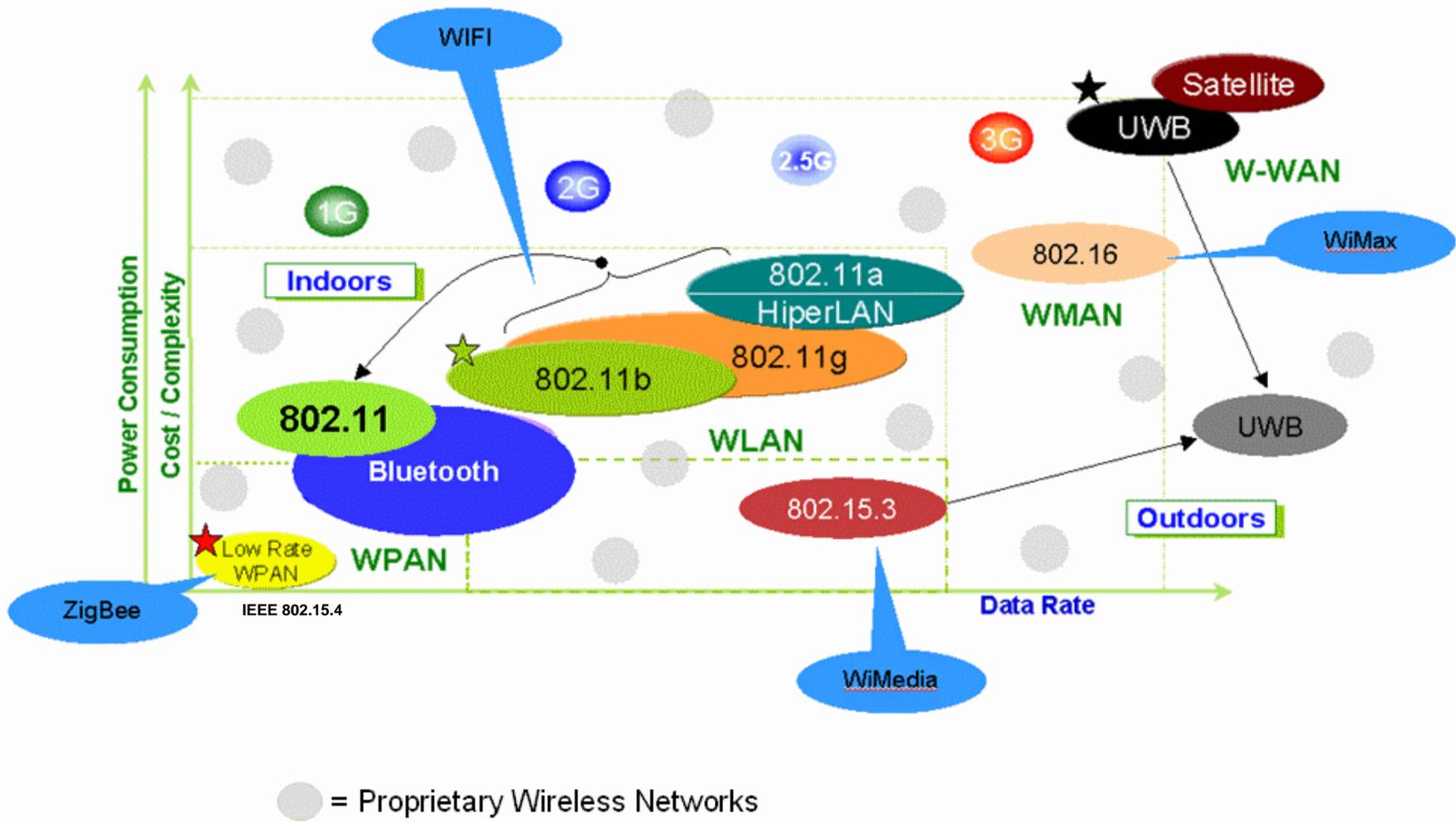
# Why Here? Why Now? Why Us!

- **It's a Hard Problem!**
  - It's interdisciplinary
  - It's the new guy
  - Much emotion surrounding issues
- **But Not Too Hard!**
  - Other People's Money – government, commercial, private
  - Successes Emerging – Comanche Peak, one-day ROI!
  - Standards emerging – ISA, others
- **Why Now?**
  - Still failures,
  - Still can be costly,
  - Expectations are high,
  - Standards slow to emerge
- **Impact! – Moving Forward**
  - Guidelines – Physics of Radio
  - First Release – ISA100.11a
  - Follow-on Releases – Users' Guide, Discrete Manufacturing, RFID, ...



*One of the reasons we're all here!*

# The Wireless Landscape – No Single Security Solution



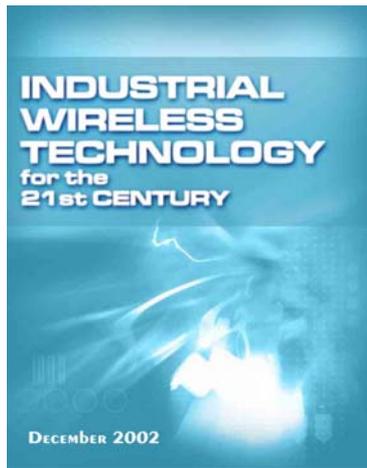
# Why Do We Care? It's The Benefit – Stupid!

- **US Government – Committee of Presidential Advisors** quoted “10% savings in energy and 15% reduction in emissions” with wireless sensors
- **Market – Estimates of \$4B per year** are called “conservative”
- **End Users – Wire costing over \$2,000 per foot** in some installations
- **Technologies – Radios, Protocols, data handling, security – wonderful problems for engineers to solve**



© Scott Adams, Inc./Dist. by UFS, Inc.

# Wireless Security – Potentially Better Than Wire?!

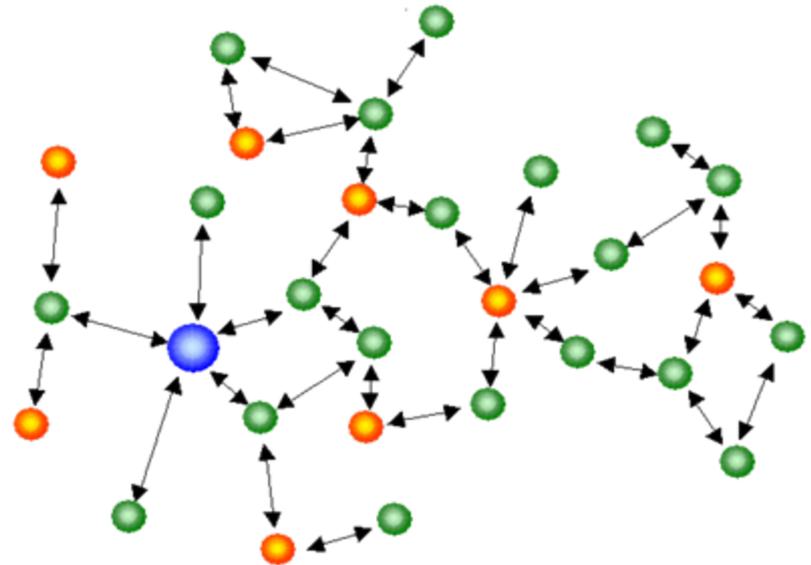


- **Marketing – sell what I have, bandwidth is king**
- **Emotion – “Wireless scares me, I can’t control it!”**
- **Incompetence/Laziness – Too difficult to configure, too big a learning curve**
- **Cost/Benefit/Risk – ROI in a day, why bother?**



# You Want Me To Put My Money Where?!

- Banks – slow to catch on; crash of '29 even more bad Karma
- Microprocessors – Software? How do I prove it?
- Seat Belts – Cars now need six air bags!
- Ethernet – “It will never make it to the factory floor, it’s not deterministic!”



*Wireless Enables a New Topology – Mesh!*

*“There is no business case for wireless! Why are we even discussing it?” – Power Engineer at PCSF 2007*

# Balancing Performance Is Critical To Success

## Reliability

(Not BER,  
Not Accuracy)

## Latency

End-to-end? Or  
Node-to-node? One-way?  
Round-trip?



*Market  
Forces  
Determine  
Performance  
Delivered!*

## Throughput

Bits-per-second or Goodput?  
End-to-end?

## Security

Performance Based?  
Procedure Based?  
Proprietary or Open?



# Wireless Industrial Sensor Networks – Pick Any Four!

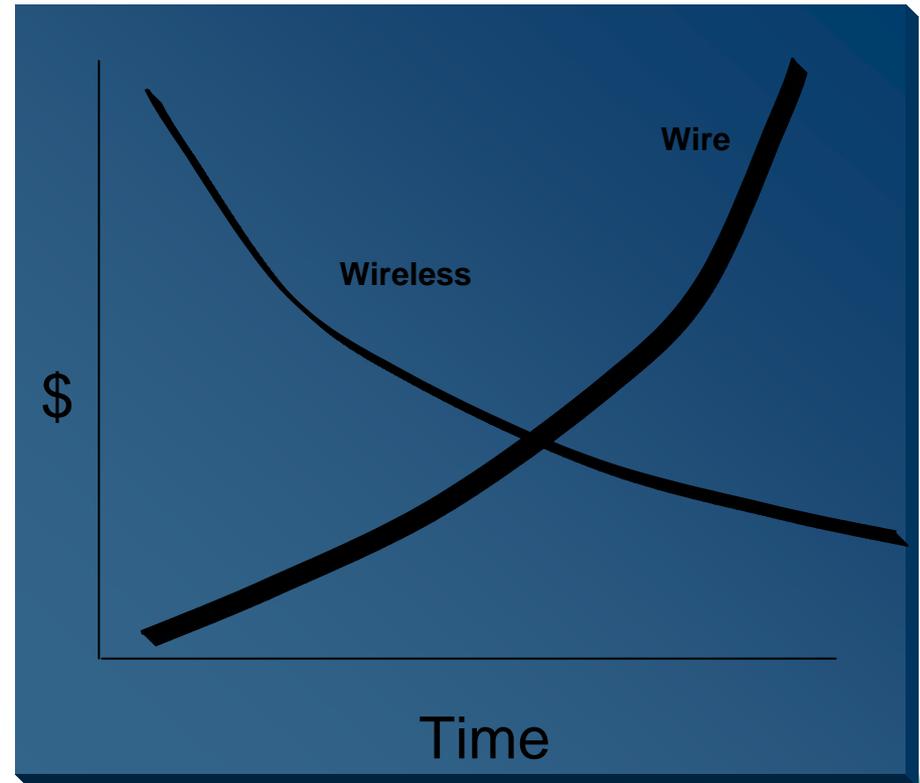
- **Wireless – radio, packaging, antenna**
- **Industrial – harsh environment, fault tolerant, safety related, cost**
- **Sensor – filters, sampling, sensitivity, interferers, controls**
- **Networks – real-time, latency, throughput, security, integrity, vertical integration**



*Any viable approach must address all four aspects!*

# Bill Gates Continues to Teach Us About Quality

- **MAP – GM once needed dual, redundant Modicon 584's; Now PCs running PLC emulators**
- **Risk/Benefit/Cost – Metrics Needed to Enable Good Decisions**
- **Moore's Law - Coming to Sensor Networks?; Industrial Controls?**
- **Performance – Can higher throughput hide a multitude of sins?**



# ISA Got The Call!

- An international nonprofit member association of 30,000+ automation professionals engaged in the design, development, production, and application of devices and systems that sense, measure, and control industrial processes and manufacturing operations.
- Provides professional education and training, certification, conferences and exhibits, and book and journal publications.
- Accredited by the American National Standards Institute (ANSI) to develop industry standards in key areas including process safety, control system cyber security, enterprise-control system integration, engineering documentation, and wireless systems for automation (ISA-SP100).
- Headquarters: Research Triangle Park, NC. Visit [www.isa.org](http://www.isa.org).



# ISA100: Wireless Systems for Industrial Automation

## *Developing a Reliable, Universal Family of Wireless Standards*

- Backed by ISA Expertise, Heritage and History
  - Nearly 30,000 Members with 140 Standards Committees using an Open Standards Development Process **Accredited by ANSI**
  - Estimated at **~1 Billion Products** Using ISA Standards Technologies
  - ISA 100 **Designed by Experts** in Wireless, Security, and Instrumentation Technologies with Direct End Users Involvement on Committee
- Family of Standards: One-Stop Standardization
  - Designed to **Accommodate all your Plant Needs**
  - Areas of Coverage Identified to Date; Process Automation (Process Focus), Factory Automation (Discrete Focus), Transmission and Distribution (Long Distance Focus), RFID (Industrial Tagging Focus)
- Universality: The Power of One
  - Allows **Deployment of a Single, Integrated Wireless Network**
  - Bring Simplicity to your Work with:
    - One Technology to Learn, Maintain and Operate
    - One Security System to Manage
    - One Set of Infrastructures
- Co-Existence: Providing Peace of Mind
  - Designed with Co-existence features
  - **Ensures Best Possible Performance**

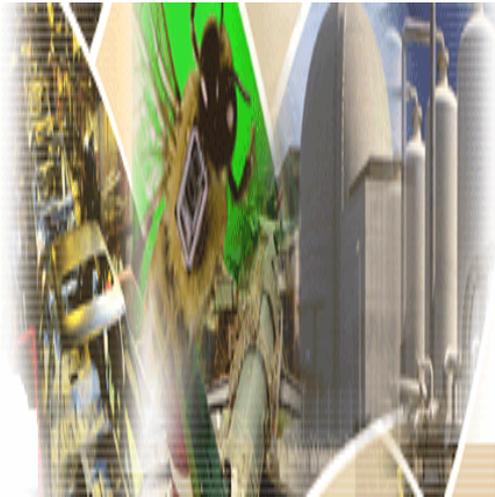
# Standardization Process – From ISA

- **Consensus Driven – progress not stagnation**
- **Structured – controls chaos, alligators, firestorms**
- **Proven – established over years**
- **Flexible – supports our parallel approach to rapid progress**



# Standards – Results Focus

ISA100 efforts will result in standards, recommendations, and technical reports focused on assuring successful wireless deployments in industrial environments

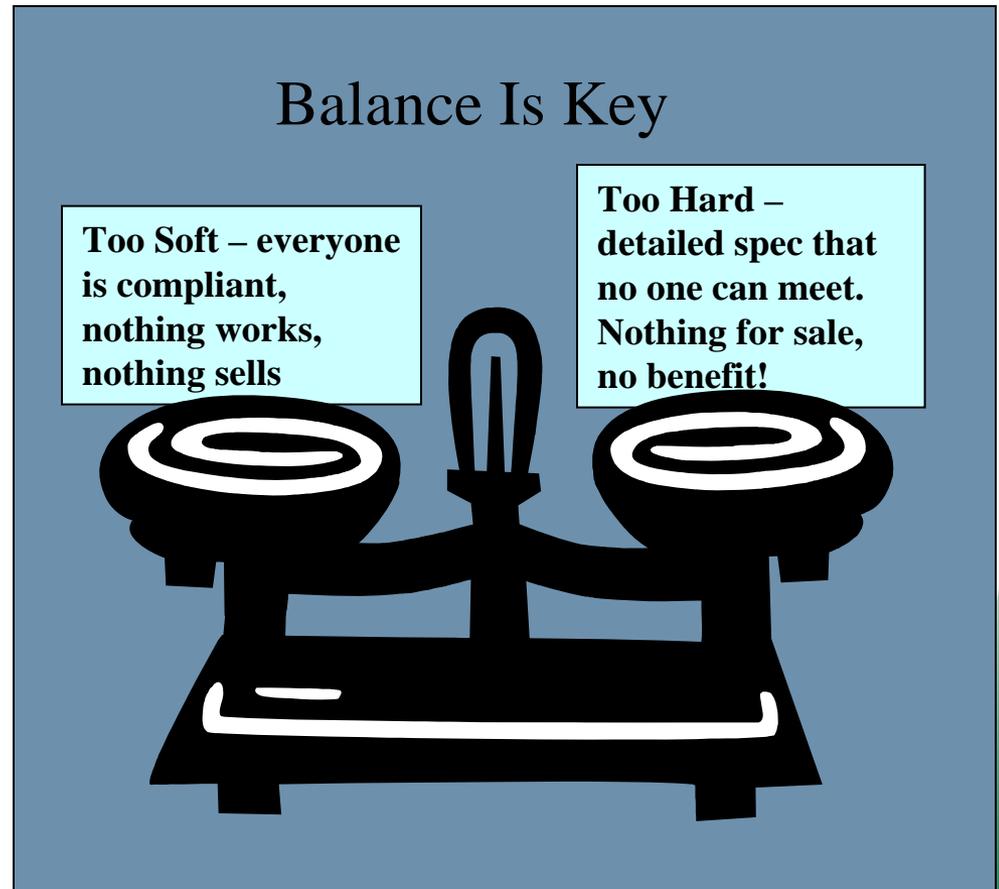


- ISA100 Compliance will assure:
  - Supplier specifications are consistent and easy to interpret
  - User requirements are succinct, relevant and easy to interpret
  - Options are clear and easily differentiable
  - Probable outcomes are quantitatively evaluated against options

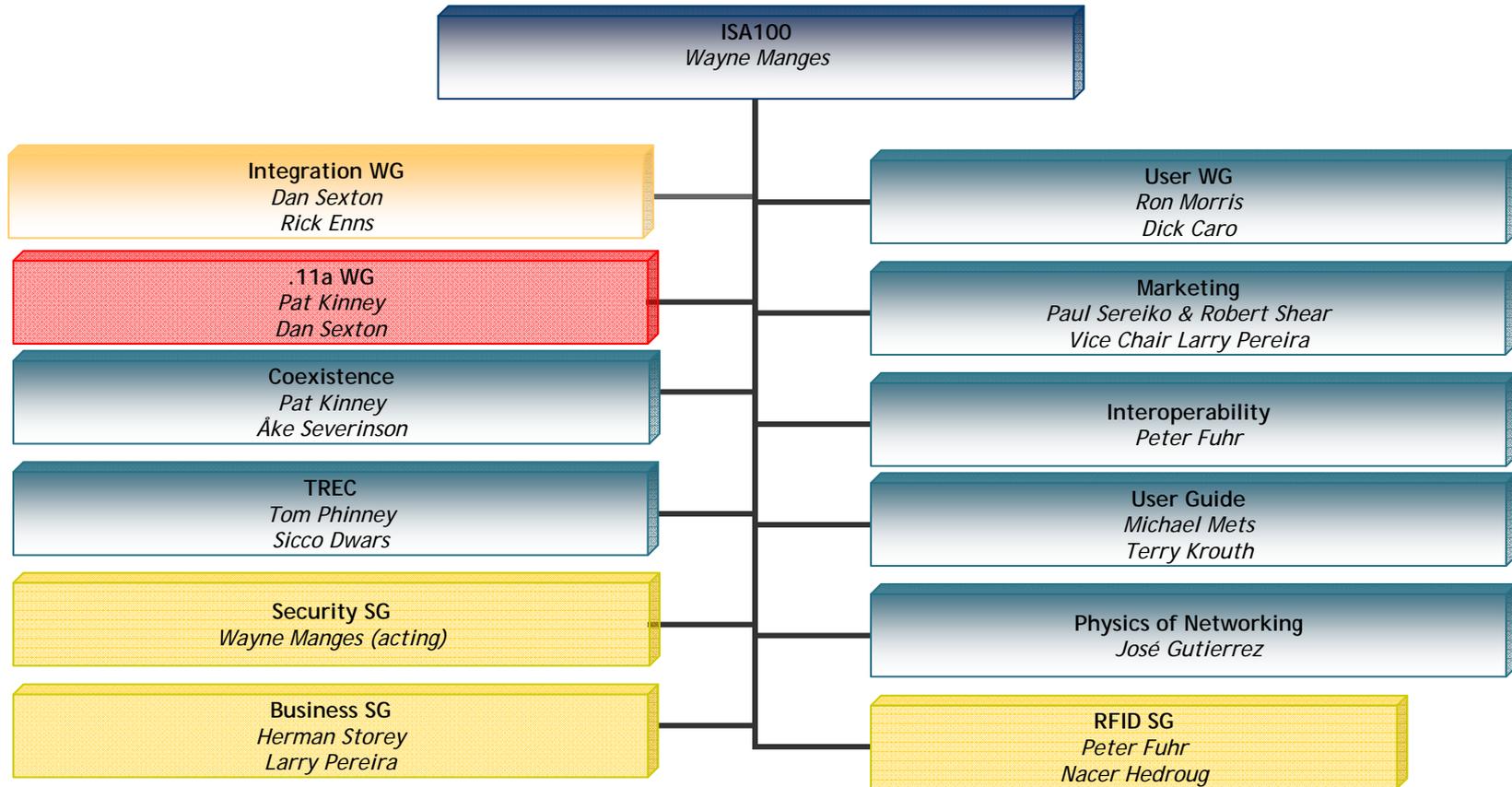
# ISA100 - Success Oriented

ISA100 efforts will leverage other standards, as appropriate, to produce a relevant result in as short a time frame as possible

- ISA100 leverages
  - ISA99 – Security
  - IEEE 1451 – Smart sensor
  - FIPS 140-2 – Security
  - ISO/OSI 7-layer model for network connectivity
- ISA100 encourages
  - New technology
  - Deployment
  - Communication among practitioners

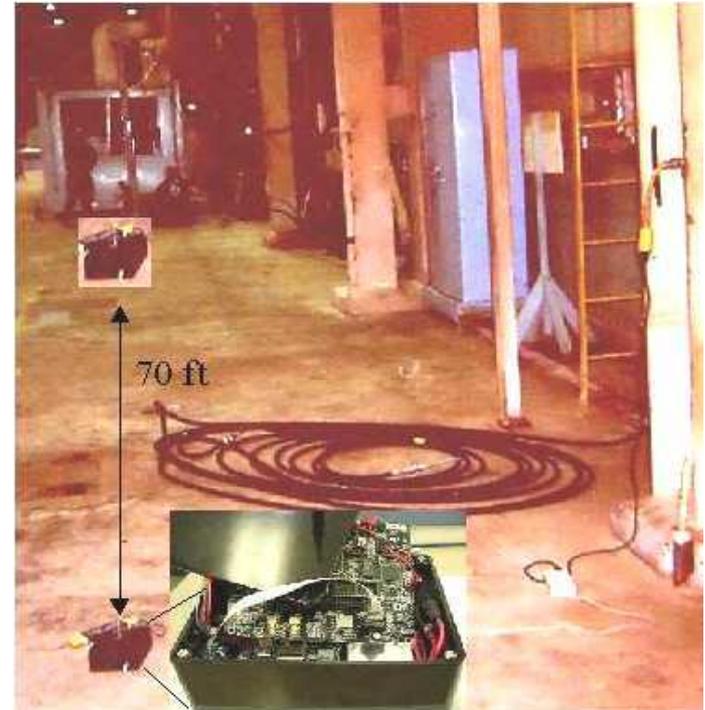


# ISA100 Organization – Work Groups & Study Groups



# The First Step – ISA100.11a!

- Immediate – non-standard products to be upgraded later
- Near-Term – ISA100.11a released for process monitoring and “soft” (>100ms) control
- Mid-Term – ISA100.11a adapted to other applications
- Longer Term (~2009) – New ISA100 standards released for:
  - Discrete manufacturing – tighter timing
  - Tracking (RFID) – passive, active, integrated
  - Security – integrated, scaleable, cost-effective
  - SCADA – geographically distributed



# Better Metrics, Better Options Are Coming

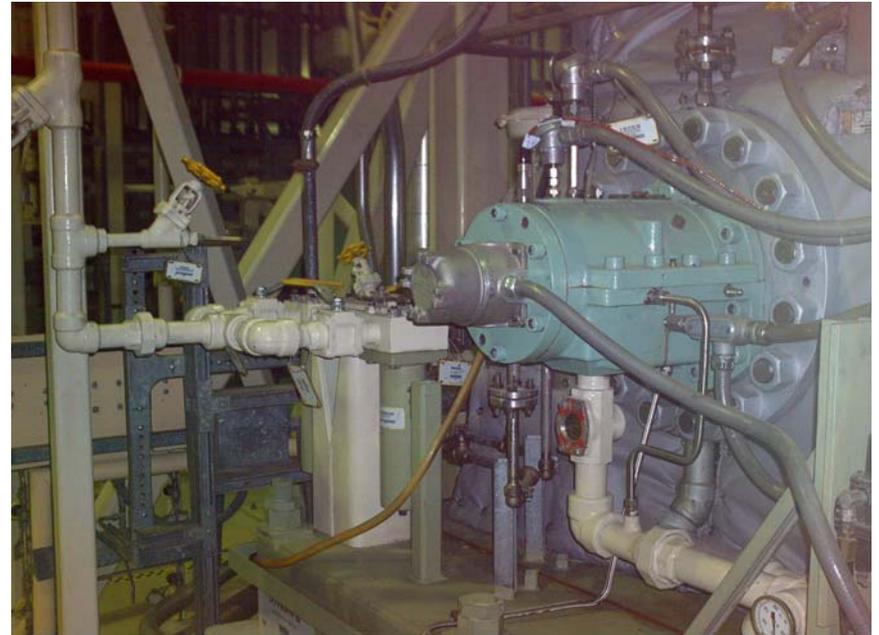
- **Conformance Metrics – How well do I conform to NIST 800-53? NERC CIP? FIPS-140-2?**
- **Performance Metrics – Mean-time-to-compromise**
- **Real-Time Options – Intrusion Detection Systems with closed-loop responses**
- **Diversity Options – NRC-like voting and fault tolerance**
- **PHY-Layer Security – No floods**



***“Our hiring practices are probably more of a risk that our wireless network” – end user at ISA100 meeting***

# Key Advances Poised for Deployment

- **Hybrid Spread Spectrum – Improvements in power, battery life, security, reliability**
- **Modeling and Simulation – For Grid Reliability, Security, Performance**
- **PHY Layer Security – Encryption is not enough**
- **Anticipatory Theory – beyond Condition-Based Maintenance**



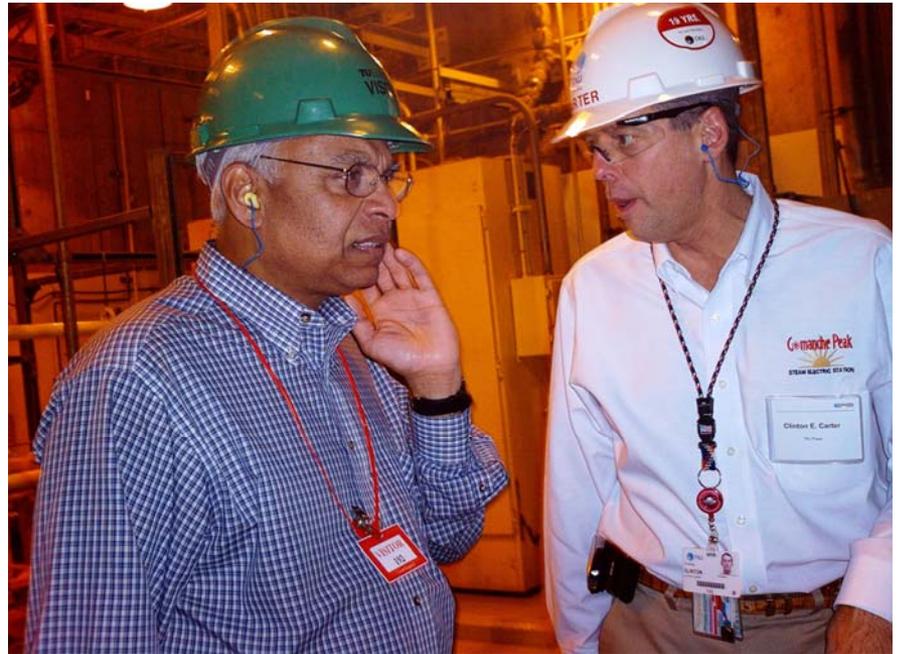
*Can simultaneously improve reliability, security, throughput, and latency!*

# Wireless Wins – Just Make It Work!



# Is Current Wireless Security Adequate?

- **Everywhere – unlikely**
- **Somewhere – almost certainly**
- **Key – sound engineering – match the application, environment, cost to the options**
- **ISA100 – ISA Wireless Industrial Automation Standard – check it out!**



*Proven in nuclear power plant?*

# Wireless **Security** - It's A System Problem!

- **Cyber Security – Just another failure mode? Like software, PCS engineers must learn it.**
- **Denial-of-Service – same impact whether adversary induced or security system induced!**
- **Security Aspects – availability, integrity, confidentiality – opposite order from most IT systems!**
- **Engineering Solutions – PCS determinism makes intrusion detection easier**
- **Goals Well Understood – Deter, Detect, Delay, Deny**



*Where is failure if password mistyped?*

# Could Wireless Provide the Business Case for Cyber?!

- **Automobiles**

- EPA provided the impetus for first microprocessors in autos
- Now 38 per vehicle!

- **Internet**

- Home computing was just a hobby until the first browsers.
- Now “Google” is a verb!

- **Wireless Is Enabler**

- Enterprise visibility
- Mobility
- Agility



*Two Fuses In Entire Vehicle!*

# OPM Investments – Impacting Industrial Applications

- **Reliability -**

- Mesh – Billions of \$ from DOD
- Spread Spectrum – Cell phones

- **Power**

- Harvesting – vibration, RF, PV
- Low-power designs – ASICs, FPGAs, DSP
- Protocols – low-duty cycle – ZigBee

- **Security**

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



# Will the REAL Wireless Sensor Please Stand Up!



Accelerating the adoption of wireless technologies in industry



**WINA**

WIRELESS INDUSTRIAL NETWORKING ALLIANCE

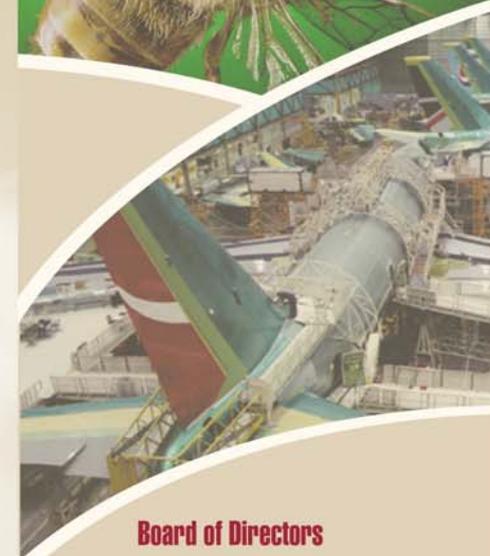
ISM frequencies

ZigBee™ 802.11 a/b/g  
802.15.4  
spread spectrum

1451.5  
cyber-  
security

Bluetooth®

[WWW.WINA.ORG](http://WWW.WINA.ORG)

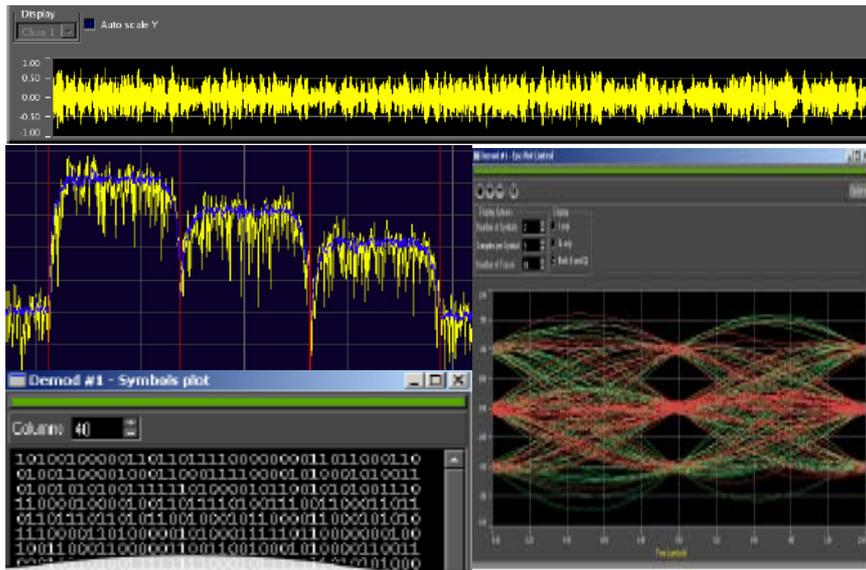


**Board of Directors**

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



# Extreme Measurement Communications Center (EMC<sup>2</sup>)



## Operational Capability

The DOE EMC<sup>2</sup> provides modeling, simulation and characterization support for industrial and other harsh environment 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

State-of-the-art microwave and digital microprobing tools for high-frequency device and circuit characterization, temperature-controlled measurements, RFIC functional testing, on-wafer TRL support, high-speed interconnect, package, and device testing

Multi-modal wireless testbed for co-existence measurement and analysis

## EMC<sup>2</sup> Program Benefits:

- EMC<sup>2</sup> formalizes the testing of industrial wireless networks to quantify the latency, throughput, security and fault-tolerance (Interference and Noise)
- The Wireless Industrial Networking Alliance (WINA) has accepted EMC<sup>2</sup> as its product testing and characterizing center for member companies
- Investigate robust wireless technologies; ultra wide band, Hybrid spread spectrum and related protocols for robust communication links in harsh environments
- Help develop or improve existing standards in industrial wireless networks to include measurement, verification and reliability of network and device parameters
- Study Co-existence and Interoperability issues among different wireless technologies (802.15.4, 802.11, 802.15.1 etc)
- 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 large-scale network modeling and simulation support; Provides ambient RF measurement surveys of harsh industrial environments.

**Deliverables:** Standards-based report generation for different wireless devices and network layouts; Software development for characteristic network testing; RF survey reports of harsh industrial floors and machinery

### **Contact Information:**

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

Teja Kuruganti  
kurugantipv@ornl.gov, 865-241-2874



# 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
- Next Step? – Find the right place to start!



**“CBM Is the Next Killer App For Wireless”  
– Dr. Jay Lee, Fortune Magazine, July 2002**