Setting the Standard for Automation™

Wireless Security – An Oxymoron?!!!

ISA EXPO 2007

Wayne W. Manges

October 3, 2007

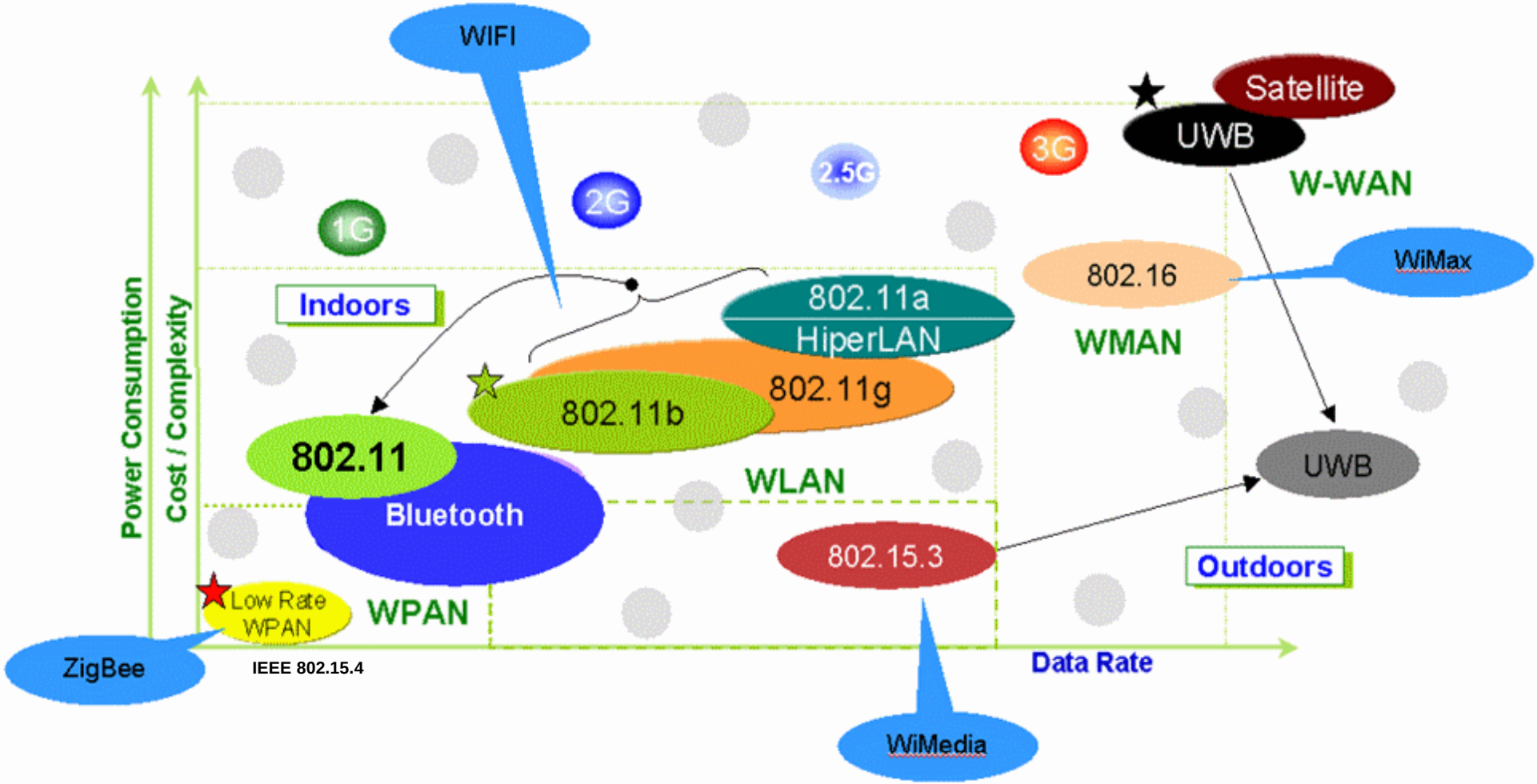
Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Welcome

- Why Me? – ISA100 Co-Chair (with Pat Schweitzer from Exxon); DOE Industrial Wireless lead; etc, etc, etc.
- Wireless Security –
  - Is it possible? Desirable? Costly?
  - What are the issues and how can they be addressed?
  - What does the future hold – better security? Or Worse?

Early Adopters – Blazing the Wireless Trail!

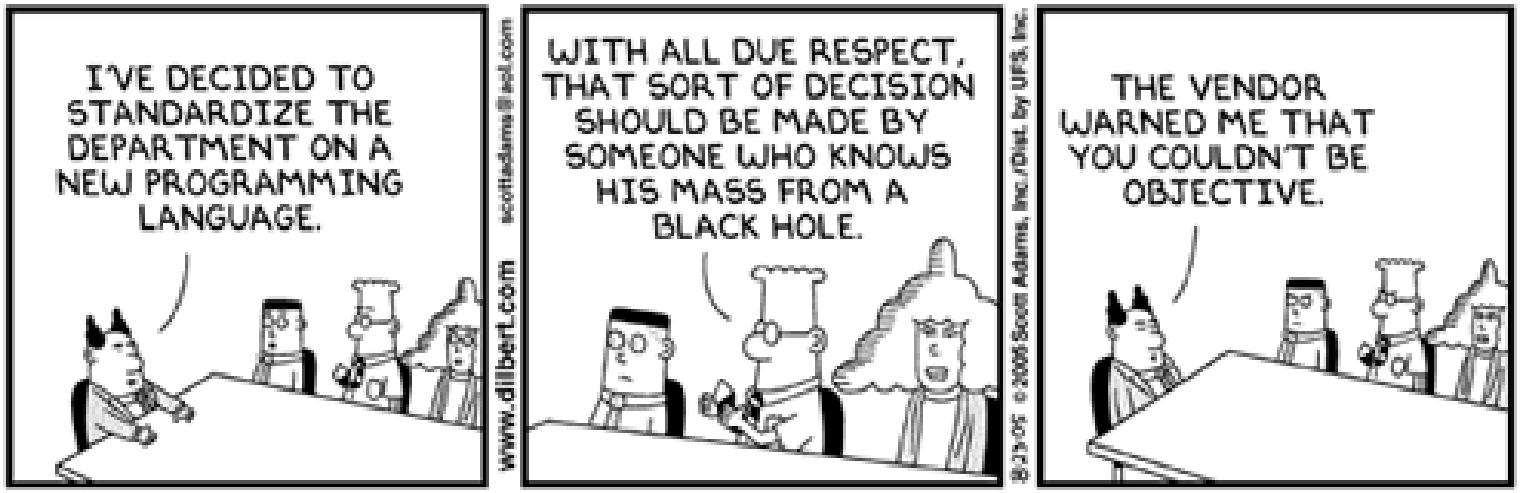
The Wireless Landscape – No Single Security Solution



= Proprietary Wireless Networks

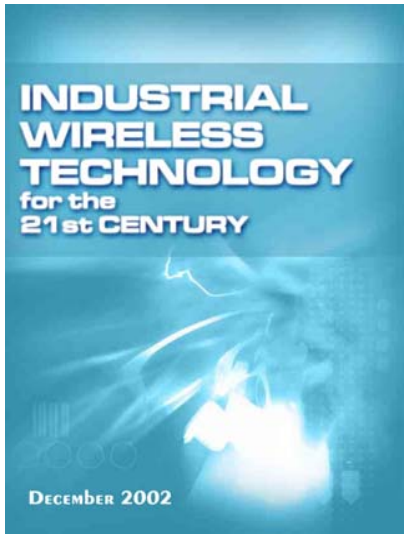
Why Do We Care?
It's The Benefit – Stupid!

- 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.

No Inherent Flaw – Wireless Can Be As Secure As Wire!

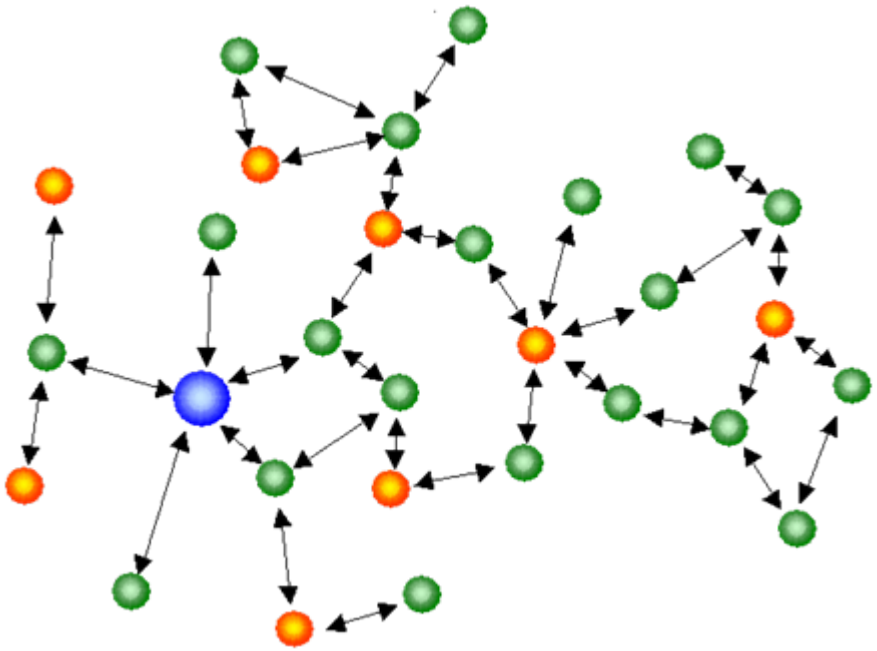


- Marketing – sell what I have, bandwidth is king
- Emotion – “Wireless scares me, I can’t control it!”
- Incompetence/Laziness – Too difficult to configure, too big a learning curve
- Cost/Benefit/Risk – ROI in a day, why bother?

Extreme Measurement Communications Center

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

Seat Belts – 25 Years from Introduction to Acceptance

Latency

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

Reliability

(Not BER, Not Accuracy)

Market Forces Determine Performance Delivered!

Throughput

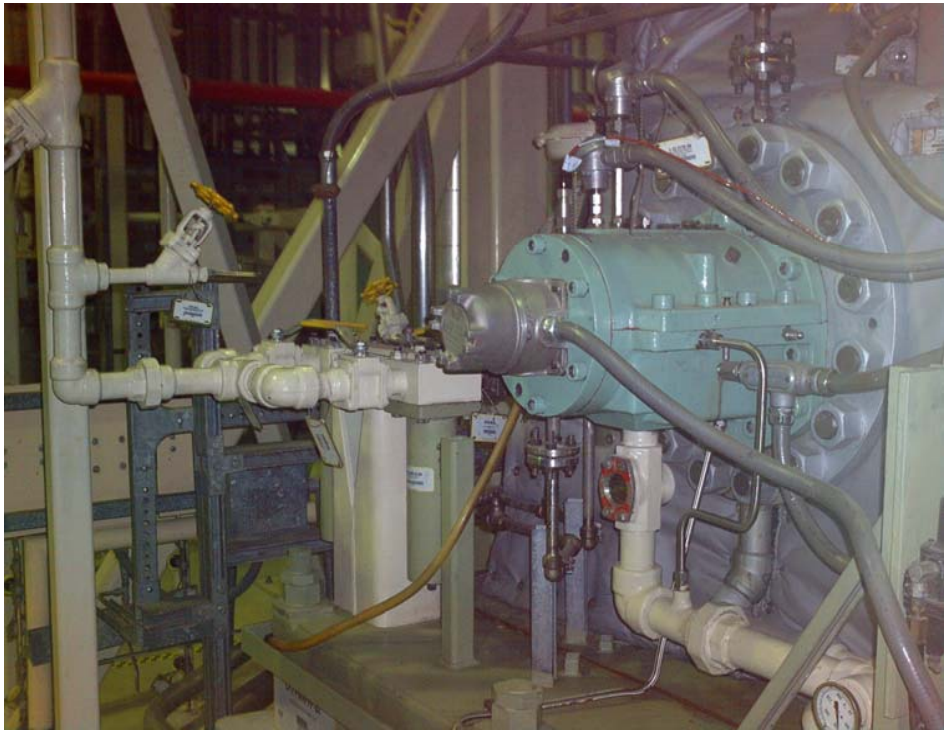
Bits-per-second or Goodput? End-to-end?

Security

Performance Based? Procedure Based? Proprietary or Open?

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!

PHY Layer Security – The Holy Grail?

- No Bits – must be present to win!
- LPI/LPD – low probability of intercept/detect
- Stealthy – buried in the noise
- Demonstrated – labs and DoD
- Low Transmitted Power – easier on surrounding stuff
- Denial Of Service Attacks – only at RF level

On the other hand:

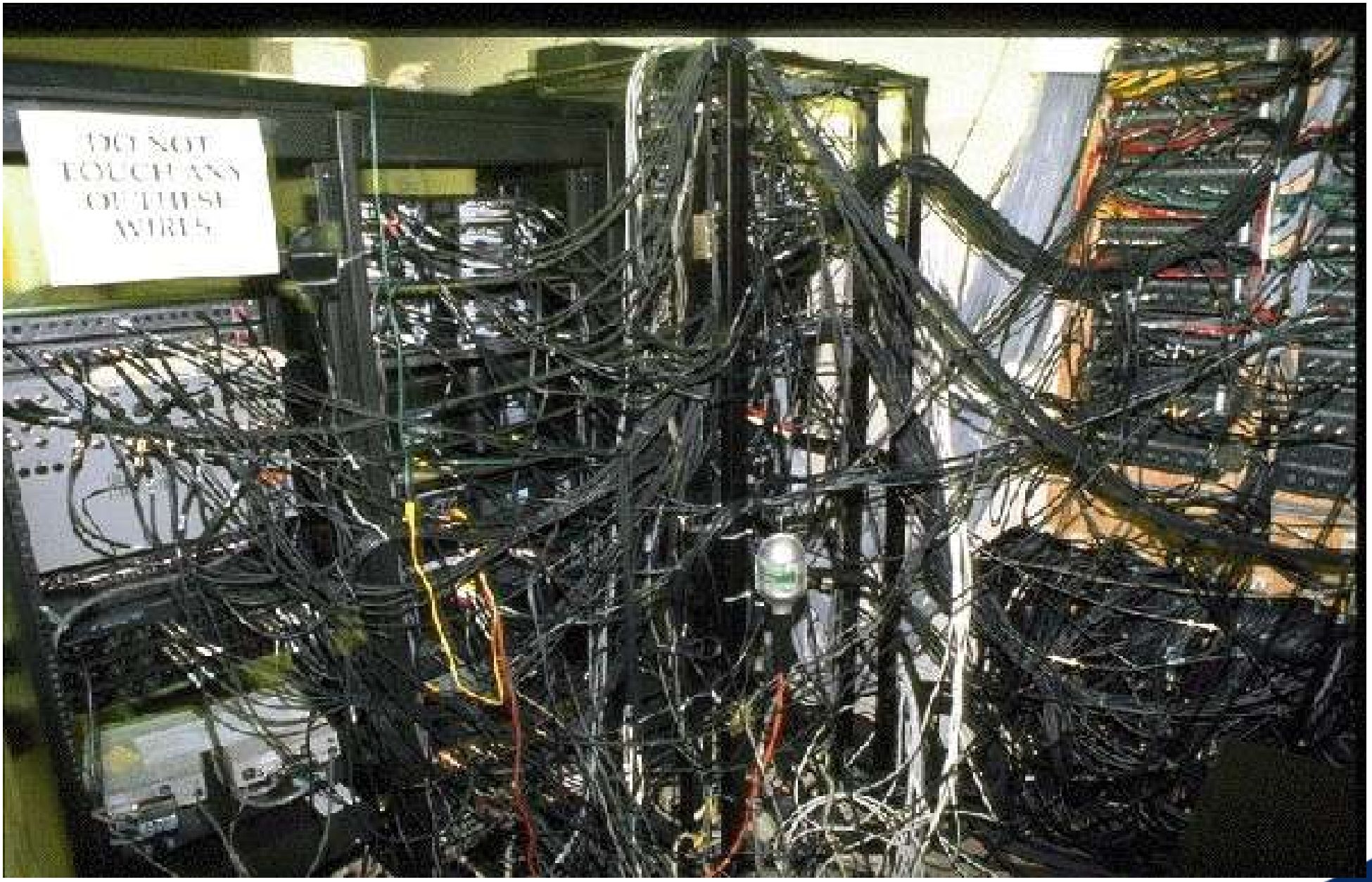
- Requires High Process Gain – around 60 db (1000 chips/bit) vs 12 db (15 chips/bit) today
- Export Control Issues – considered too stealthy
- Highly Complex – no currently available commercial products
- Key Management – always an issue

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

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!
- Wireless Compliance Institute – supporting ISA100
- Security Compliance Institute – supporting ISA99
- WINA – Education, marketing, collaboration

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?

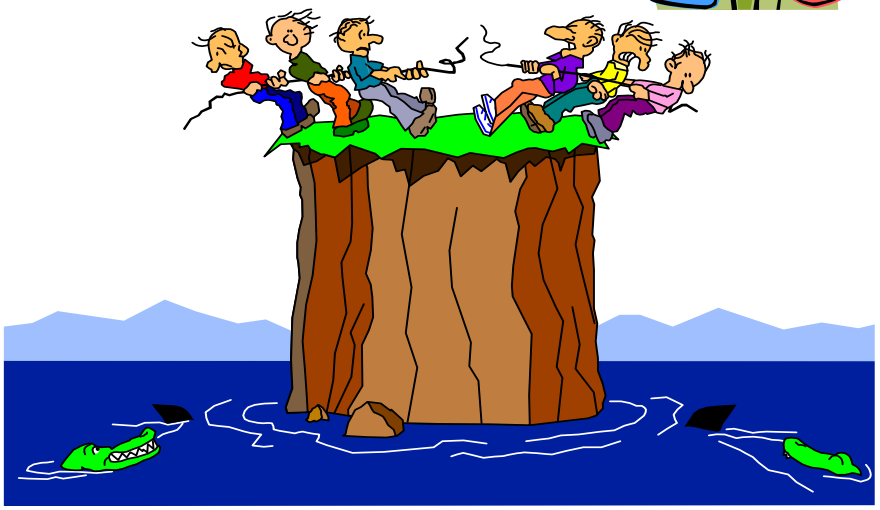
Could Wireless Provide the Business Case for Cyber?!

- **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!

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