

# **Secure Wireless Infrastructure**

**Greg Burns**  
**Invensys Process Systems**

# **Secure Wireless Infrastructure**

**Wireless Technologies**

**Applications**

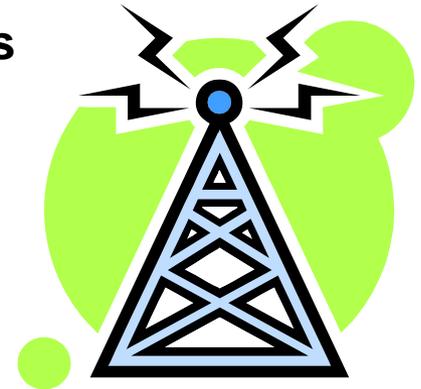
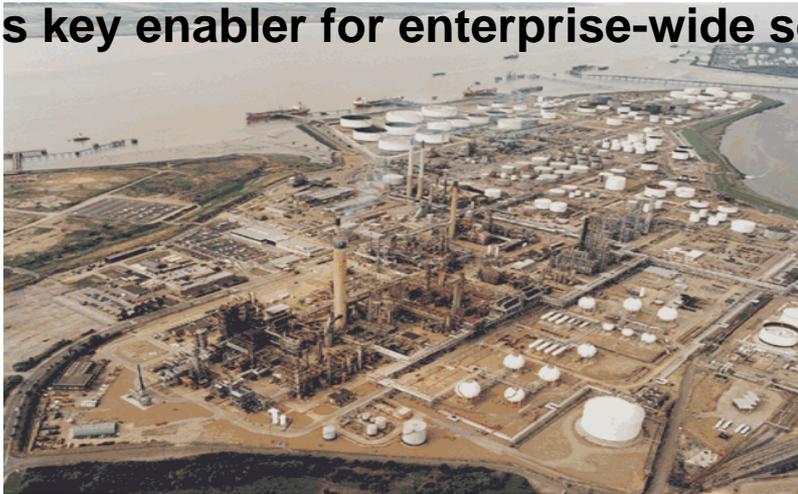
**Case Studies**

**Concerns**

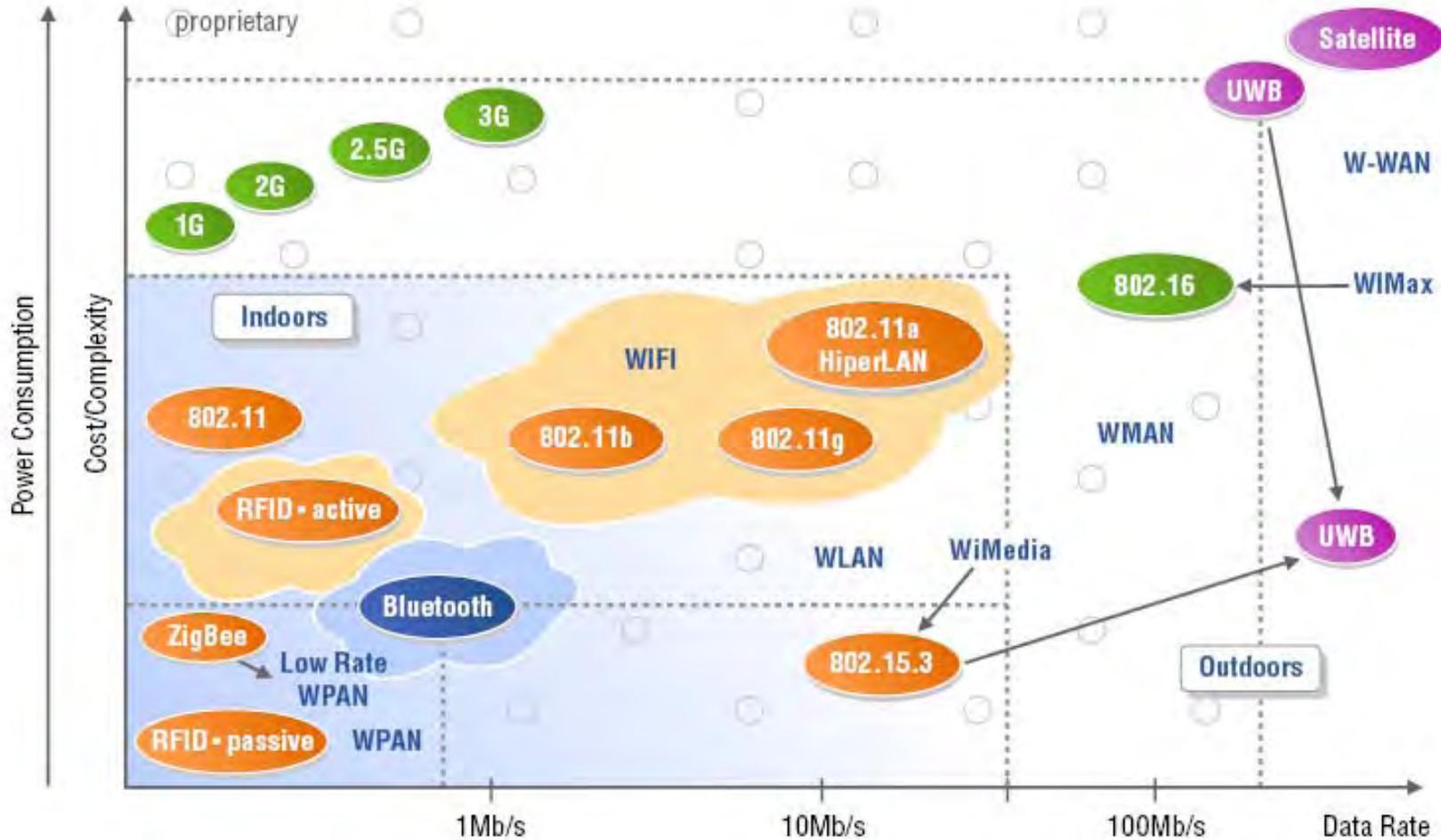
**Discussion**

# The Promise of Wireless Technology

- More measurement at lower cost
- Eliminating wires means significant cost savings
- More mobile workforce
- New applications drive bottom line improvements
- New measurements address mandated requirements
- Wireless is key enabler for enterprise-wide solutions



# RF: One size does NOT fit all....



# What Does 'Wireless' Mean?

## WiFi

Examples: Mobile Operator Terminals; data logging; security; maintenance; IT

## WiMax

Examples: Long distance broadband backhaul; high bandwidth (video) applications

## WSN

Examples: Condition monitoring; wireless instruments

## RFID

Examples: Asset tracking; safety and security; location

# 802.11 Standards

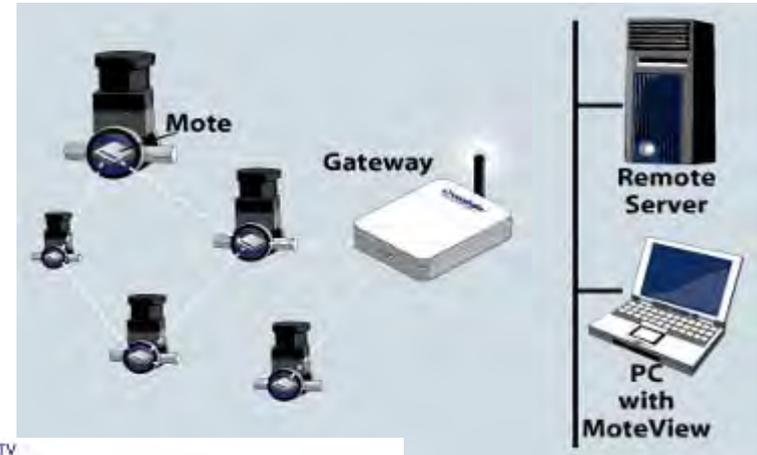
Breakdown of Popular 802.11 Standards			
Wireless Standard	802.11b	802.11a	802.11g
Speed & Frequency	Up to 11 Mbps in the 2.4 GHz band.	Up to 54 Mbps in the 5 GHz band (5X faster than 802.11b).	Up to 54 Mbps in the 2.4 GHz band.
Special Features	The worldwide standard for wireless networks.	Better at supporting multimedia, voice, video and large-image applications.	Enhanced for greater security than 802.11b.
Range	Up to 300'. Indoors, typically 100'-150' due to building materials.	Up to 75' indoors.	Up to 300'. Indoors, typically 100'-150' due to building materials.
Public Access	The standard wireless connection for WLANs and public hotspots (see below).	None. Better suited for businesses that deal with many simultaneous users and a higher rate of data transmission.	Its compatibility with 802.11b indicates that, in time, most 802.11b hotspots will convert to 802.11g.
Interference	Possible interference with cordless phones and microwave ovens in the crowded 2.4 GHz band.	None on the relatively vacant 5 GHz band.	Possible interference with cordless phones and microwave ovens in the crowded 2.4 GHz band.
Compatibility	Wide availability ensures compatible access virtually worldwide.	Not compatible with 802.11b or 802.11g.	Backwards compatible with 802.11b.

# 802.16 Standards

	WiMAX Air Interface Standard		
	IEEE 802.16	IEEE 802.16-2004	IEEE 802.16e
<b>Estimation Date</b>	2003	Certification in 2005	2006
<b>Frequency Band</b>	Licensed 10-66 GHz	Licensed and unlicensed sub-11 GHz	Sub-6 GHz
<b>Service</b>	Fixed	Fixed/Nomadic	Fixed, Mobile
<b>Primary Market Segment</b>	Urban: high density multi-tenant buildings	Urban, suburban, rural residential: SME, Wi-Fi backhaul	Broadband access to laptop, PDA or smart phone
<b>Air Interface</b>	SCA OFDM/OFDMA	OFDM/OFDMA	SOFDMA
<b>Range</b>	LOS up to 5 km	LOS & near-LOS up to 30 km; non-LOS up to 5 km	Non-LOS up to 10 km
<b>Channel BW</b>	20, 25, 28 MHz	Various from 1.75 to 20 MHz (depending on frequency)	Various from 1.25 MHz to 20 MHz (depending on frequency)
<b>Channel Capacity</b>	Up to 134 Mbps	Up to 70 Mbps	Up to 35 Mbps
<b>Duplexing</b>	TDD or FDD	TDD or FDD	TDD or FDD
<b>QoS</b>	Voice/data/video, differentiated services	Voice/data/video, differentiated services	Voice/data/video differentiated services

# WSN

- 802.15.4 / ZIGBEE
- Various Topologies
  - Star
  - Ring
  - Bus
  - Full Connected
  - Mesh
- TSMP
- Each node can route
- Gateway to Plant





# Technology Brief

## ● IEEE 802.16 (WiMax)

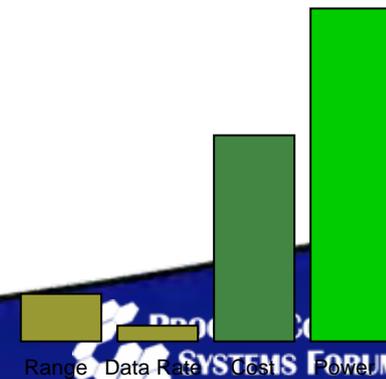
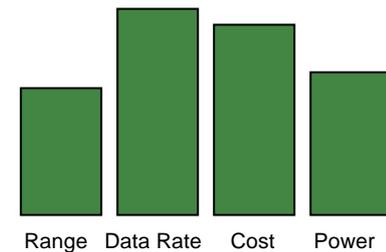
- LOS and NLOS applications
- Range up to 50KM LOS, 5KM NLOS
- Data Rate up to 70 Mbps
- Frequency range 2-11GHz
  - Deployment in ISM bands at 2.4-2.5 GHz and 5.725-5.875 GHz
  - Other frequencies typically require licensing

## ● IEEE 802.11 (WiFi)

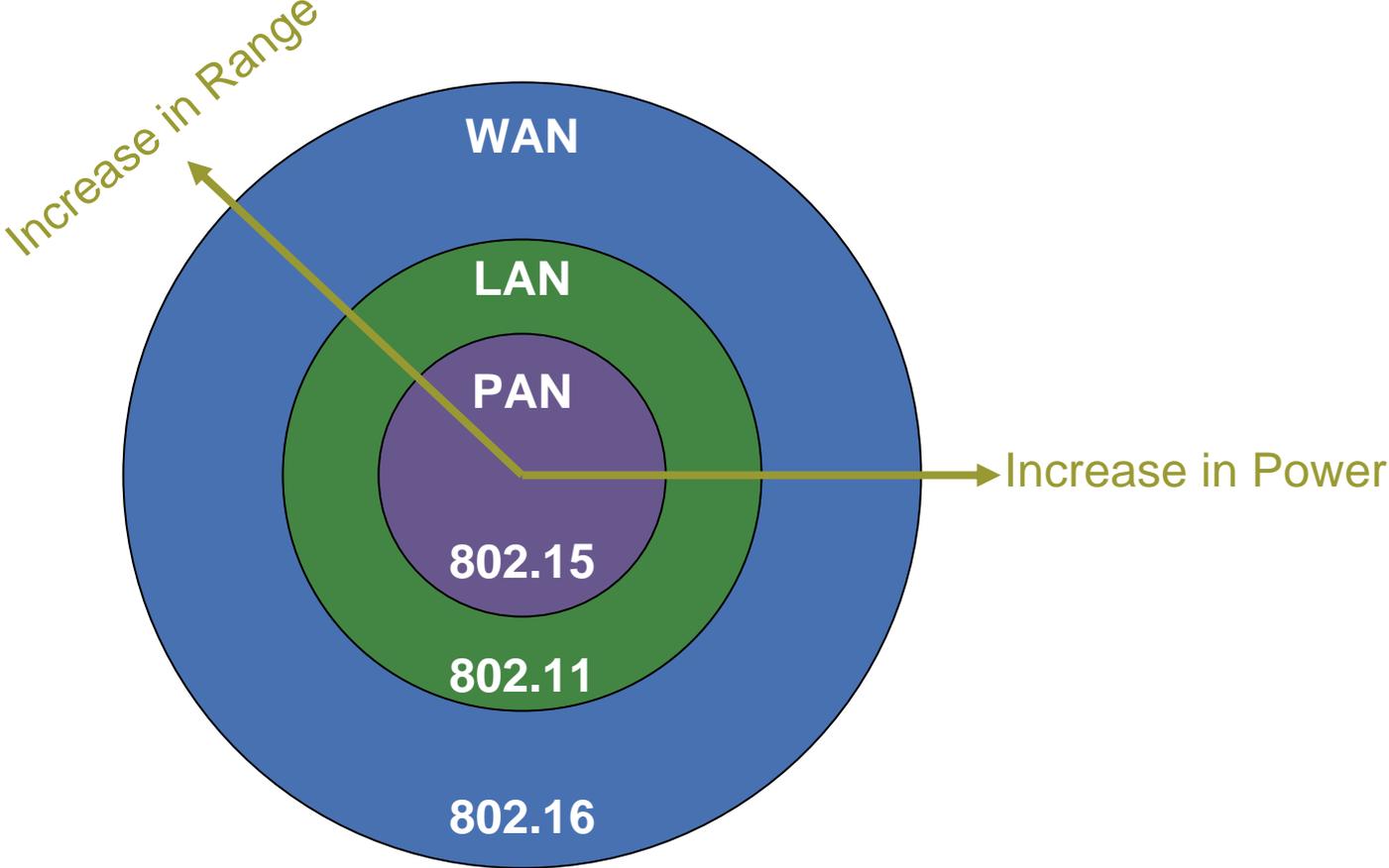
- NLOS
- Range typically 100M
- Data Rate up to 54Mbps (802.11g)
- Frequency range ISM 2.4 GHz (802.11g) and 5 GHz (802.11a)

## ● IEEE 802.15.4

- NLOS
- Range typically 50M
- Very low data rate
- Frequency range ISM 900 MHz and 2.4 GHz
- Low Power

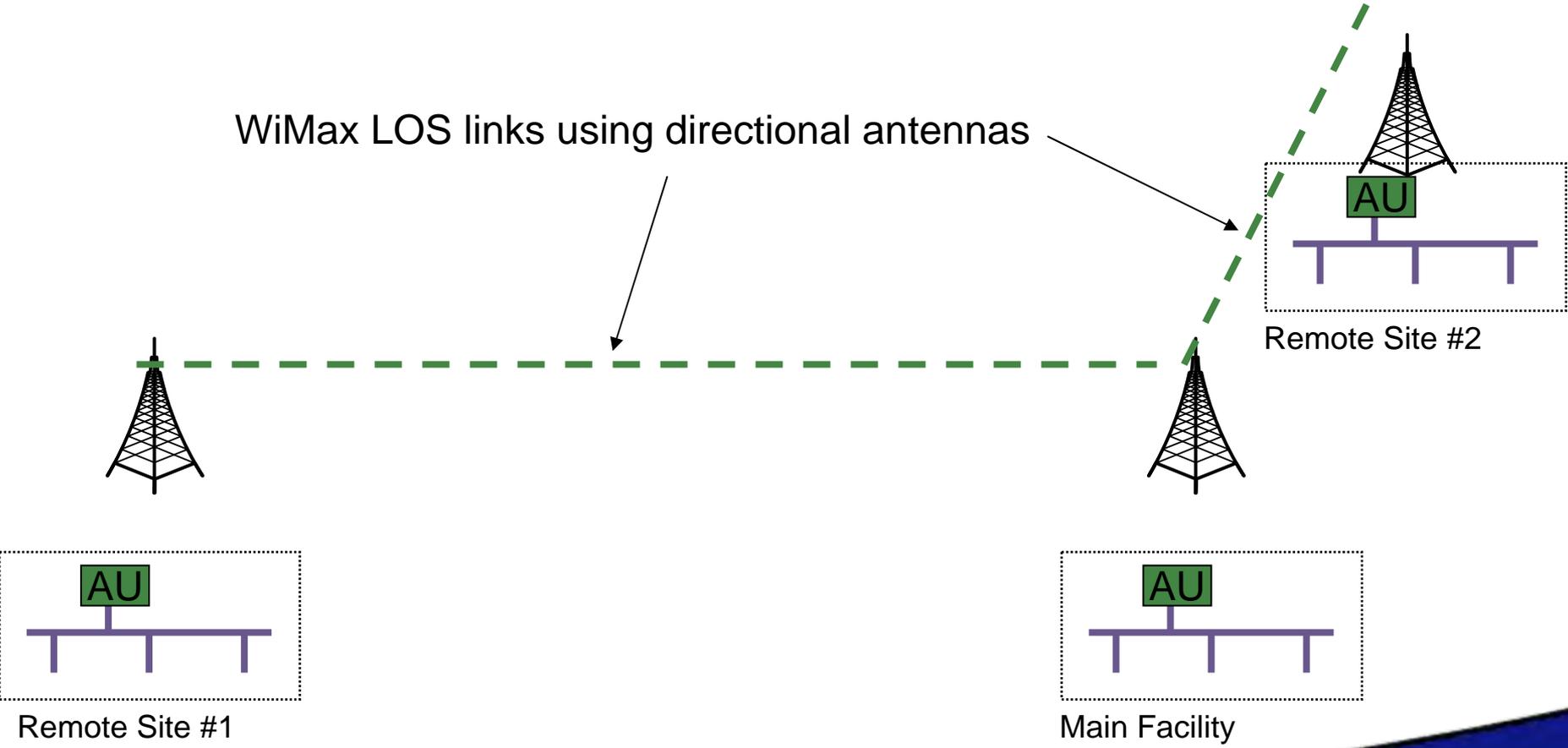


# Wireless Range Vs. Power

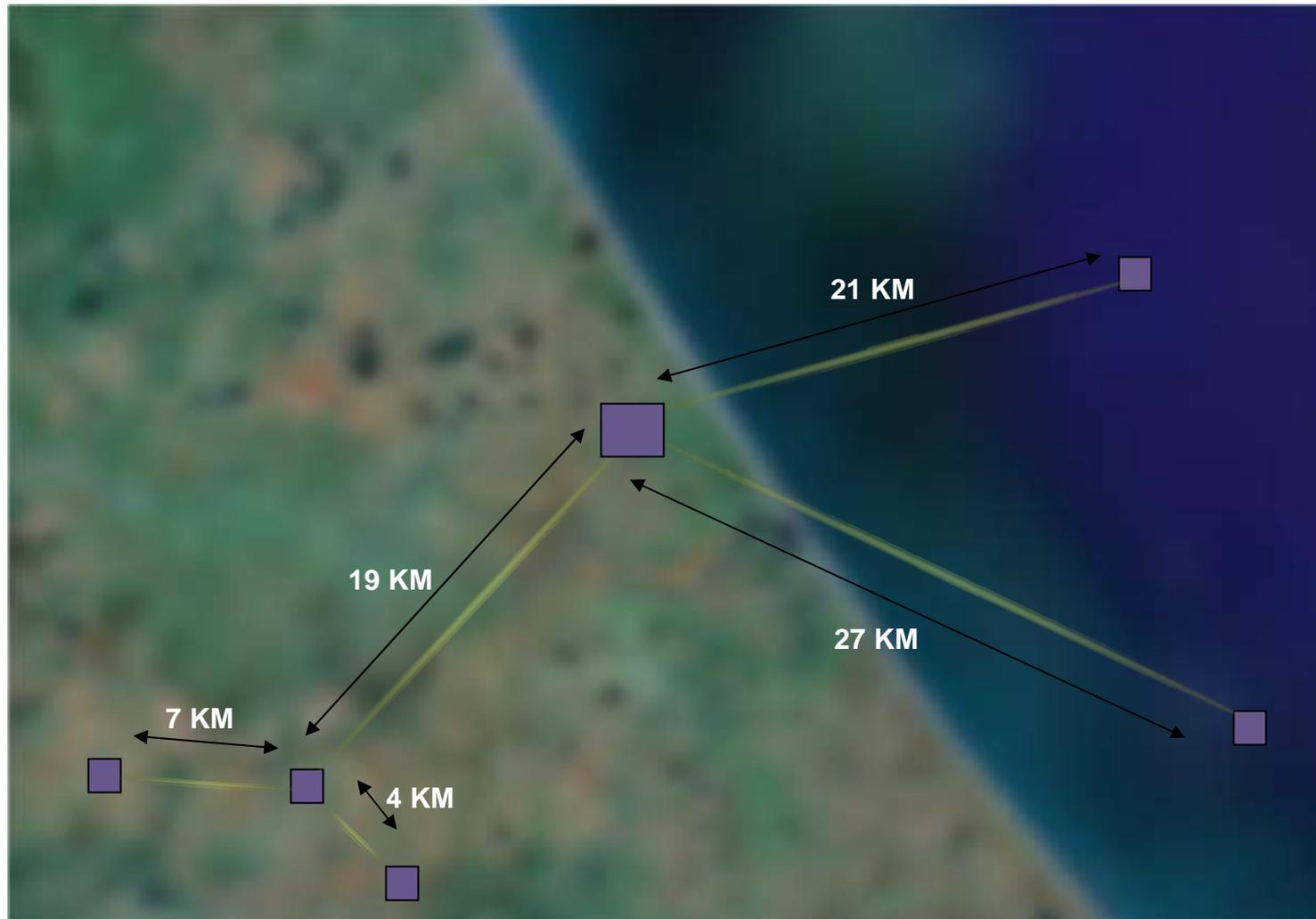


# Typical LOS Design

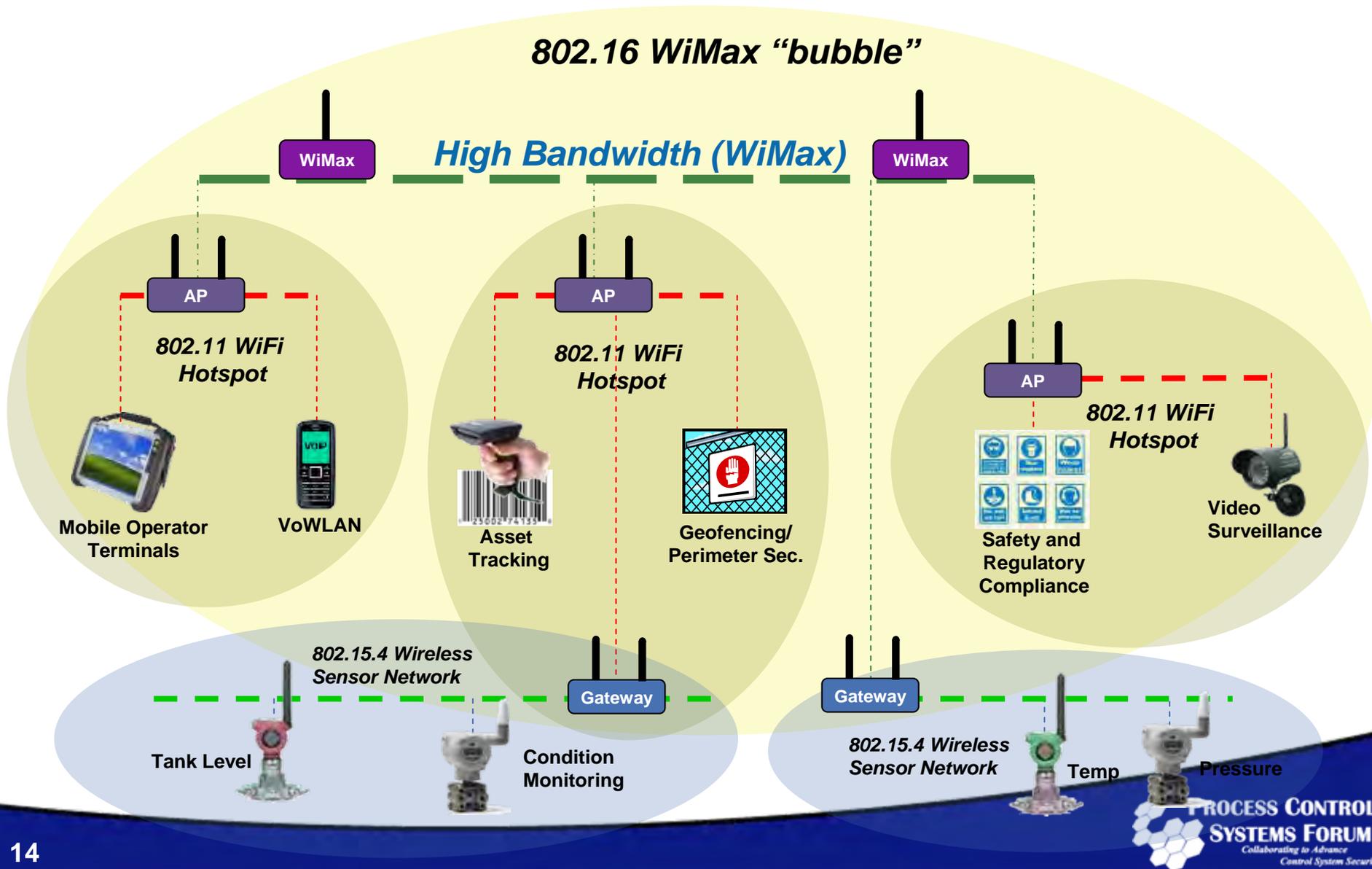
WiMax LOS links using directional antennas



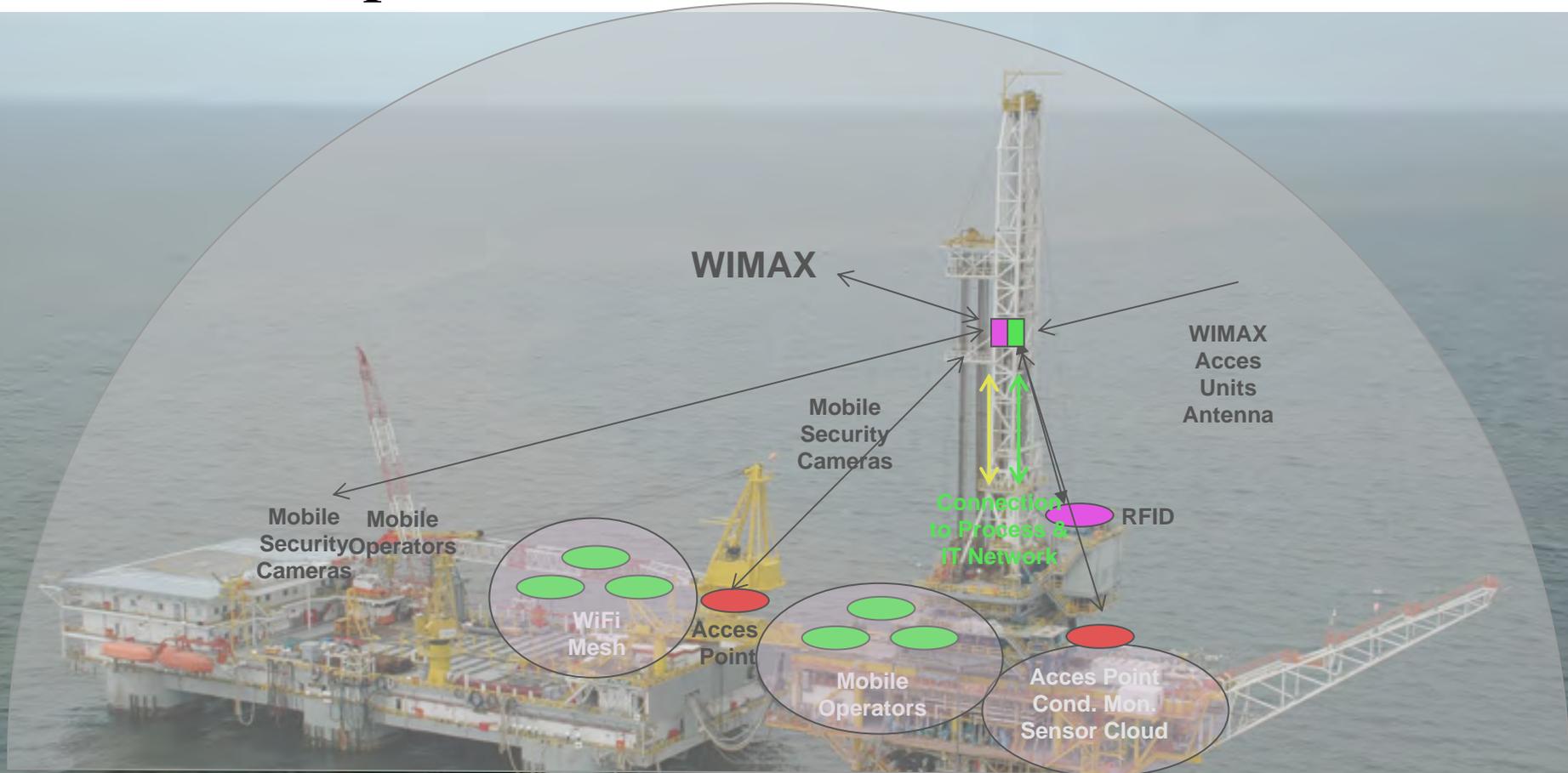
# LOS Example



# Typical NLOS Design



# NLOS Example

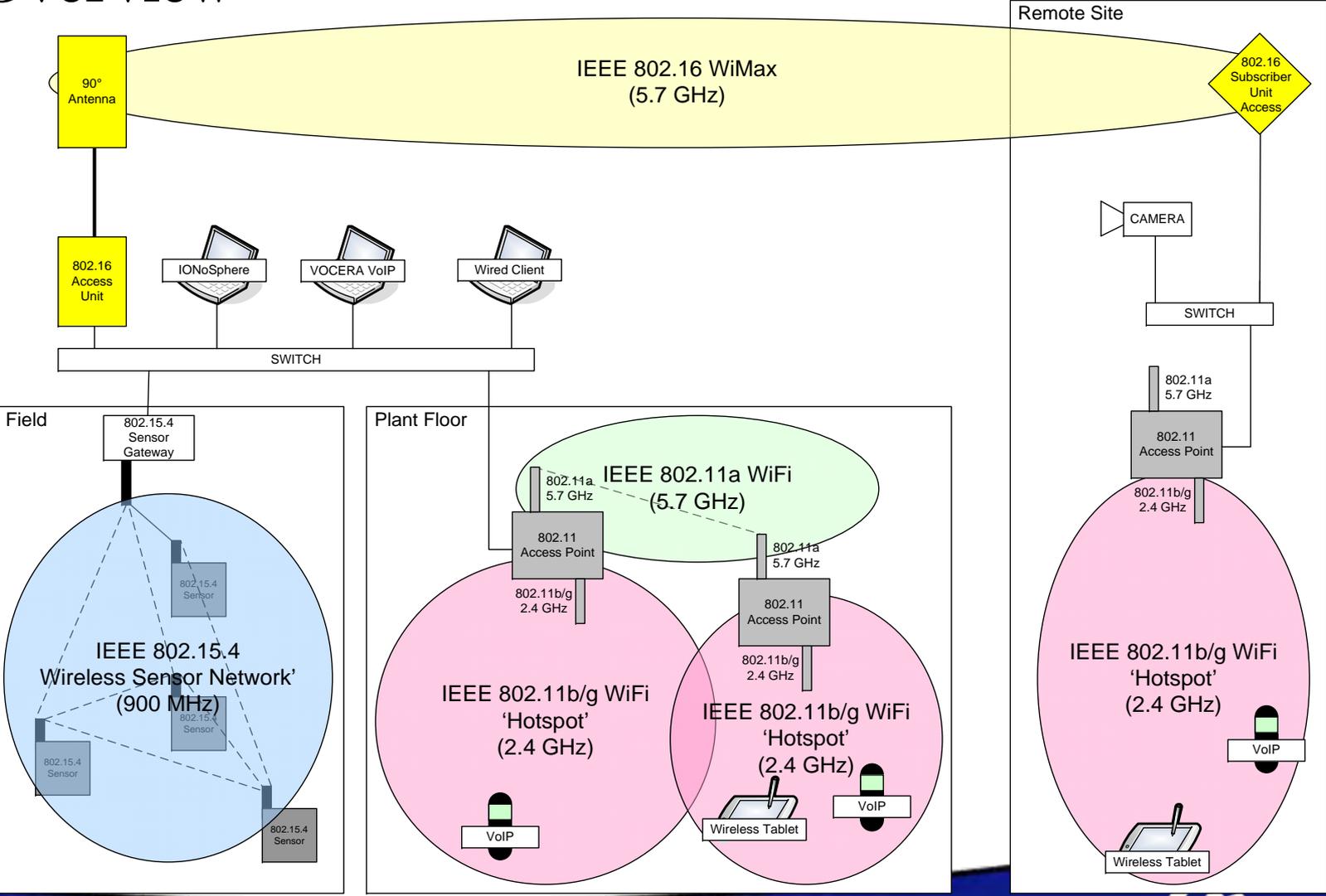




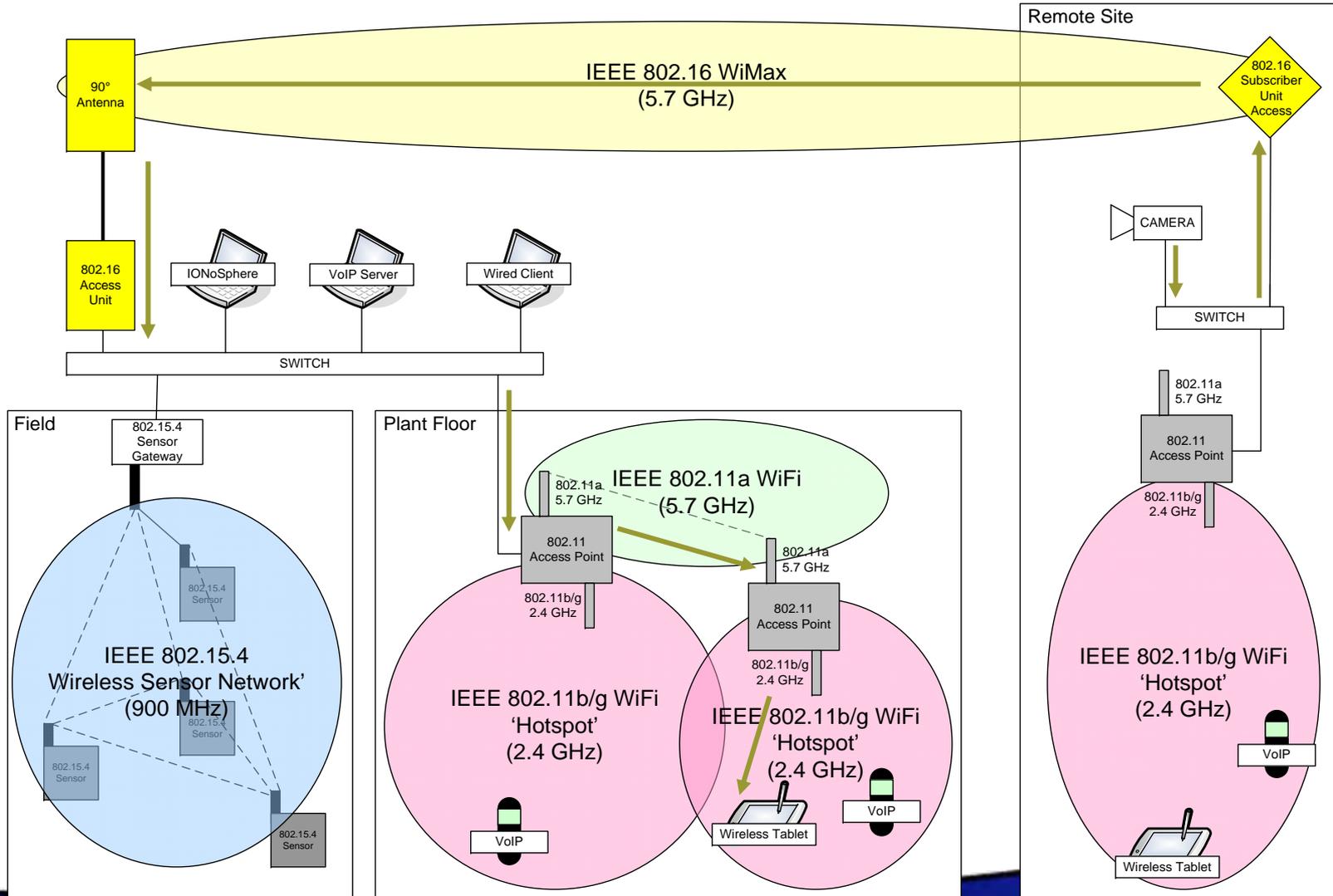
# Wireless Technologies

- ◆ **WiMax LOS link backhaul or Point to Point**
  - Up to 50KM, depending on bandwidth and environmental conditions
- ◆ **WiMax NLOS ‘bubble’ can surround entire plant**
  - Approx. 5KM Radius
- ◆ **WiFi ‘hotspots’ give mobility to workers**
  - Live Video, VoIP, Realtime Tracking, Remote Access to data/HMI etc.
- ◆ **These integrated technologies allow for:**
  - Reduced personnel / less transport
  - Faster response / intervention
  - More mobility / better communications
  - Superior remote capabilities
  - Safer working environment

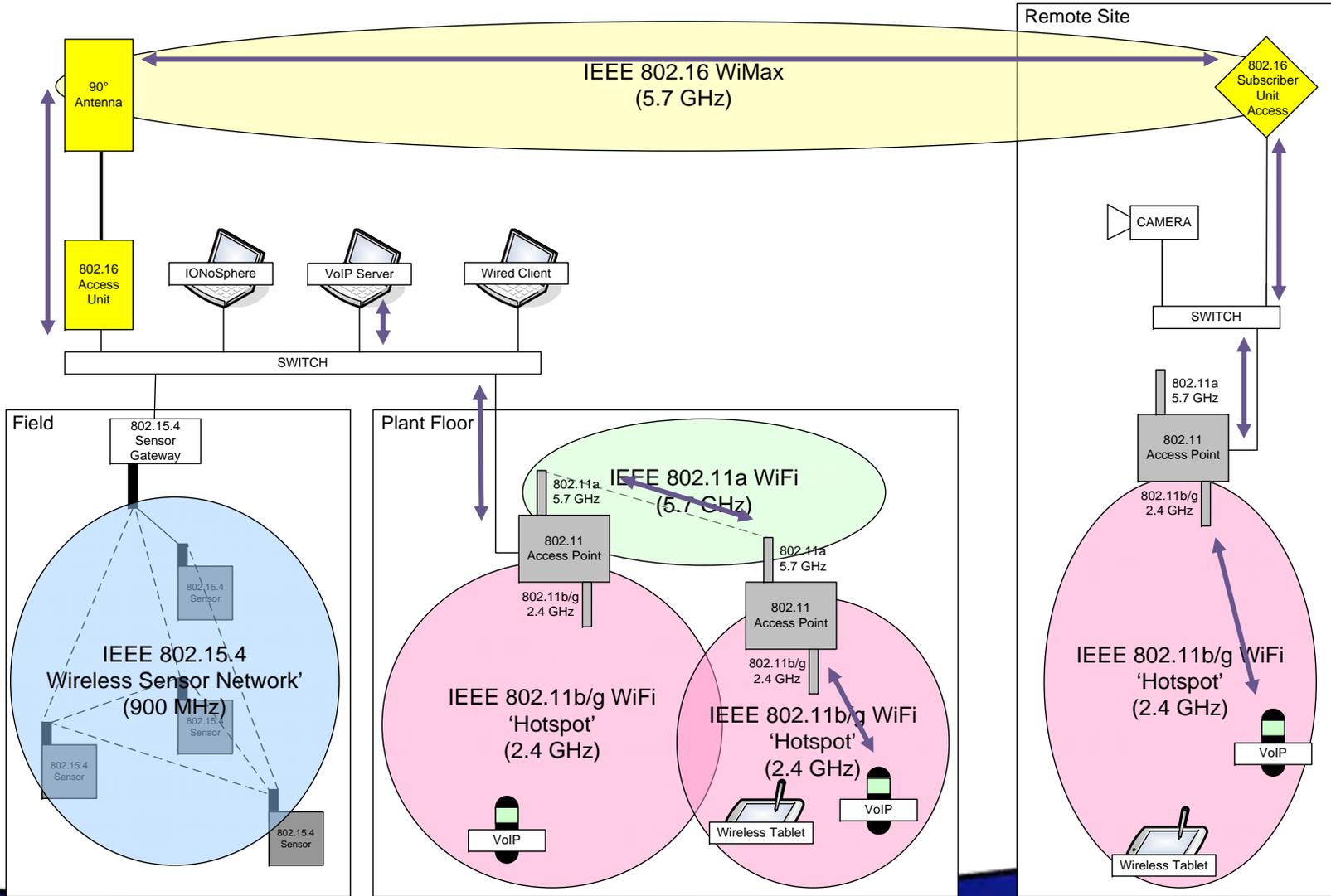
# Wireless Sample Configuration: Overview



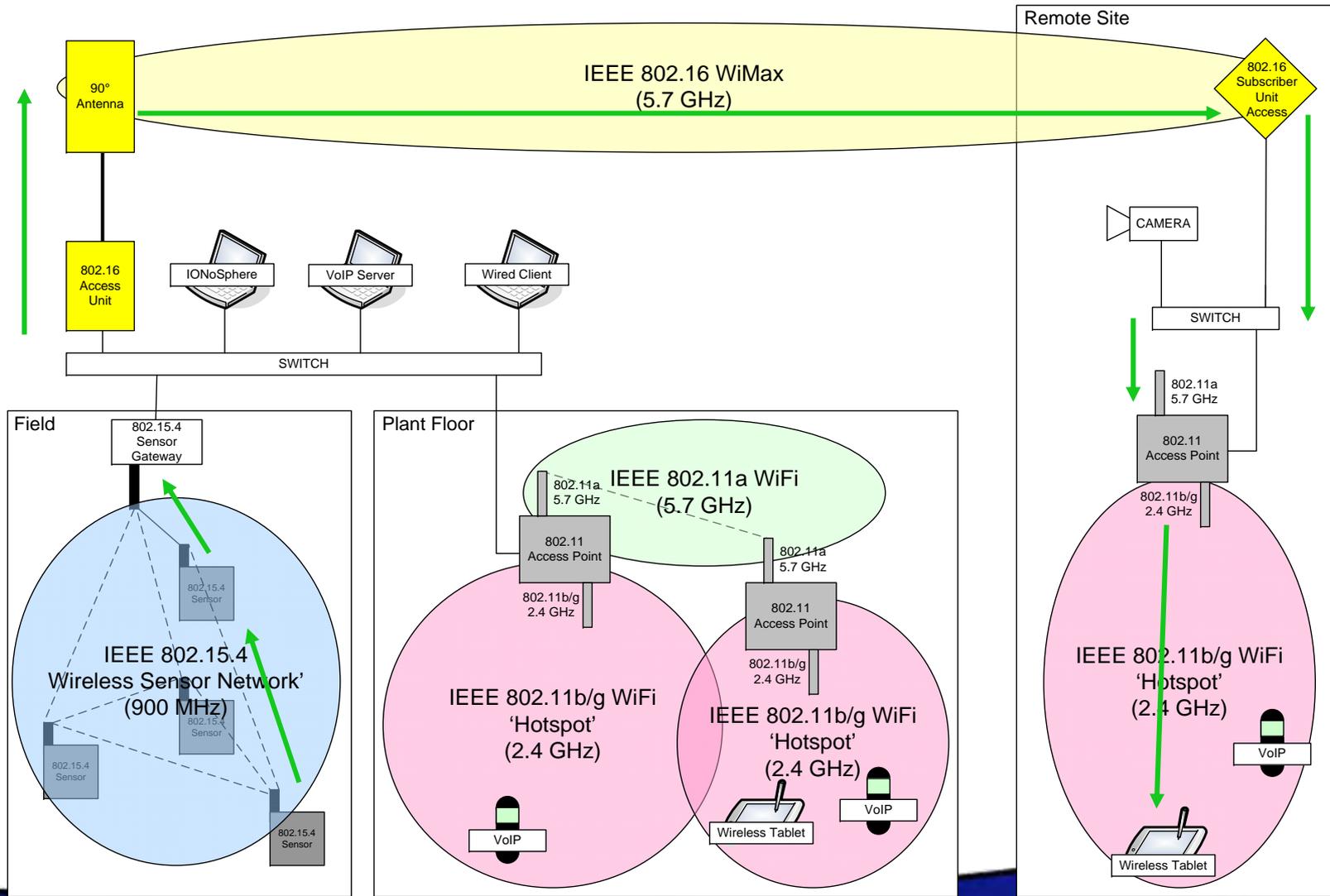
# Wireless Sample Configuration: Video Over IP



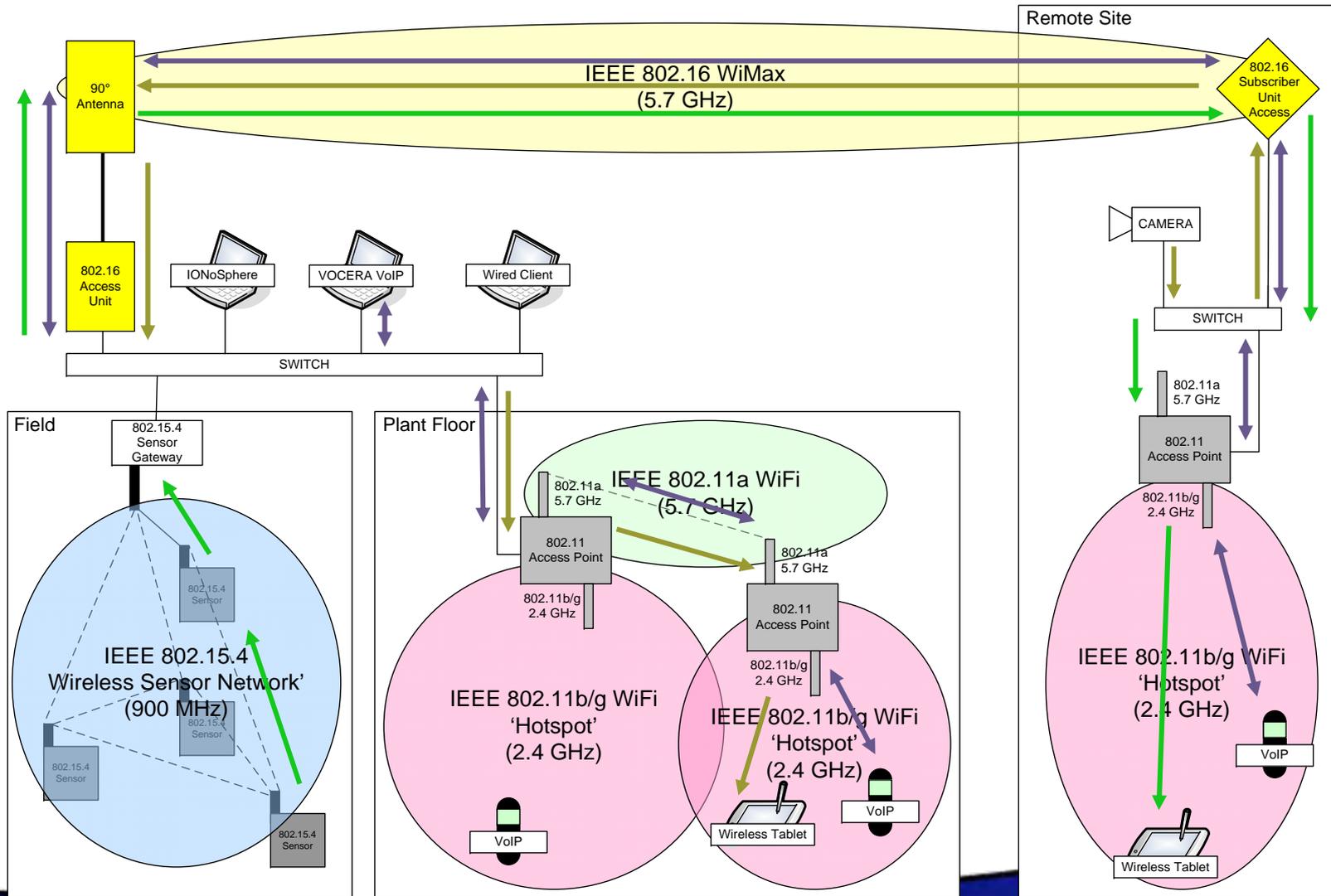
# Wireless Sample Configuration: Voice Over IP (VOIP)



# Wireless Sample Configuration: WSN Monitor



# Wireless Sample Configuration: Multiple Applications – Single Infrastructure



# Enables Integrated Solutions Throughout Industrial Environment

- ◆ Effective asset tracking
- ◆ Inexpensive condition monitoring & predictive maintenance management
- ◆ Greater process measurement & optimization
- ◆ OSHA-mandated safety, security & employee location
- ◆ Low-cost wireless VoIP voice communications & video
- ◆ Highly secure wireless access for laptops/handhelds
- ◆ More plant security – perimeter/access



© John Combs

# Example Application –Energy Management

Application:

Temperature profile on steam pipe to reduce condensation and consequential damages of millions of dollars

Answer:

Logistically nearly unfeasible if wired based.



Wireless led to significant time and cost savings

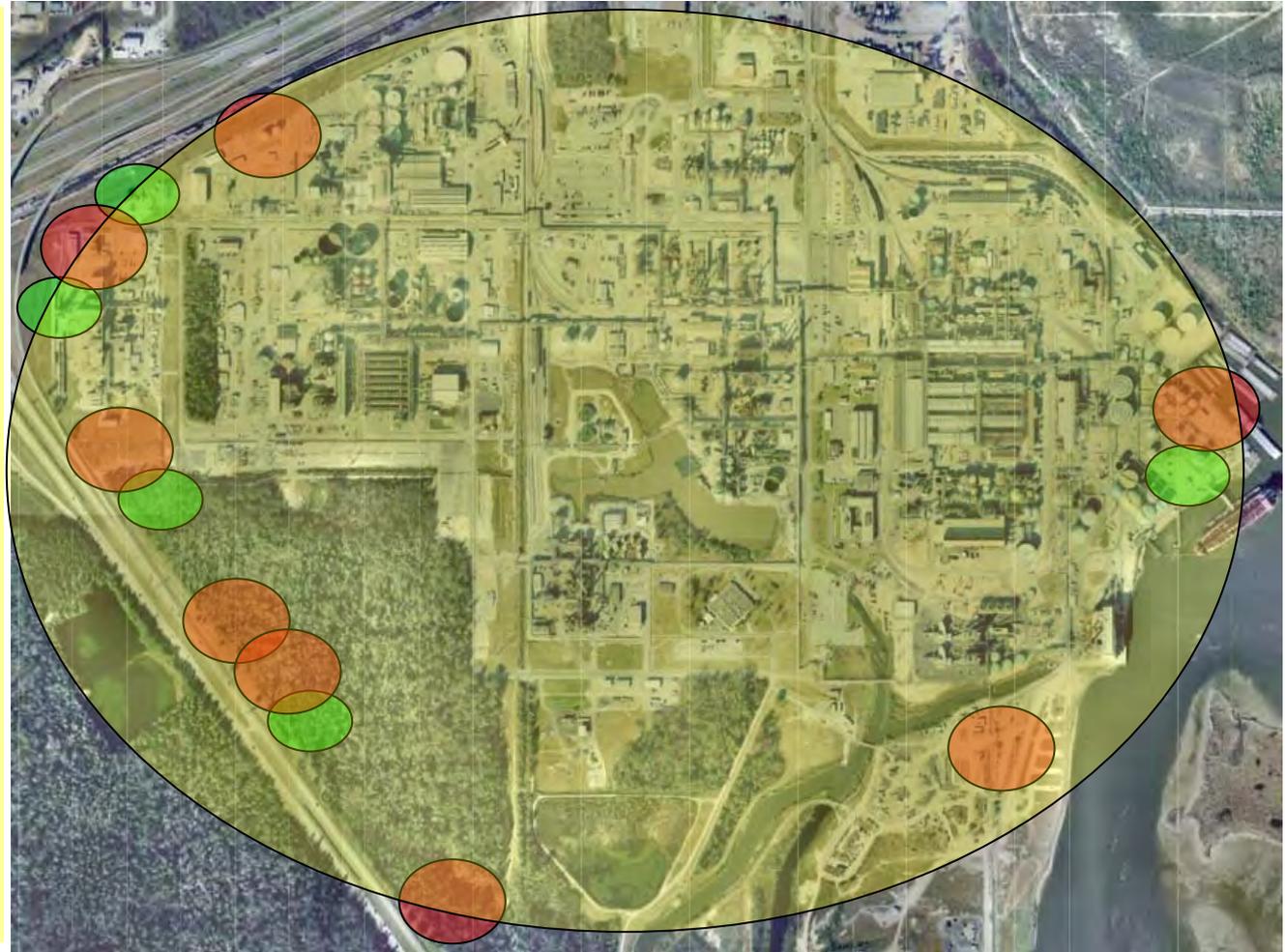
# Example Application – Perimeter Security

Application:  
Perimeter security application with WMD detection, video, and "other" sensors.

Answer:

Wireless network connectivity which is the only practical solution due to terrain and cost.

Meeting regulatory compliance



Sensors and Video integrated into WiMax for remote access

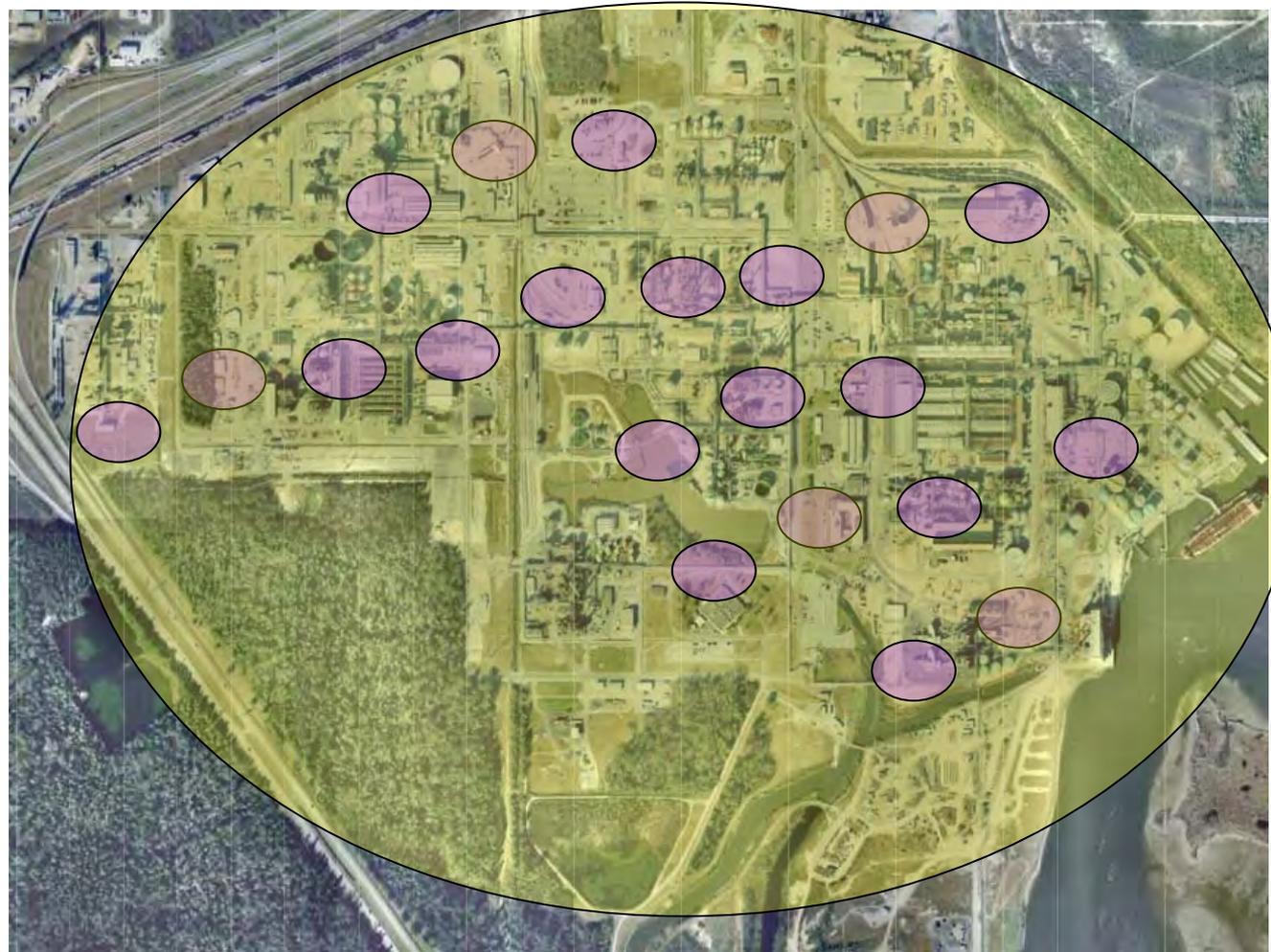
# Example Application – Safety Shower Notification

Application:

OSHA  
recomendations for  
activation  
notification

Answer:

Over 1000 showers  
need simple  
activation sensors  
back to Emergency  
Services

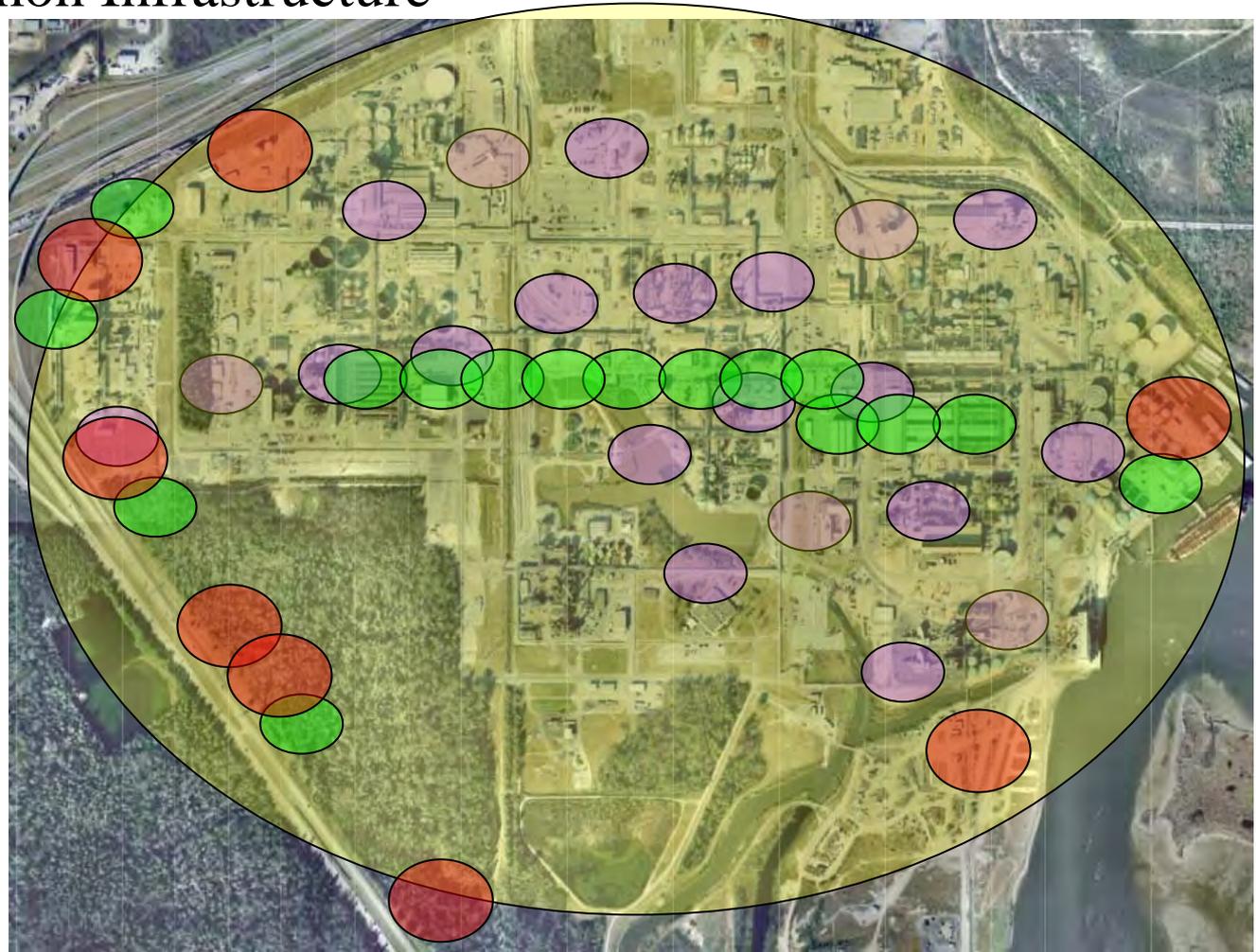


**WiMax backhaul allows integration of Sensors at any location**

# Multiple Applications Crossing Multiple Business Units – Sharing a Common Infrastructure

## Benefits:

Once significant application can build the “hi-way” for future applications and technologies



**Scalable, Secure Common Infrastructure. Add Apps at any location**

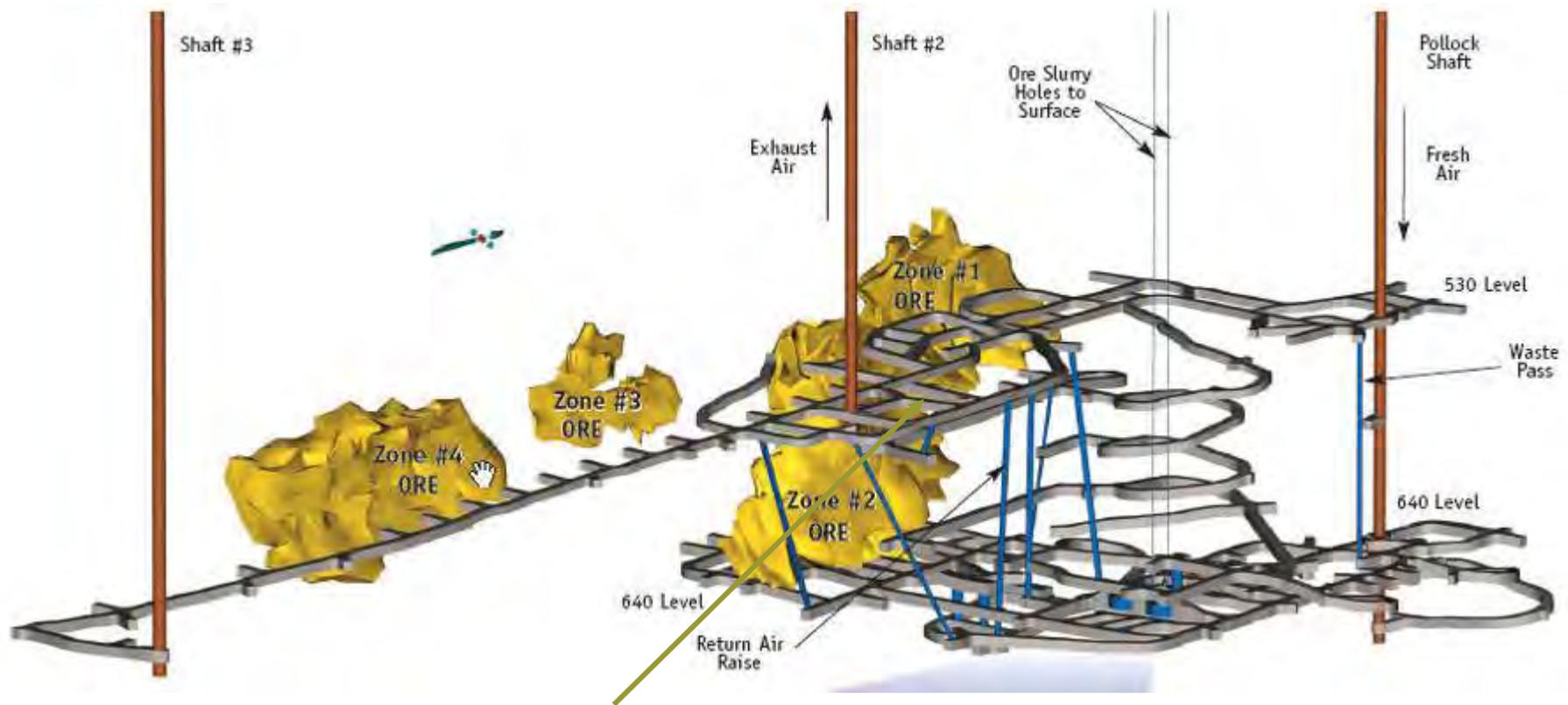
# Wireless Communications

- ◆ Replace Legacy PA and Radios
- ◆ Implement a Wireless PPT an PA system



**Example: VoIP, Video, Asset Tracking,  
Mobile Workers, Remote I/O**

## ◆ A Uranium mine in Northern Canada



Multiple Applications all supported by the  
Reuse of the same wireless infrastructure!

# Potential Enterprise Applications

- Personnel tracking/locating
- Safety event monitoring & management
- Plant security & extended visibility (video)
- Material & product tracking
- Rolling stock tracking
- Field operator efficiency
- Field maintenance efficiency
- Access control & intrusion detection
- Leak detection
- Hand-held HMI
- Incremental process/equipment measures
- Process management
- Mobile asset management
- Evacuation management

**A virtually unlimited range of high-value applications**

# Wireless Solutions – Available Today

- **Wireless IT Security**
  - Manage all of your existing and future wireless communications with world class continuously current security and systems management
- **The Mobile Operator**
  - Interface to any Control system application or enterprise application with an industrial wireless tablet PC
- **Wireless Communications – VoIP**
  - Communicate via wireless voice over IP with industrial quality hands free devices and a configurable interface into existing paging and phone systems
- **Field Data Logging**
  - Improve reliability with wireless workflow technology – automate maintenance procedures and data logging.
- **Asset Performance Optimization**
  - Provide new insight into the condition of a machine in real time with advanced assessment tools to determine the probability of failure as well as the identification of affected machine parts
- **Plant Security – Video and Sensors**
  - Add Video and sensors to improve plant and process security. Streaming video on the process or perimeter coupled with intrusion sensors help meet new mandated security requirements

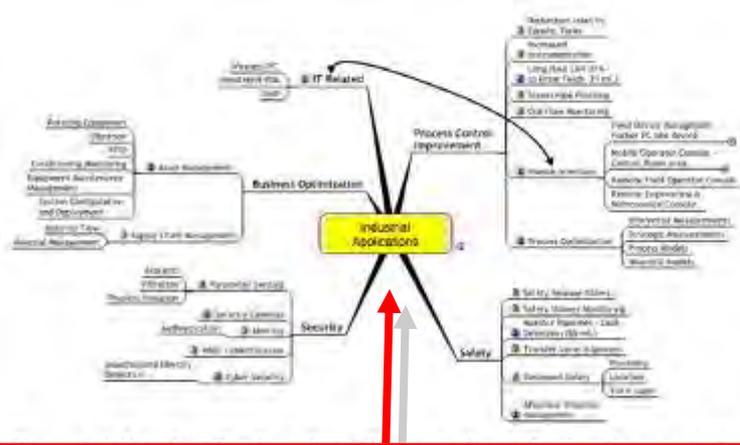
# A Site Assessment Study- A Team Approach

- ◆ A strategic review with representatives from various functional units to ascertain current, near-term and future “needs”
- ◆ Working with the facility/corporate IT department to address connectivity and security needs and requirements
- ◆ An RF site survey to ascertain the current wireless activity at the facility & RF signal measurements & coverage

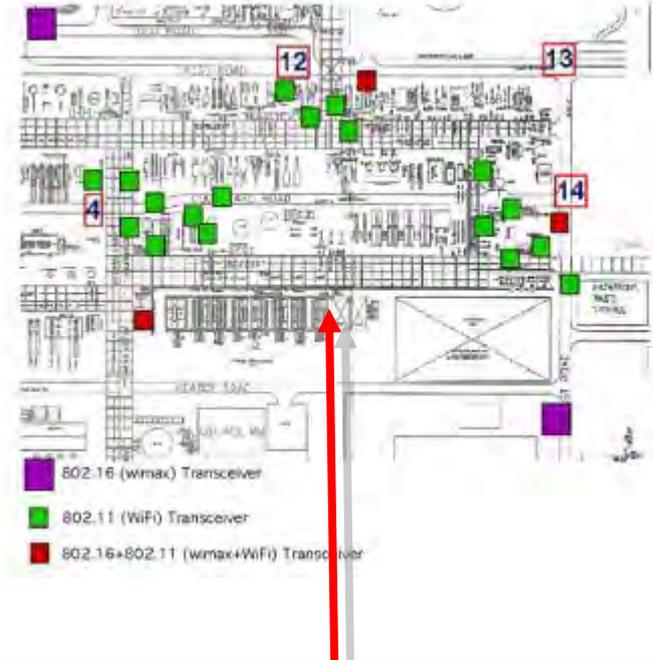
**Low Impact**  
**Highly Coordinated**  
**Non-Disruptive**  
**Comprehensive Report**

**(Inc. Strategic Alternatives & Recommended Action Plan)**

# SAS: Typical Report



**An Applications/Need Assessment**



**Recommendations for deployment locations of various types of wireless**



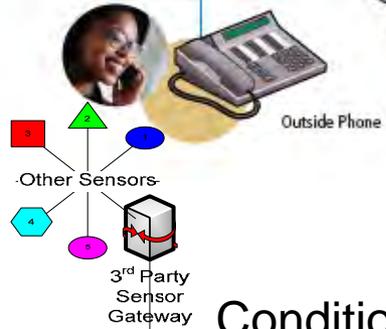
**RF Measurements and Coverage maps**

# Many solutions now become viable for the Industrial Environment

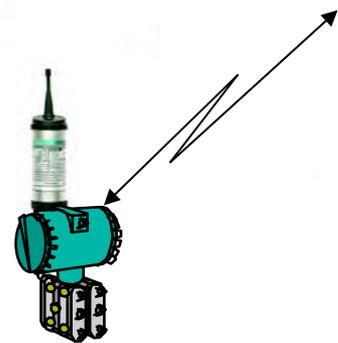
## Voice Communications – Employee Location



Process Alarms  
Enterprise Applications  
Field Data Logging



Condition Monitoring  
Asset Management

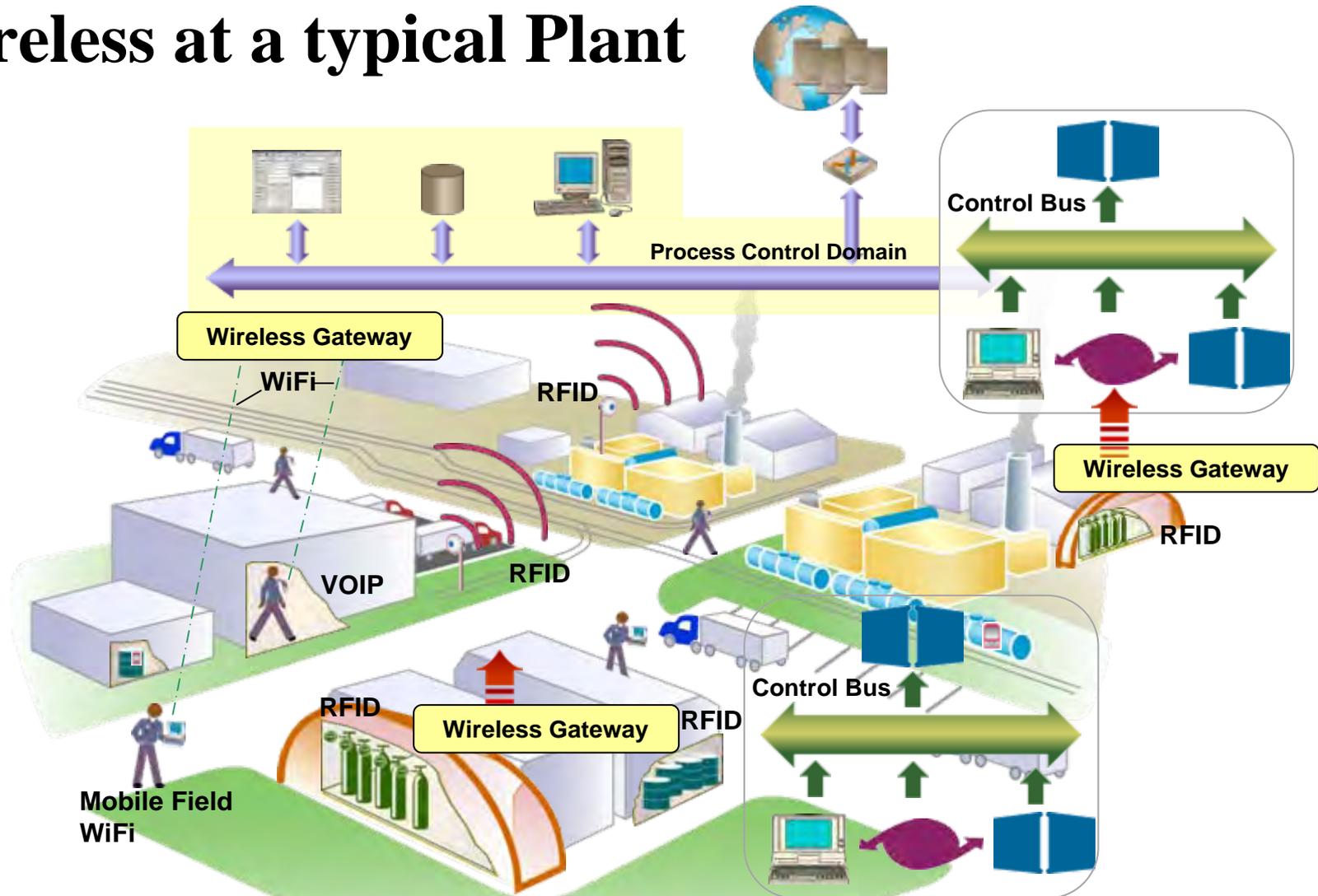


Process Measurements

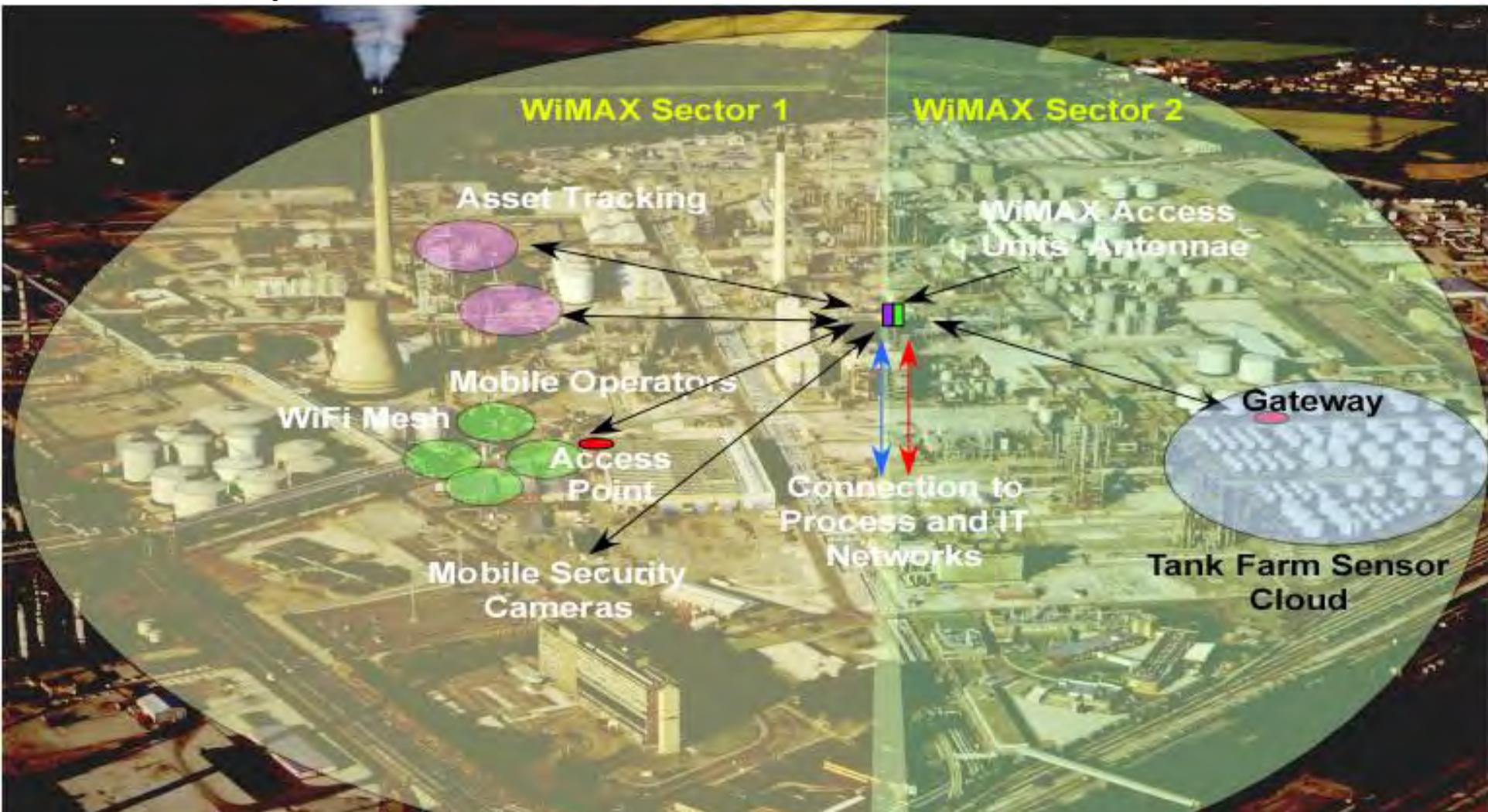


Industrial Video

# Wireless at a typical Plant



# This is NOT simply WiFi for Mobile Operators... It's A Facility-Wide Secure Infrastructure

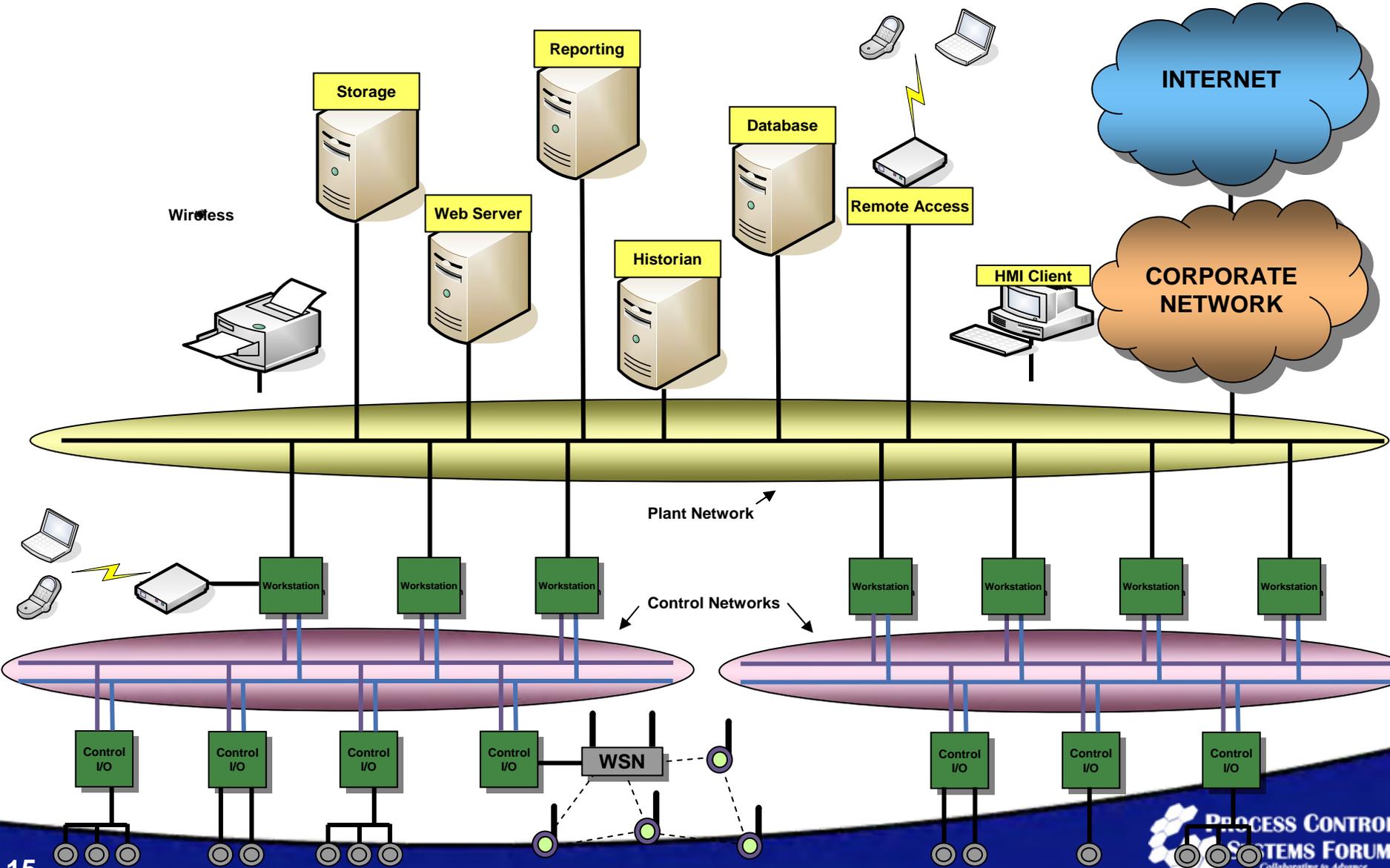


**Scalable, Secure Common Infrastructure. Add Apps ACROSS the plant**

# What's Important in a Process Control Environment

- ◆ **Safety**
- ◆ **Data Integrity**
- ◆ **Real-time Data**
- ◆ **Availability**
- ◆ **Production Uptime**
- ◆ **Regulatory Drivers**

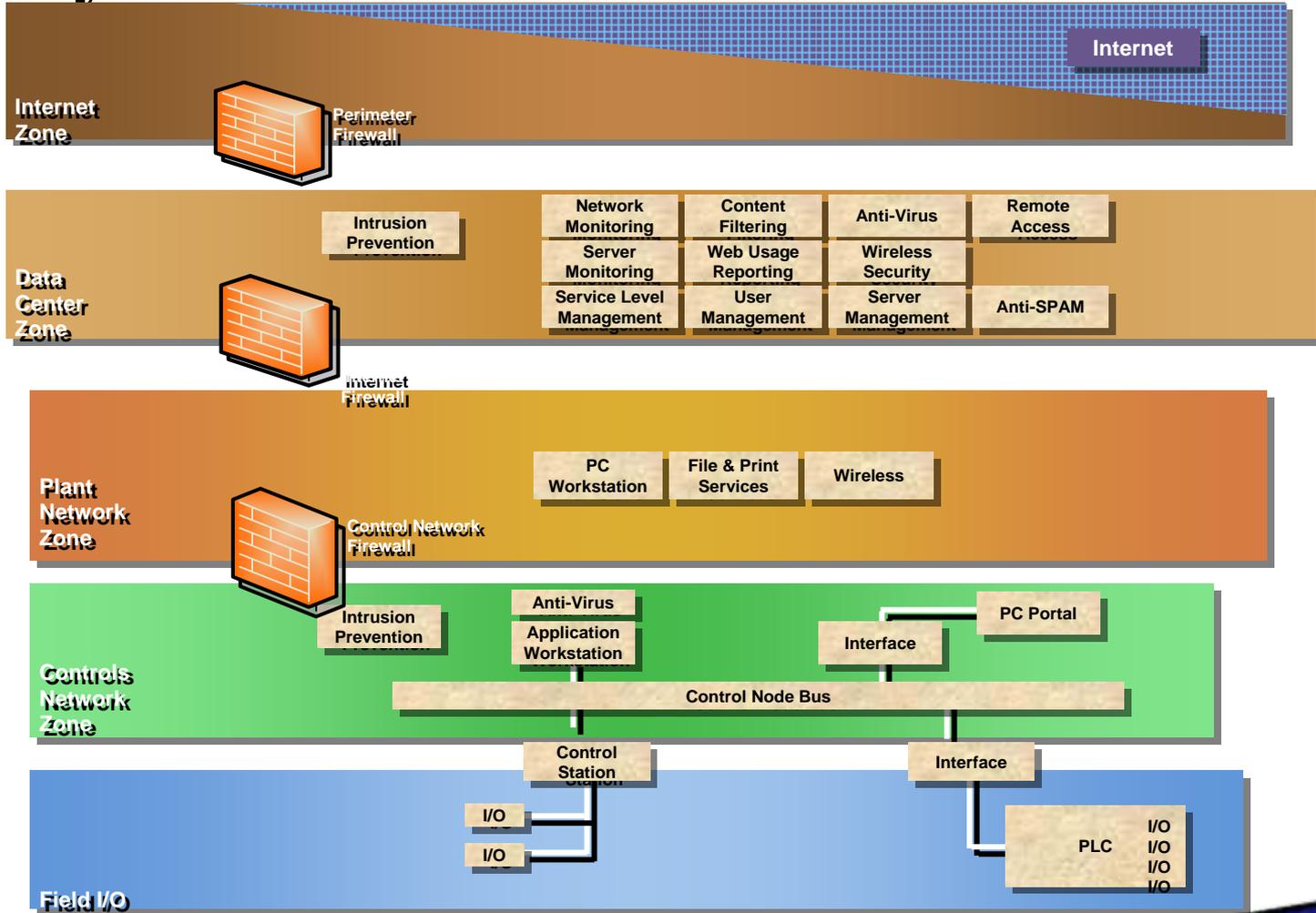
# The Modern Control System



# Basic Areas of Protection

- ◆ **Virus / Worm Protection**
- ◆ **Intrusion Detection / Prevention**
- ◆ **Firewall & DMZ Implementation / Configuration**
- ◆ **Remote Access / VPNs**
- ◆ **Physical Access Security**
- ◆ **Security Updates / Patches**
- ◆ **Security Policies**

# A Layered Defense



Multiple Zone Network

# Wireless ROI Survey



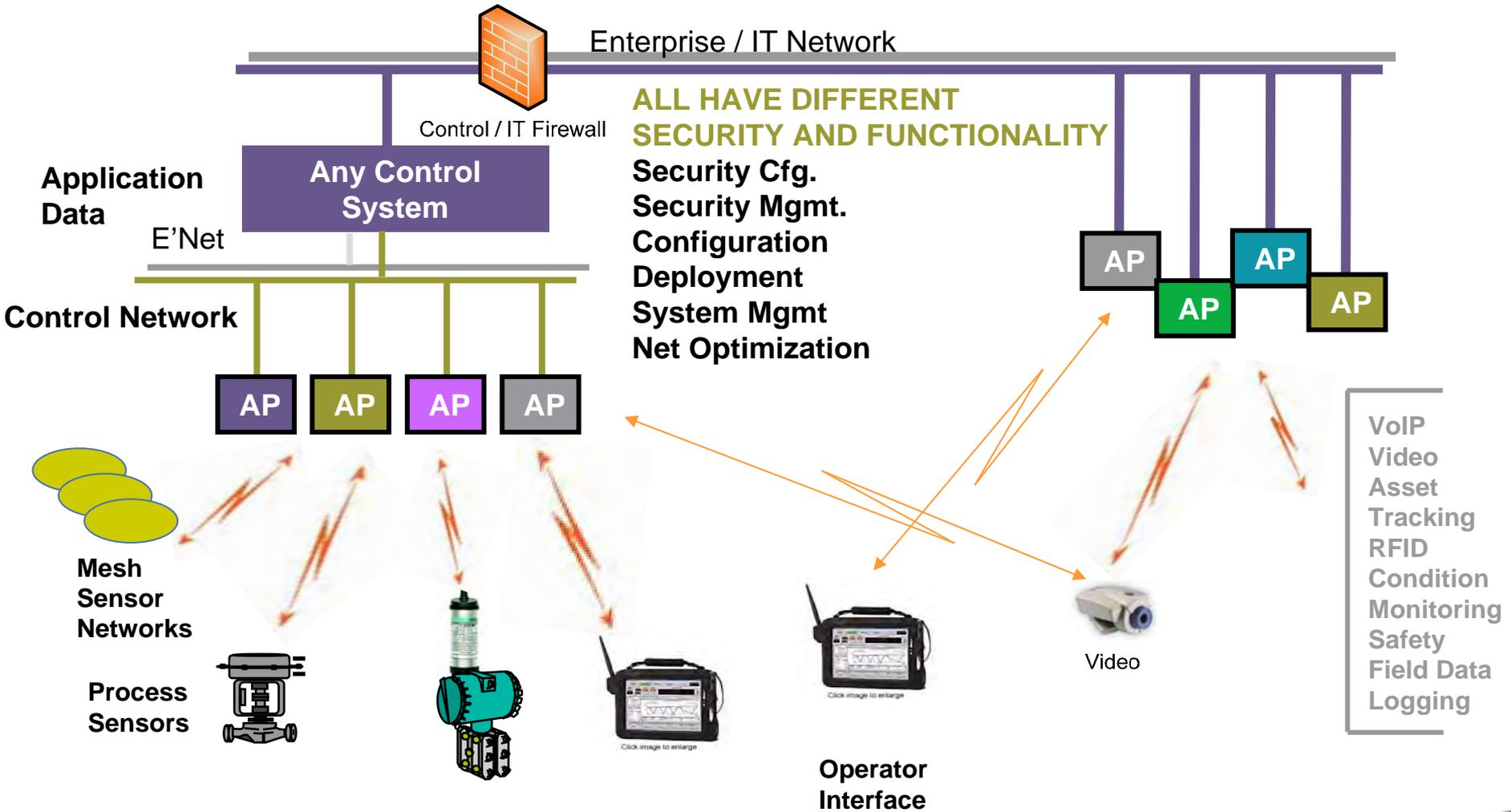
- ◆ **89% of the companies experienced a successful implementation.**
- ◆ **92% of respondents interviewed believe there is a definite economic and business benefit after installation.**
- ◆ **92% of respondents reported that they will continue to deploy wireless technology.**
- ◆ **Payback was less than one year, across all industries surveyed. (education, healthcare, manufacturing, retail, financial)**

# Wireless ROI

## ◆ Factors include:

- Cable vs AP's
  - Trenching \$\$\$
  - Cable Pulls - Surveillance
- Duplication of effort – Data Logging
- Availability of assets – RFID/RTLS
- Coverage – mobility
- Backhaul – circuit costs
- Mesh technology

# The Root Cause Barrier to Acceptance



Every vendor has their own security and management model  
This is impossible to manage for SECURITY

# The Reality of Wireless Technology

- ◆ **Difficult, variable security environment**
- ◆ **Incomplete & conflicting standards, frequencies, protocols**
- ◆ **Haphazard growth & inconsistent quality of point solutions**
- ◆ **Not industrial quality**
- ◆ **Poor migration path for investment preservation**
- ◆ **Inconsistent support within IT organizations**
- ◆ **Cost of operation uncertainties**
- ◆ **Network management challenges**



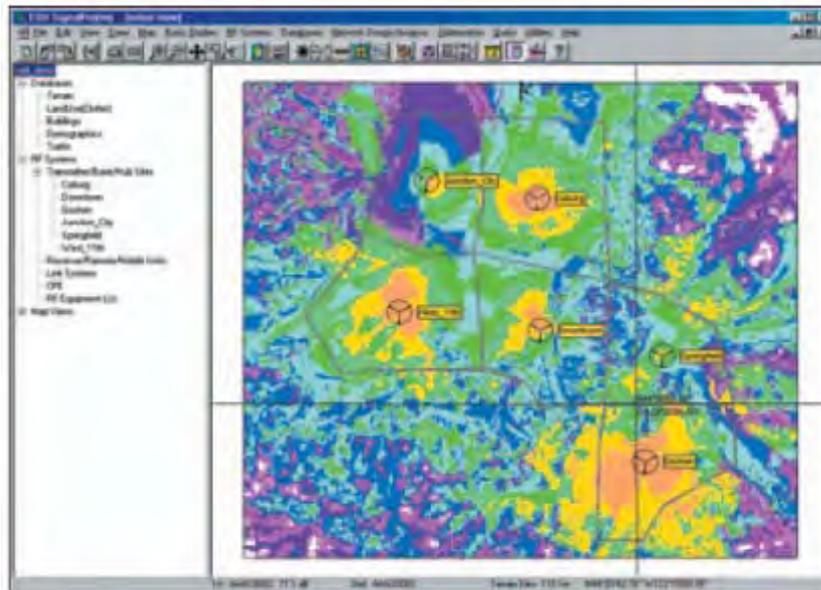
# Some Concerns for Plant Owners

- ◆ Reliability
- ◆ Licensing from Government
- ◆ Range
- ◆ Security
- ◆ Bandwidth
- ◆ Management
- ◆ Site Assessment and Consulting

# Some Concerns for Plant Owners: Reliability

## Reliability

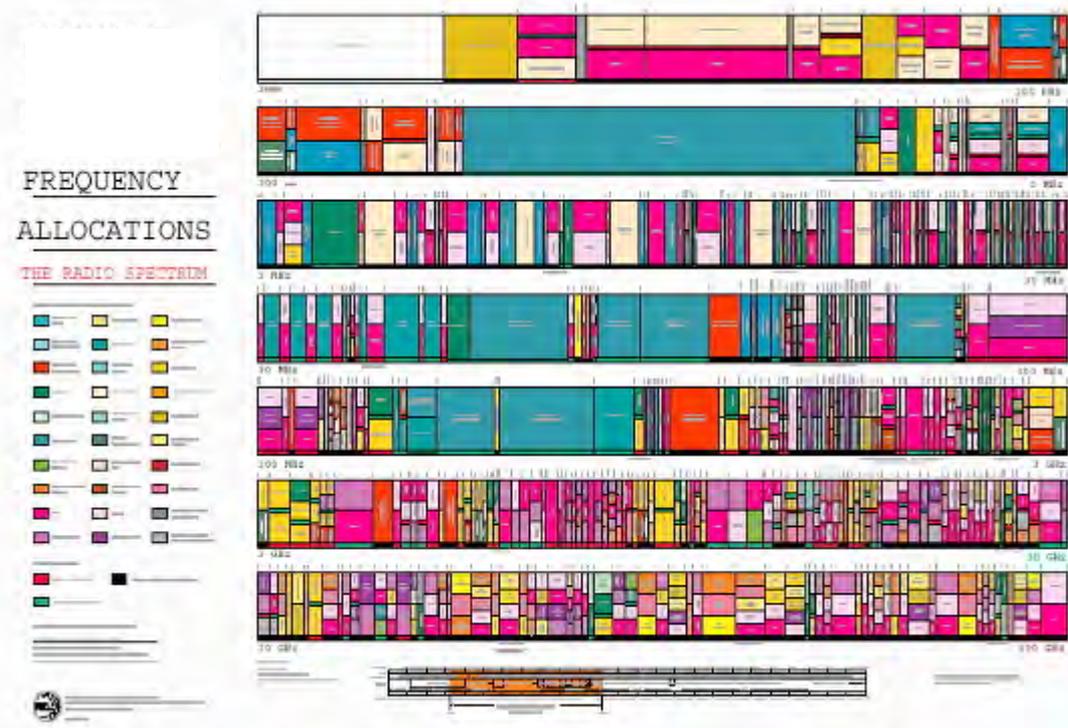
- A WiMax solution is designed to give a minimum bandwidth, at a certain distance considering the geographical layout and environmental conditions. The equipment, modulation techniques and error correction are selected



# Some Concerns for Plant Owners: Licensing from Government

- ◆ **Licensing from Government**

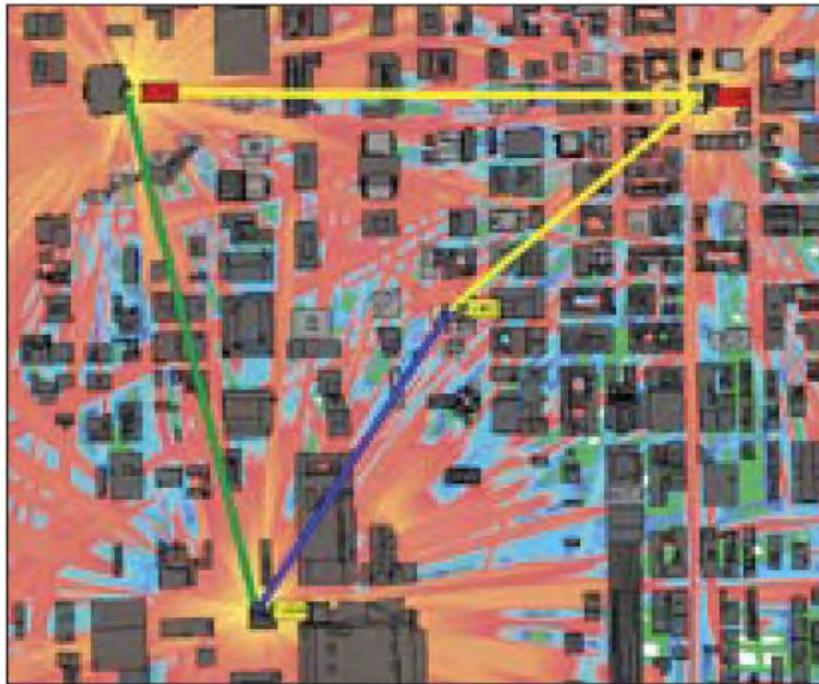
- If using the ISM bands at 2.4-2.5 GHz and 5.725-5.875 GHz, no. For all other frequencies, a license is required.



# Some Concerns for Plant Owners:Range

## Range

- The maximum distance is 50KM, but factors that will limit this distance are environmental, geographical, required reliability, required bandwidth and the frequency used.



# Some Concerns for Plant Owners: Security

## Security

- WiMax uses a combination of X.509 encryption for session establishment and 56-bit DES encryption for the transmission.

The screenshot shows the Merlin network analysis tool interface. The main window displays a list of transactions and protocol details. The transactions are as follows:

Trans	TYPE	T Addr	opcode	Length	Time
28	OBEX req	M 0x7	FGet	3	17.696s
29	OBEX res	S 0x7	Continue	485	17.799s
30	OBEX req	M 0x7	FGet	3	17.947s
31	OBEX res	S 0x7	OK	6	17.970s

Below the transactions, the protocol details for RFCOMM (Protocol 43) are shown:

Protocol	TYPE	T Addr	DLCI	C/R	Control	P/F	Length	Data	FCS	Time
43	RFCOMM	S 0x7	2	0	UIH	0	6	6 bytes	0x40	17.970s

The message details for the RFCOMM message (Message 64) are:

Message	L2CAP	T Addr	L2Len	L2CID	A	Data	Time
64	3 Pkts	S 0x7	10	Dyn: 0x0041	R	10 bytes	17.970s

The packet details for the three packets in the message are:

Packet	T Freq	Pre	CAC	Trail	Addr	DM1	Flow	Arqn	Seqn	HEC	L_CH	L2FL	Len
19788	S 2466	0x5	0xB077A3C55BB47D39	0xA	0x7	0x3	1	0	1	0xF5	..UAUI	1	14
41925	S 2411	0x5	0xB077A3C55BB47D39	0xA	0x7	0x3	1	0	0	0x10	..UAUI	1	0
41929	S 2439	0x5	0xB077A3C55BB47D39	0xA	0x7	0x3	1	0	1	0xF5	..UAUI	1	0

The CRC and Ack'd status for each packet are:

Packet	CRC	Ack'd	Idle	Time Stamp
19788	0x3192	Yes	274.000 µs	00017.970.4958
41925	0x57BB	Yes	439.000 µs	00030.248.2580
41929	0x57BB	Yes	439.000 µs	00030.249.5080

Finally, the transaction details for the last OBEX request (Trans 32) are:

Trans	TYPE	T Addr	opcode	Length	header	header value	header length	header value	Time
32	OBEX req	M 0x7	FGet	31	Conn ID	0	Name	23	30.215s

# Some Concerns for Plant Owners: Bandwidth

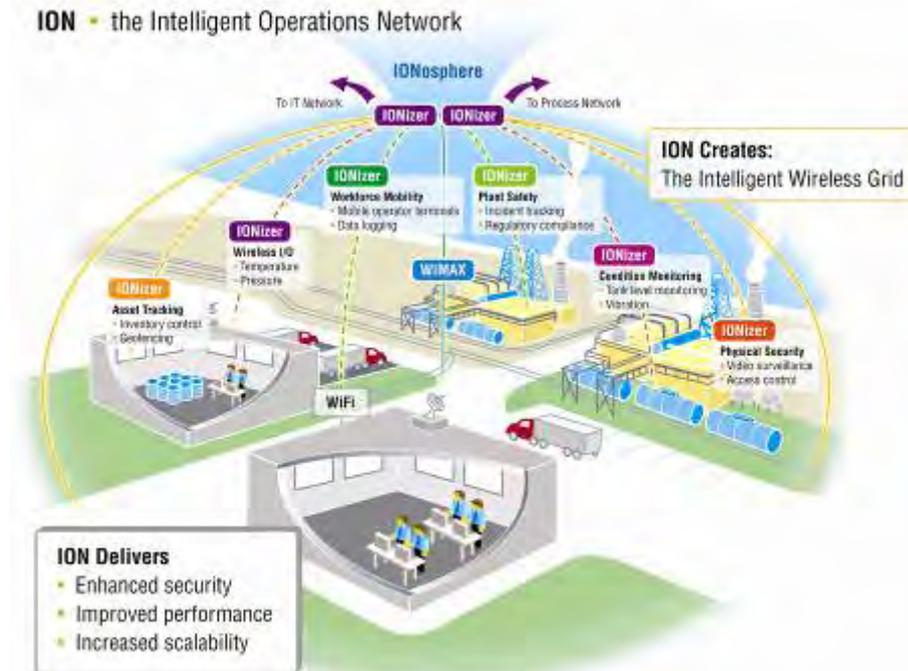
## Bandwidth

- The maximum is typically around 54Mb/s. The minimum is typically a factor of the model for designing the WiMax implementation. Typically the minimum bandwidth required is determined, and the worst case considered to keep actual bandwidth at or above the minimum. The frequency and channel bandwidth will also affect this.



# Some Concerns for Plant Owners: Management Management

- The Network Management server provides a common interface for the management of all wireless devices. It can be used to manage the entire wireless infrastructure, which typically is a combination of several wireless technologies and vendors.



# Some Concerns for Plant Owners: Site Assessment and Consulting

## RF Spectrum and “neighbors” in same space

