Paul Mercier, Senior Project Sales Engineer – Phoenix Contact USA

Making Wireless Reliable and Secure

Agenda

- Background
- Industrial Communications
- Wireless Radio 101
- Choosing Wireless Technologies
- Resiliency, Reliability and Security
- Need for Cybersecurity
- AWWA Cybersecurity Guidance & Tool

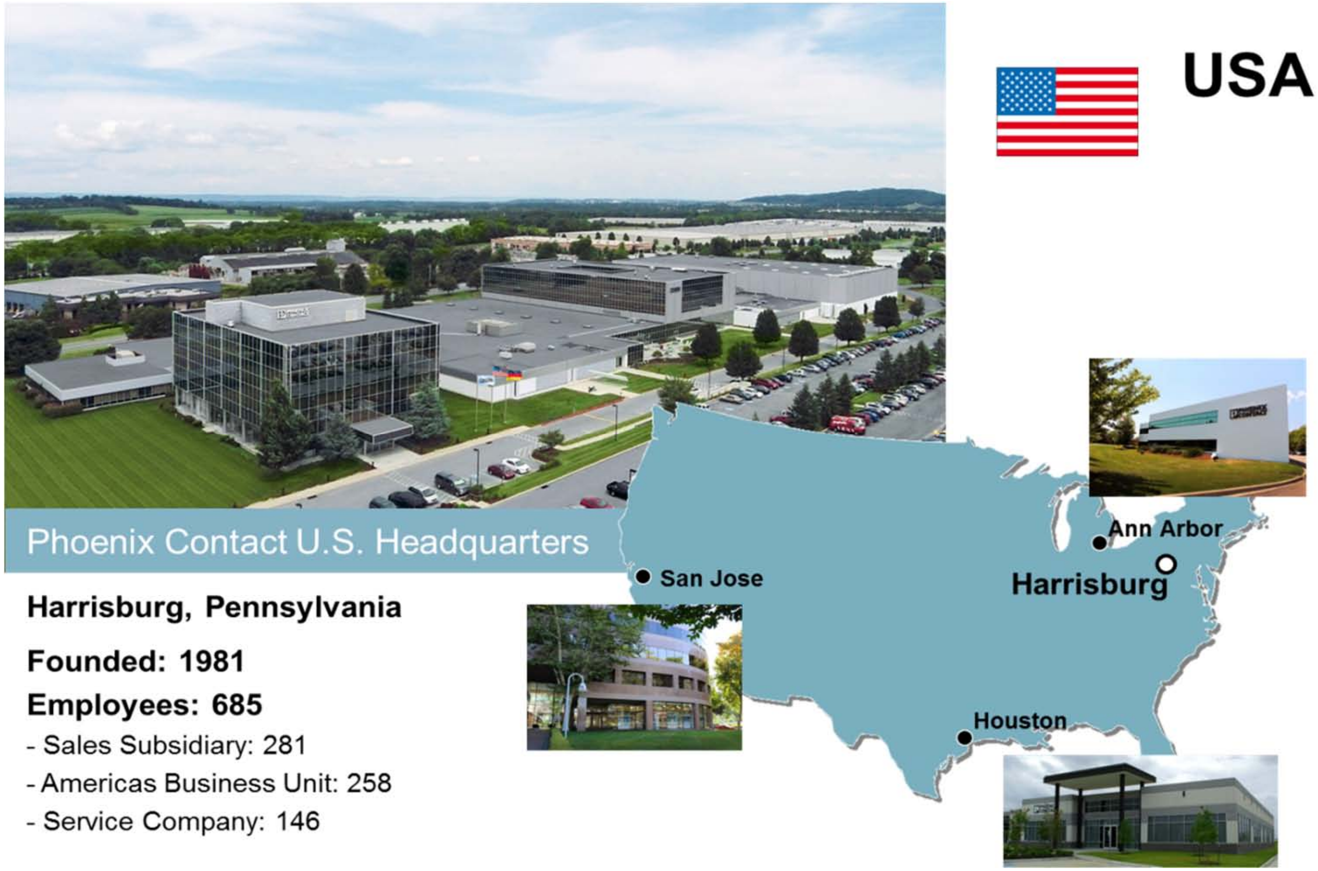
Corporate Overview

Corporate Headquarters, Germany

Corporate Overview

US Headquarters

USA



Harrisburg, Pennsylvania

Founded: 1981

Employees: 685

- Sales Subsidiary: 281
- Americas Business Unit: 258
- Service Company: 146

Corporate Overview

US Engineering and Manufacturing Facility

Water/Wastewater Industry

- Terminal Blocks
- Power Supplies & UPS
- Surge Protection
- Signal Isolators and Conditioners
- Ethernet Switches
- Industrial PCs
- Wireless

PHOENIX CONTACT’s wireless products

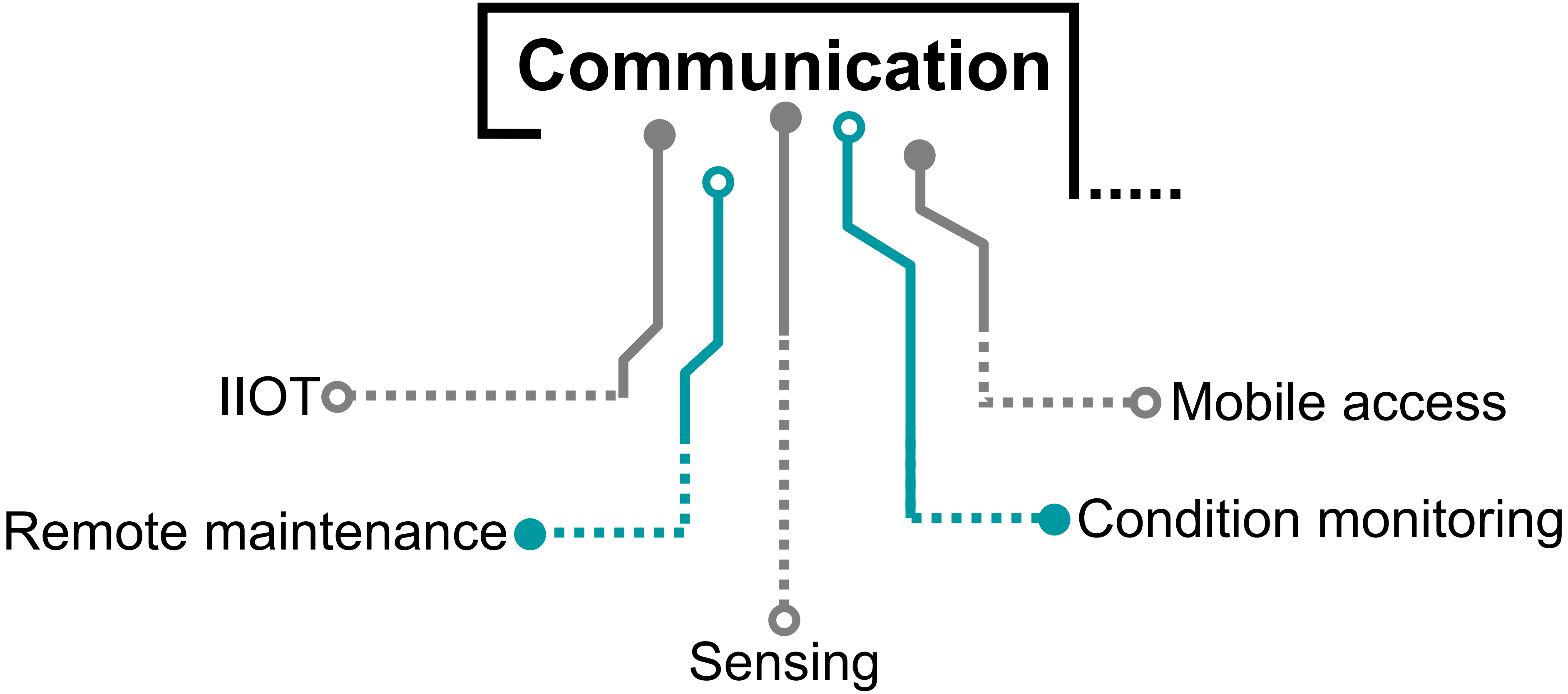
Wireless Sensors

Wireless I/O

SCADA 900MHz
& Cellular

Wireless LAN

Communication



IIOT

Mobile access

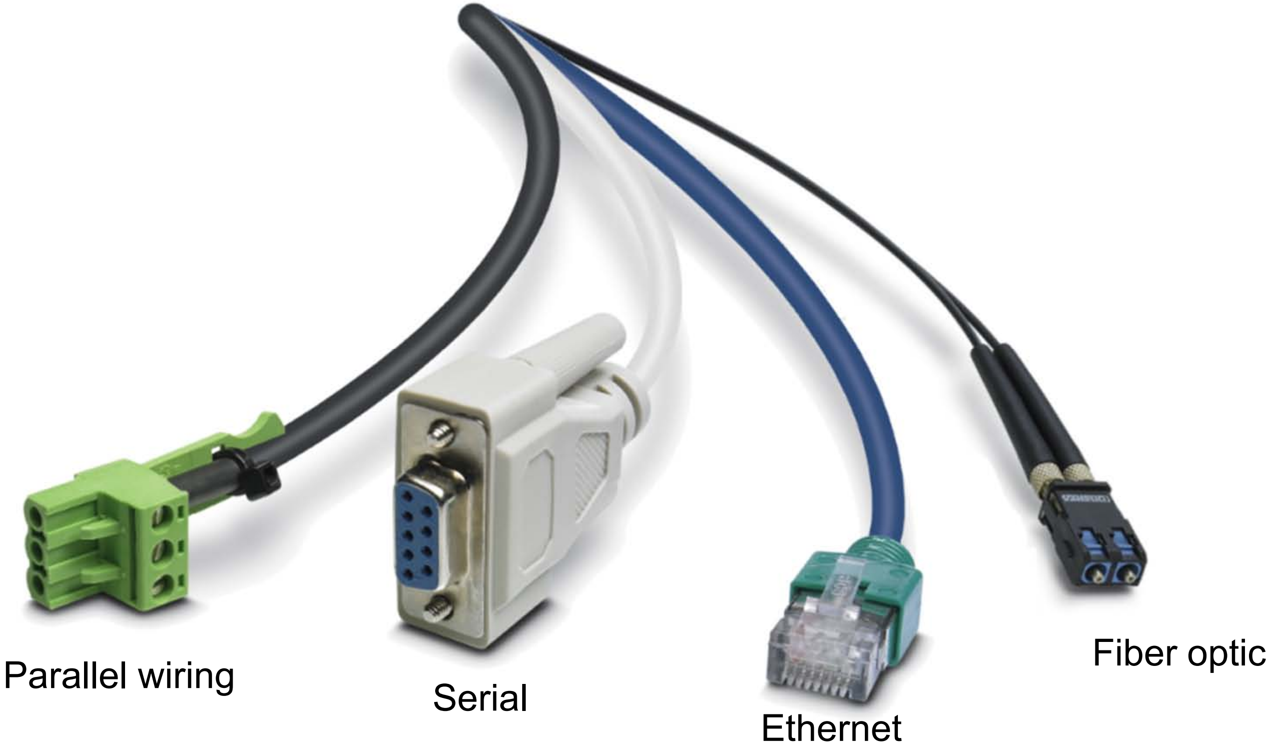
Remote maintenance

Condition monitoring

Sensing

Traditional methods of industrial communication

Traditional methods of industrial communication



Traditional methods of industrial communication

SneakerNet

BikeNet^{TM}

ChevyTruckNet®

Challenges with hard wired solutions?

deployment time

I/O capacity

cost

distance

cable damage

infrequent measurements

IS THERE A RELIABLE COMMUNICATION ALTERNATIVE?

Lose the wires,
not the signals

ONE SIZE FITS ALL: GREAT FOR SOCKS, BAD FOR WIRELESS.

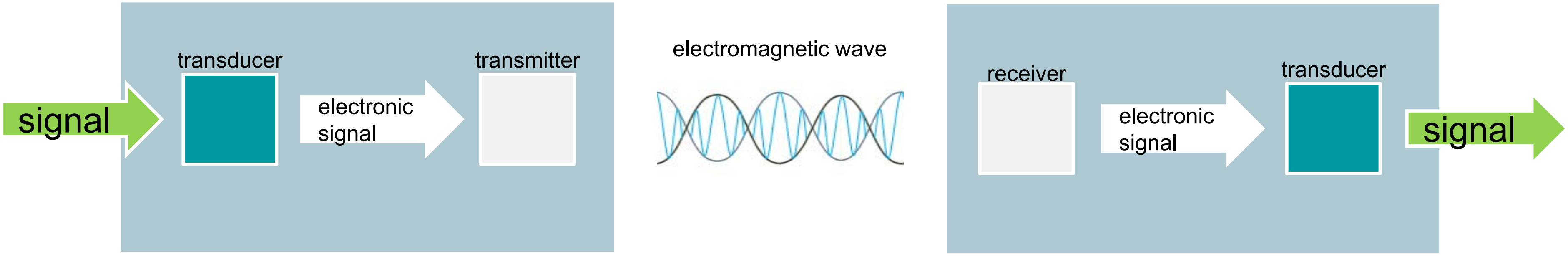
Identifying potential wireless use case

Deployment time	• New construction and plant updates, addition of new measurement points
I/O capacity	• DCS/PLC systems with full chassis or I/O cards. Non-critical points can be un-wired and run via radio to free up I/O points for critical measurements • Maxed out Ethernet switches may indicate need for WLAN
Cable damage	• Rodent damage to cables/fiber optics • Heavy equipment • Failed leased lines
Cost	• Cable and conduit in a hazardous area can be $1000/ft • Addition of new remote monitoring locations, avoid adding a local controller
Distance	• Bicycle and truck rounds to remote sites or plant cells • Leased lines • End of life wireless stations (old VHF, UHF, etc)
Mobile equipment	• Maintenance with tablets or laptops for temporary connection • Temporary equipment for troubleshooting or start up • Rental equipment and skids • AGVs
Infrequent measurements	• Employees making rounds with tablets or clipboards for manual measurements • Bicycle and truck rounds to remote sites or plant cells

Physics of Radio

PART I

What is a radio?



RF power

measured in Watts or dBm

$$\text{dBm}=10*\log(X\text{mW})$$

- indicates RF transmitter power output
- also indicates the minimum signal a receiver can hear

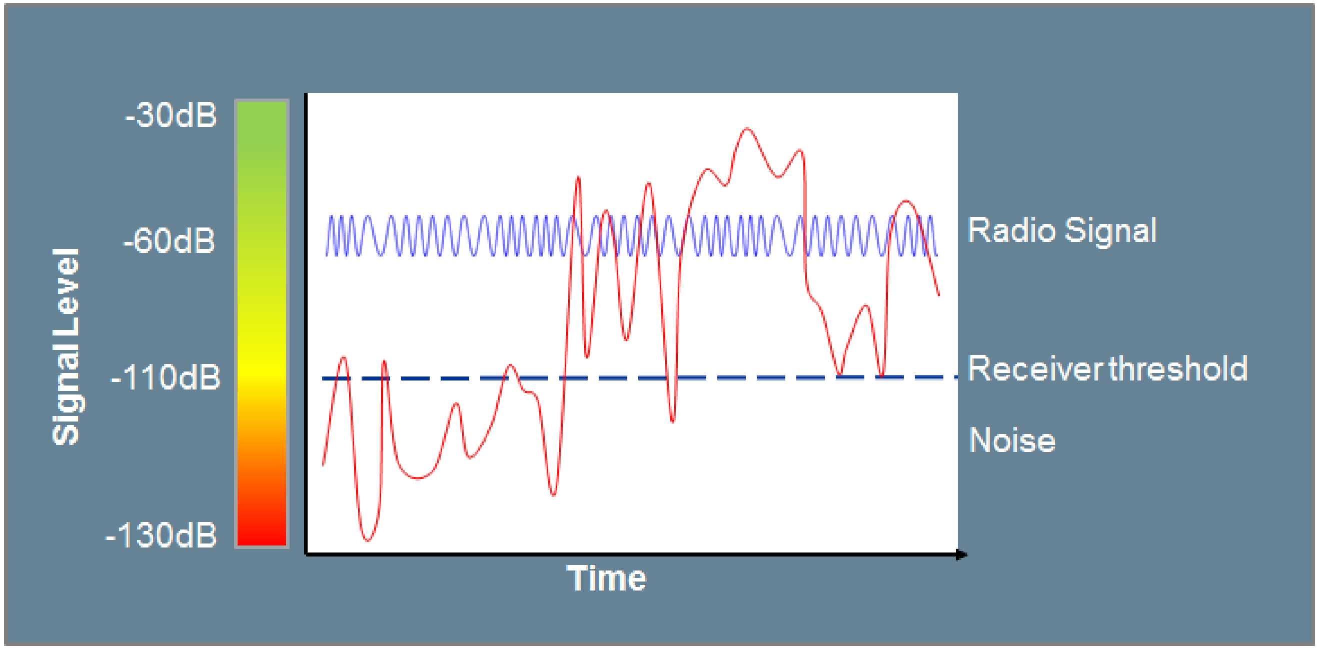
Milliwatt	dBm
0.001mW	-30dBm
0.01mW	-20dBm
0.1mW	-10dBm
1mW	0dBm
10mW	10dBm
100mW	20dBm
1000mW	30dBm

- dBm is a logarithmic value
- a 3dBm increase is 2x mW

Milliwatt	dBm
10mW	10dBm
20mW	13dBm
50mW	17dBm
100mW	20dBm
500mW	27dBm
1000mW	30dBm

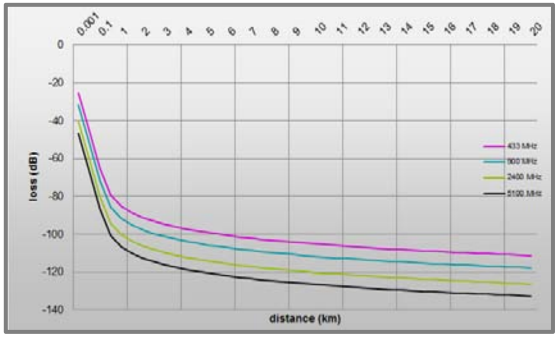
Receive Signal

a radio signal becomes unreliable when the level falls below the receiver sensitivity threshold



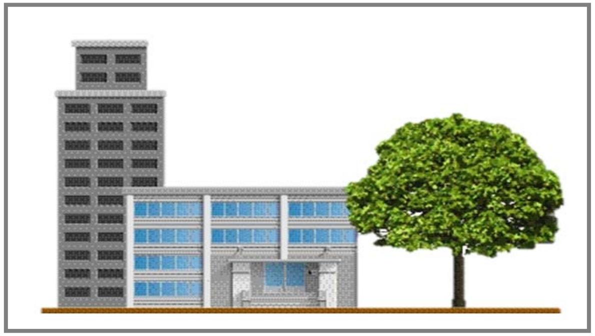
RF signal loss

attenuation is caused by several factors



free space

loss=32.4+20log(f_{MHz})+20log(d_{km})



obstructions

buildings, trees, etc

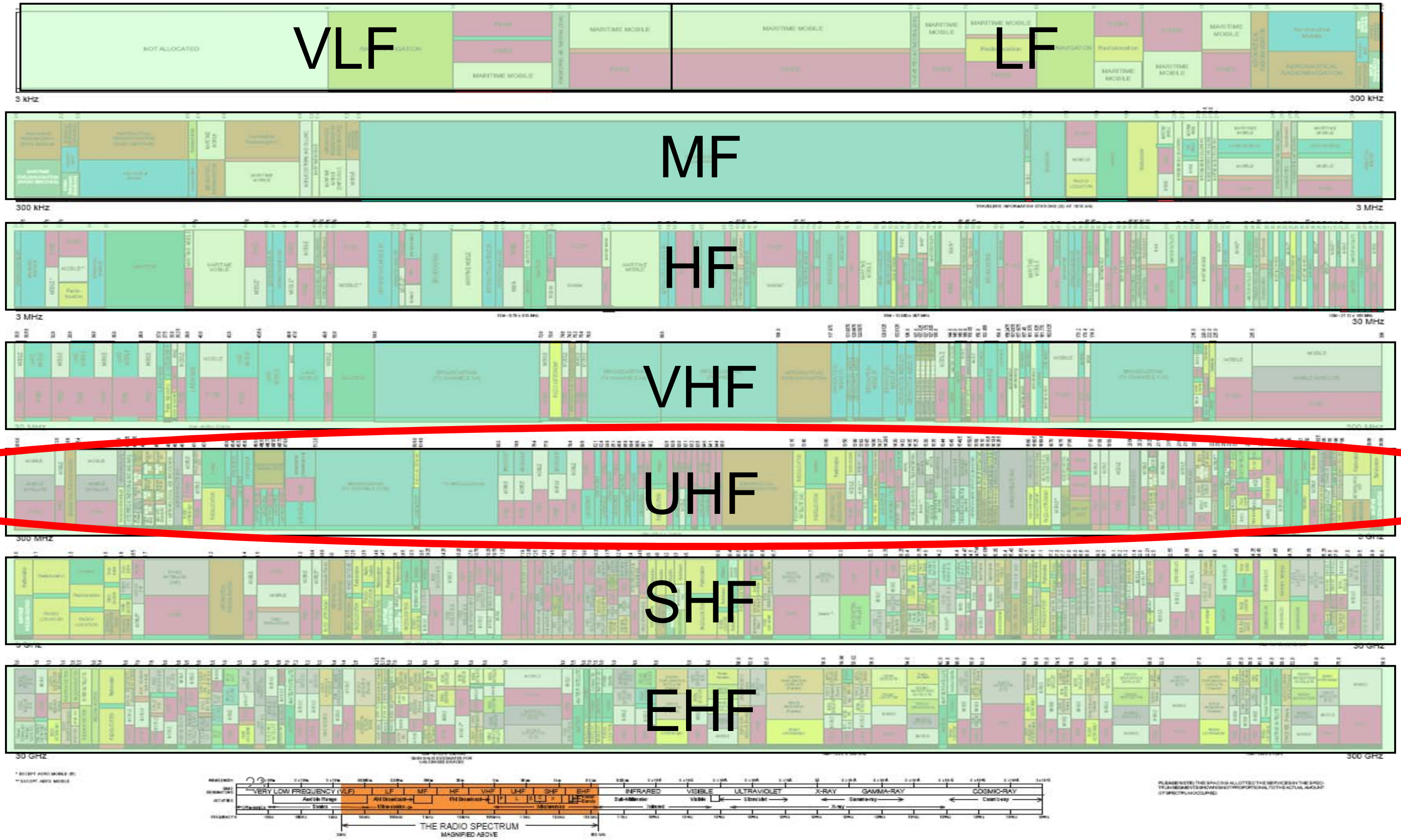
coaxial

cables, adapters, attenuators, etc.

Choosing a Wireless Technology

PART II

Radio Frequencies
What’s in our spectrum



What’s in the UHF band 300-3000MHz

- Cellular
  - 850MHz -USA
  - 900MHz -Europe
  - 1800MHz -Europe
  - 1900MHz -USA
- Licensed Radio solutions
  - 400MHz Range
  - 700MHz
  - 900MHz Range
- Unlicensed Radio solutions
  - 900MHz
  - 2.4GHz

Wireless Breakdown

- All wireless technology can be defined as either a Public Standard System or Proprietary System.

  - **Public Standard:** A governing body exists to create/certify a specification to guarantee interoperability between manufacturer's devices.
    - Radio "language" is known
    - Equipment is readily available
    - Encryption is the only protection
    - Examples: 802.11 (**Wi-Fi**), 802.15.1 (**Bluetooth**), 802.15.4 (**Zigbee**)

Wireless Breakdown

- All wireless technology can be defined as either a Public Standard System or Proprietary System.

  - **Proprietary System:** The manufacturer controls the design so that the product will only work with other devices from that manufacturer
    - System only known by manufacture (inherently secure)
    - Not subject to public interference
    - Encryption helps although it may not be necessary
    - Designed for specific applications
    - Examples: Motorola Canopy, GE MDS iNEt, Freewave HHT, Phoenix TWE

Wireless Breakdown

- All wireless can be broken down into Fixed Frequency or Spread Spectrum technology
  - **Fixed Frequency:** Defined as having a specific frequency that is used during RF communications. Typically dedicated frequencies will be used for receiving and transmitting of RF signals.
    - Advantage: Generally frequencies are licensed and there will be little to no interference in the system providing for robust communications.
    - Disadvantage: Licensed frequencies have associated fees. Also, if other radios or interference does enter the system RF comms can become useless.
    - Used primarily for long distance applications (5-40 miles) where Spread Spectrum technologies do not work.

Wireless Breakdown

- All wireless can be broken down into Fixed Frequency or Spread Spectrum technology
  - **Spread Spectrum:** A method of transmitting a signal by "spreading" it over a broad range of frequencies much wider than the minimum bandwidth needed to transmit
    - Advantage: Works well in high interference areas, reduces needed transmit power, and allows for multiple networks to occupy the same RF space
    - Disadvantage: Lower throughputs
    - Used in most applications today because of increased performance over Fixed frequency technology

Wireless Breakdown

- One last criteria that is used to define wireless systems is the frequency at which they operate. This is typically defined as Licensed frequencies or Un-Licensed frequencies.

  - **Licensed Frequencies:** Require applications to be filed and typically fees to be paid.
    - Advantage: In general the licensed RF system should be free of interference. There is legal recourse for any rogue system causing interference.
    - Disadvantage: Fees must be paid to maintain the system. Frequency bandwidths are typically small and do not allow for fast data rates. Available frequency are limited and can be hard to find.

Wireless Breakdown

- One last criteria that is used to define wireless systems is the frequency at which they operate. This is typically defined as Licensed frequencies or Un-Licensed frequencies.

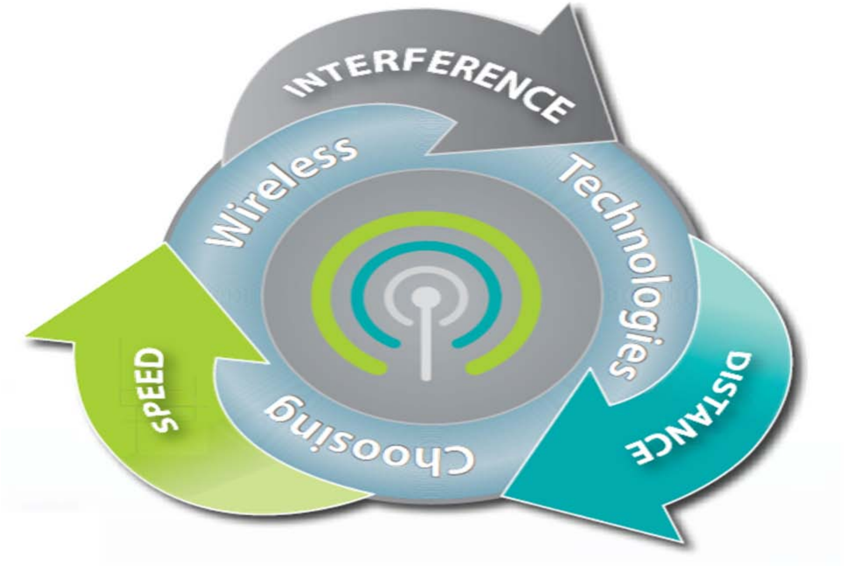
  - **Un-Licensed Frequencies:** Frequencies defined by the FCC as license free which are known as the ISM bands.
    - Advantage: No fees associated with using the frequencies
    - Disadvantage: Many different RF systems operate in these frequencies. Interference and system Co-Existence is critical.

Choosing Wireless Technology

- The decision is made much easier by outlining the requirements for a product and technology
  - RF Requirements
  - Network Topology
  - Device Connectivity
  - Network Size

There is no one-size-fits-all for wireless!!

Wireless Performance

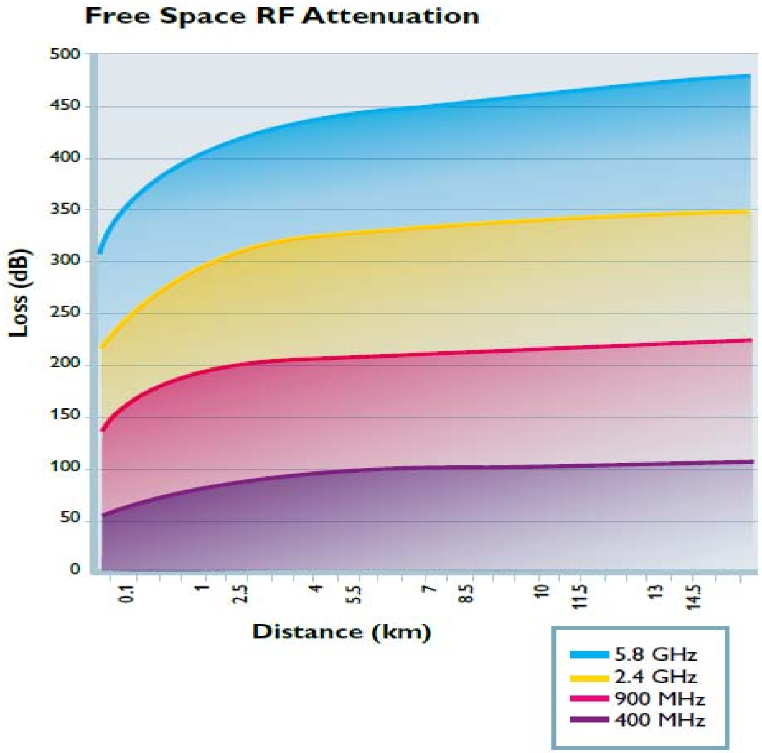


- There are several key factors in determining a technology's performance
  - Distance
  - Data rate/volume
  - Interference

- All 3 are interdependent

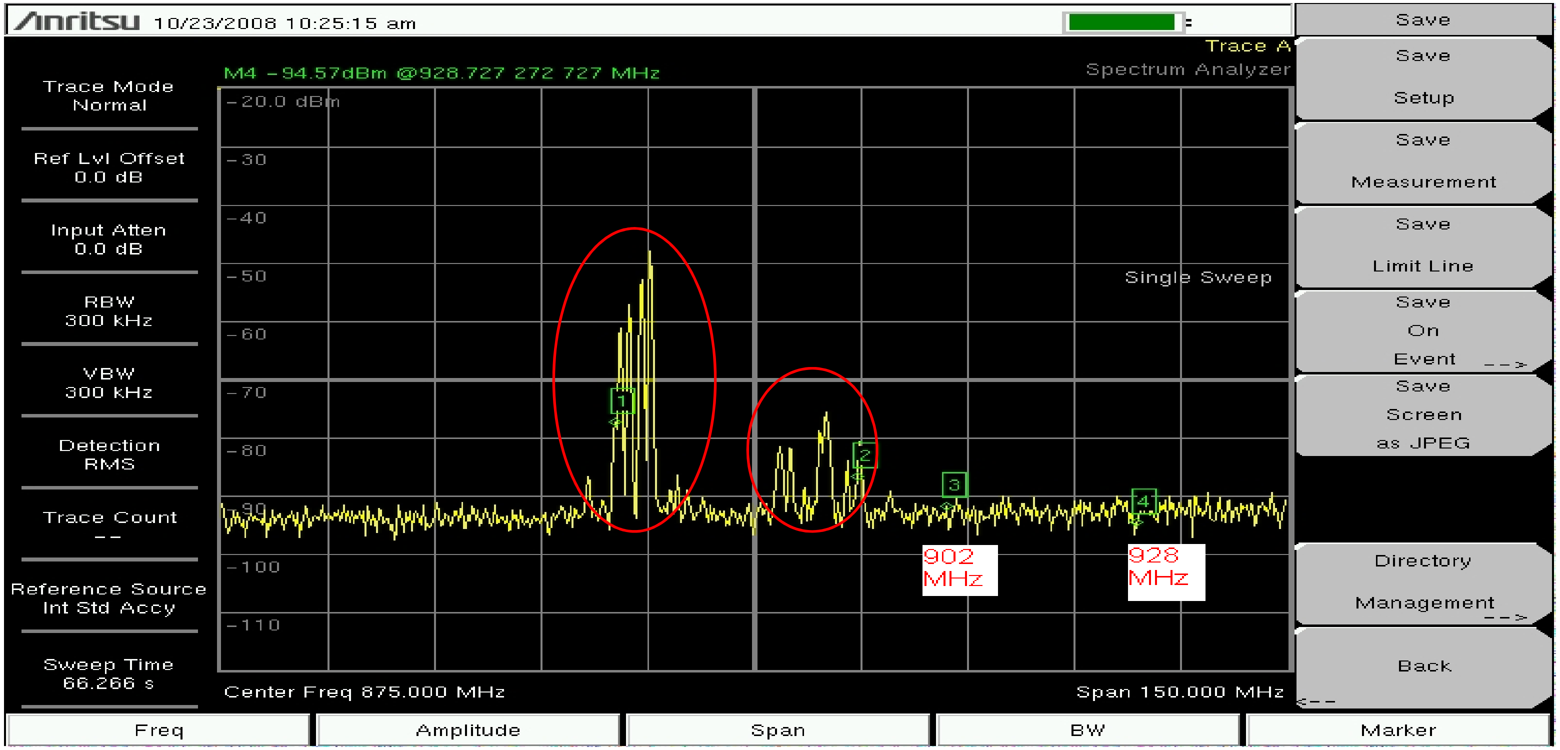
- Users must find the correct balance

Range



- Transmission range is affected by:
  - Operating frequency: as frequency increases, range decreases
  - Over-the-air speed: as speed increases, range decreases
  - Interference: as interference increases, range decreases
  - RF Power: Higher power goes farther, may be limited by technology or government

Interference



Anritsu 10/23/2008 10:25:15 am

M4 -94.57dBm @928.727 272 727 MHz

Trace Mode Normal

Ref Lvl Offset 0.0 dB

Input Atten 0.0 dB

RBW 300 kHz

VBW 300 kHz

Detection RMS

Trace Count --

Reference Source Int Std Accy

Sweep Time 66.266 s

Center Freq 875.000 MHz

Span 150.000 MHz

Single Sweep

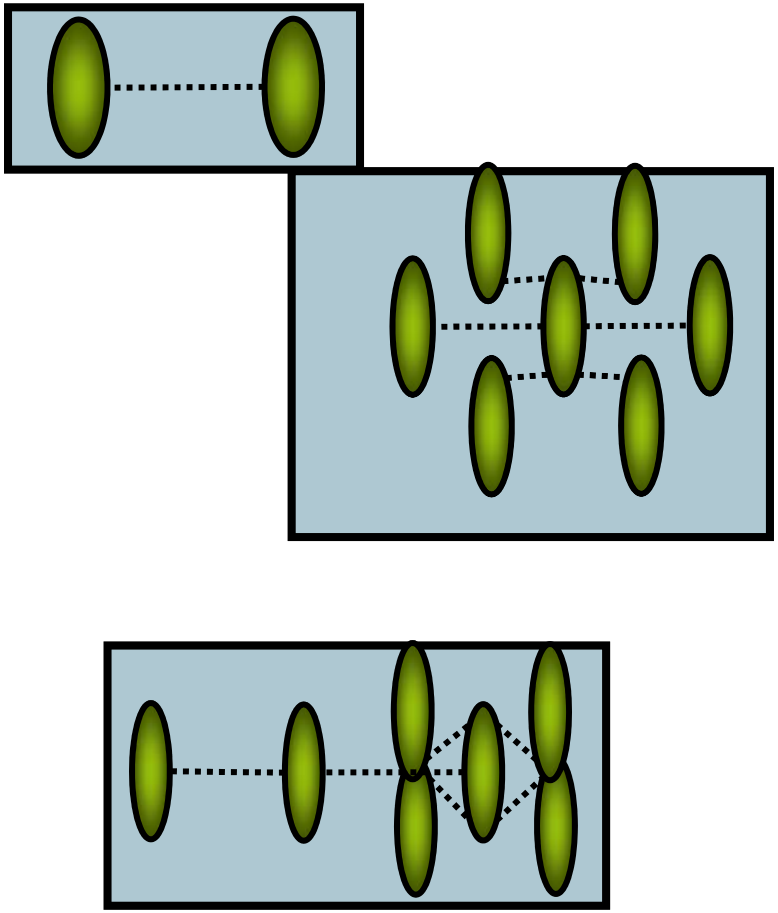
Choosing Wireless Technology

- The decision is made much easier by outlining the requirements for a product and technology

  - RF Requirements
  - Network Topology
  - Device Connectivity
  - Network Size

Network Topologies

- **Point-to-Point**
  - Information is exchanged between 2 points
- **Star / Point-to-Multipoint**
  - A central station communicates with multiple remote devices
- **Repeaters**
  - Repeaters receive and retransmit the weak or low-level signal at a higher level so that the signal can cover longer distances or avoid obstacles

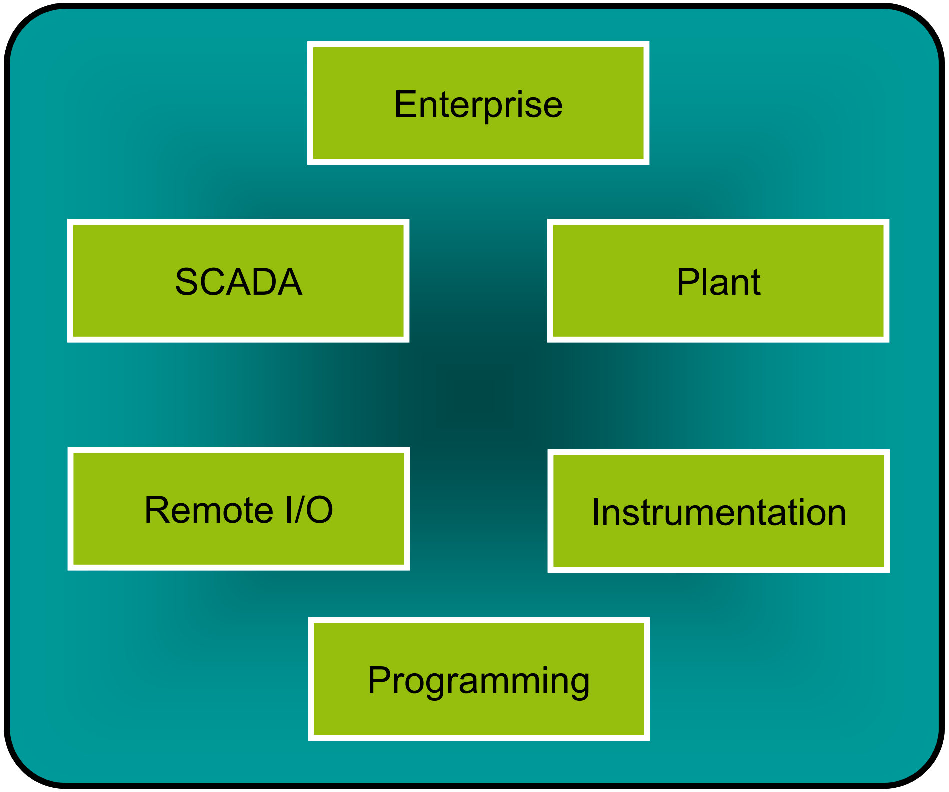


Choosing Wireless Technology

- The decision is made much easier by outlining the requirements for a product and technology

  - RF Requirements
  - Network Topology
  - Device Connectivity
  - Network Size

Device Connectivity



Enterprise

SCADA

Plant

Remote I/O

Instrumentation

Programming

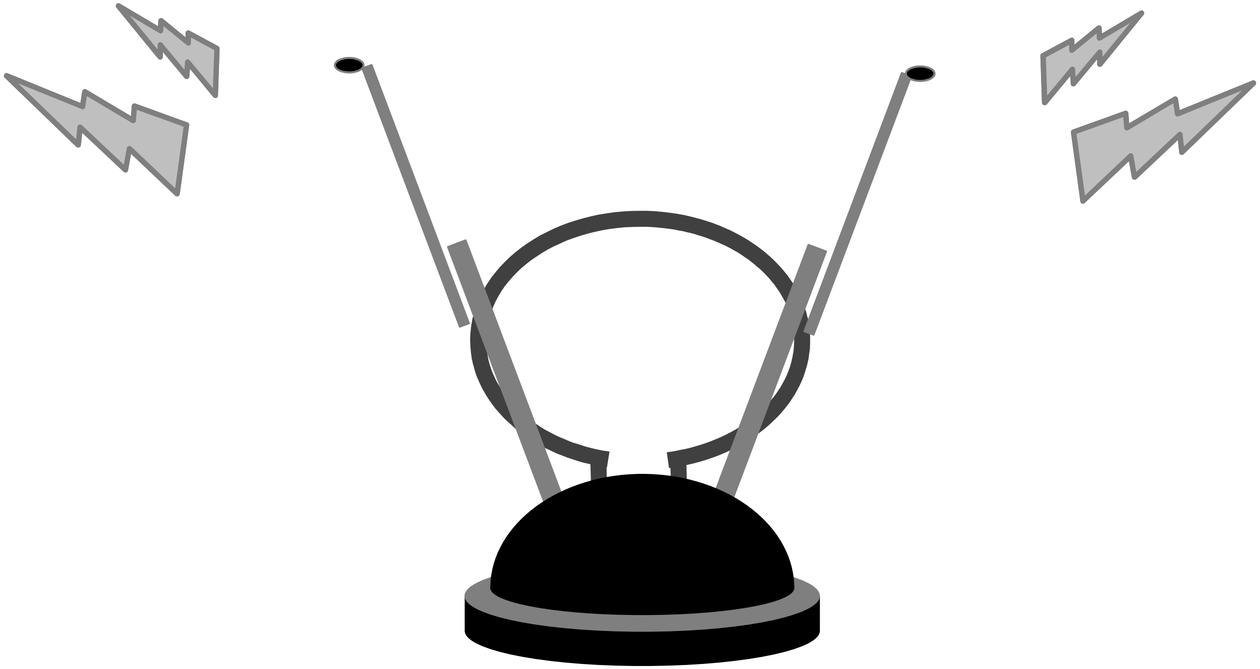
- What type of data?
  - Ethernet
  - Serial
  - I/O
- How much data?
  - Megabytes or kilobytes
  - Bytes or bits
- Use case
  - Convenience
  - Monitoring
  - Control

Antenna Basics

PART III

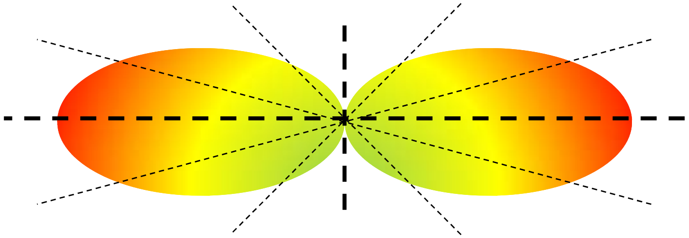
More than tin foil and rabbit ears?

an antenna converts radio frequency electrical energy to an electromagnetic wave propagated into space (a “radiator”)

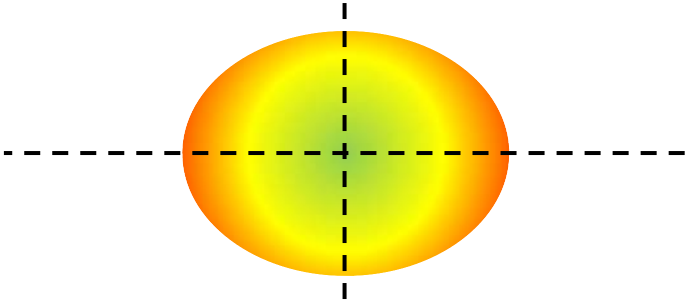


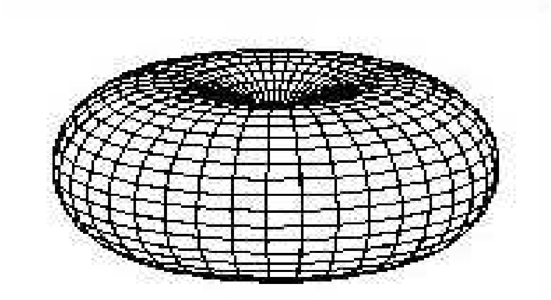
Omni antennas

radiate RF energy in all directions



horizontal

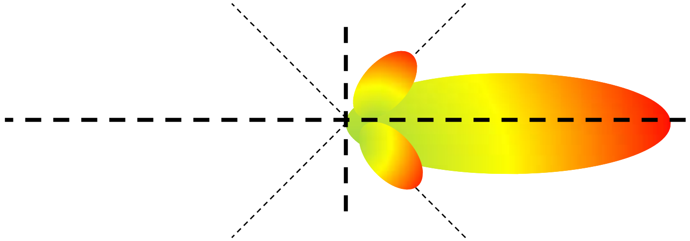




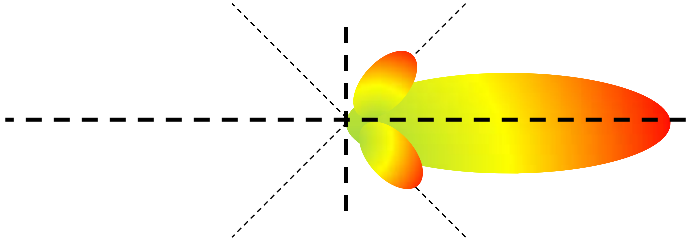
- Horizontal radiation pattern resembles a donut centered around the antenna
  - As the gain increases, the donut flattens
- Vertical radiation pattern is round (or nearly so)
- Use for the base station and repeaters

Directional antennas

radiate RF energy in a specific direction



horizontal

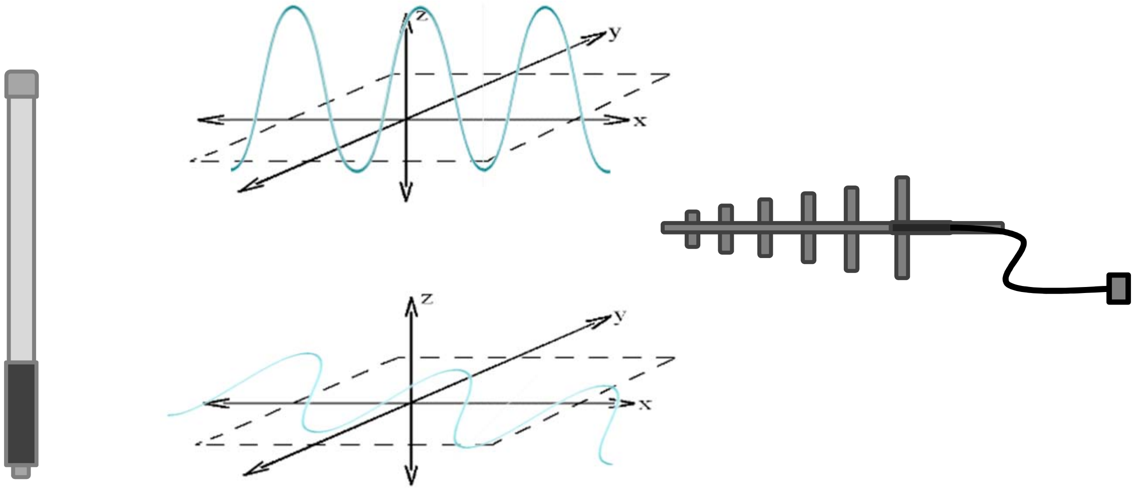


vertical

- Radiate RF energy in a given direction
- Horizontal and vertical radiation pattern is like a flashlight beam
  - As the gain increases, the beam narrows
- Common types are Yagi, Panel, Sector and Parabolic antenna
- Use for remote sites

Antenna polarization

cross-polarization introduces approximately 30dB of attenuation

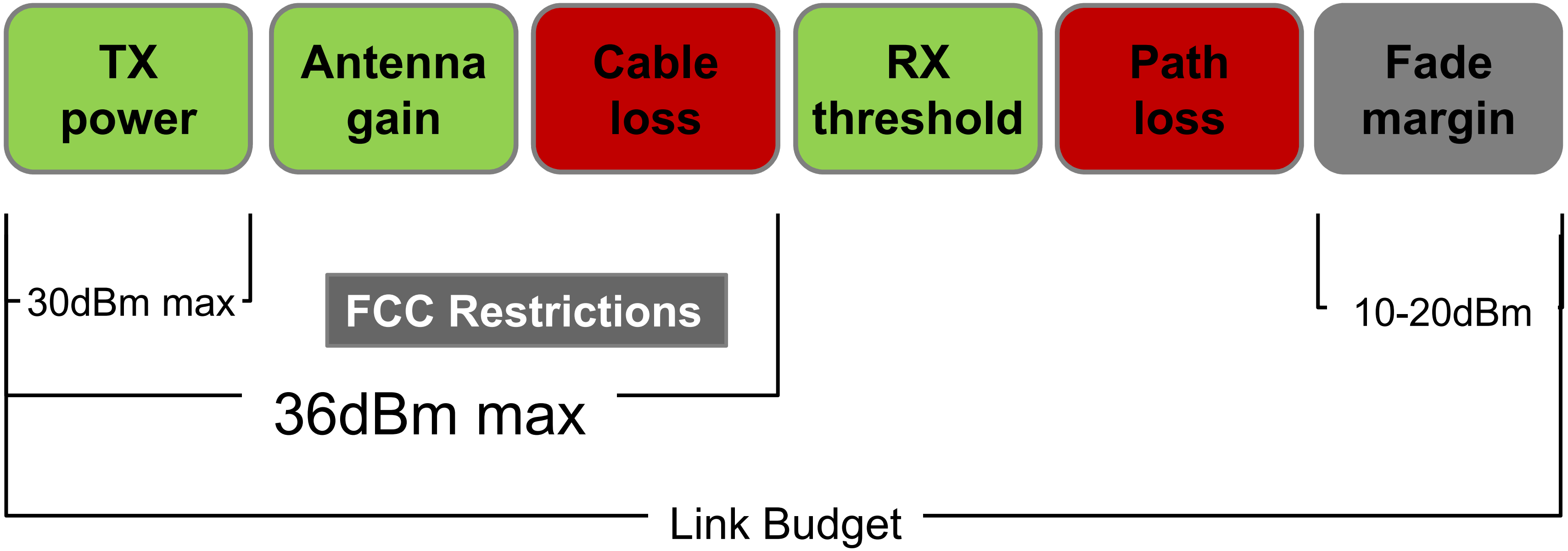


Vertical polarization
The “H” plane

Horizontal polarization
The “E” plane

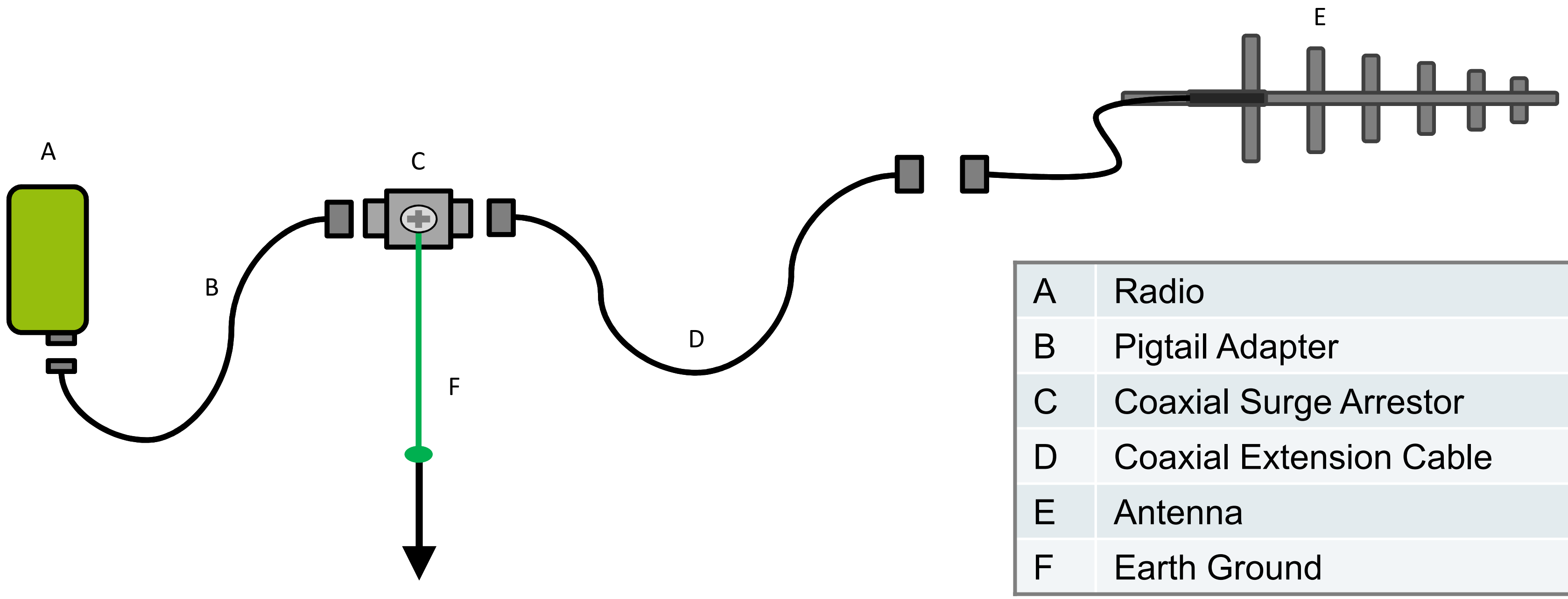
Link budget of un-licensed type radio

the total of all the RF signal gains and losses in a wireless link



Put it all together

a typical radio and antenna system

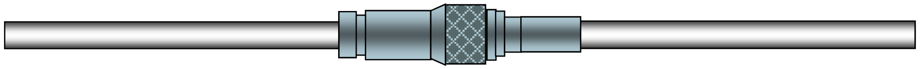


A	Radio
B	Pigtail Adapter
C	Coaxial Surge Arrestor
D	Coaxial Extension Cable
E	Antenna
F	Earth Ground

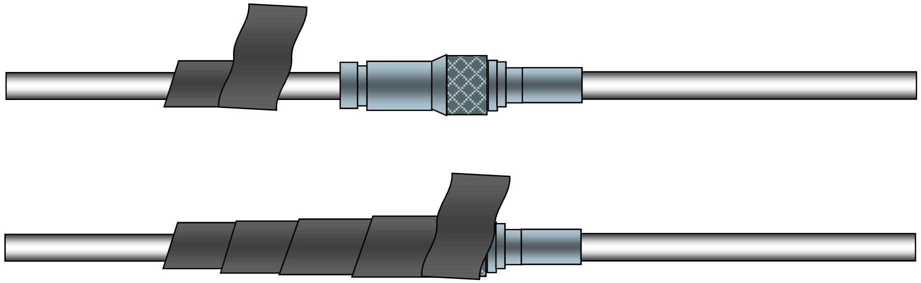
Not rain, nor sleet, nor snow

exterior connections should be wrapped in a rubber vulcanizing tape to prevent moisture ingress.

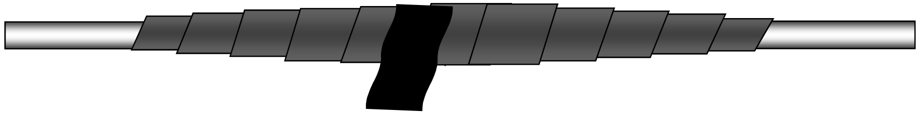
mate connectors securely



stretch to elongate sealant tape while wrapping over the connection

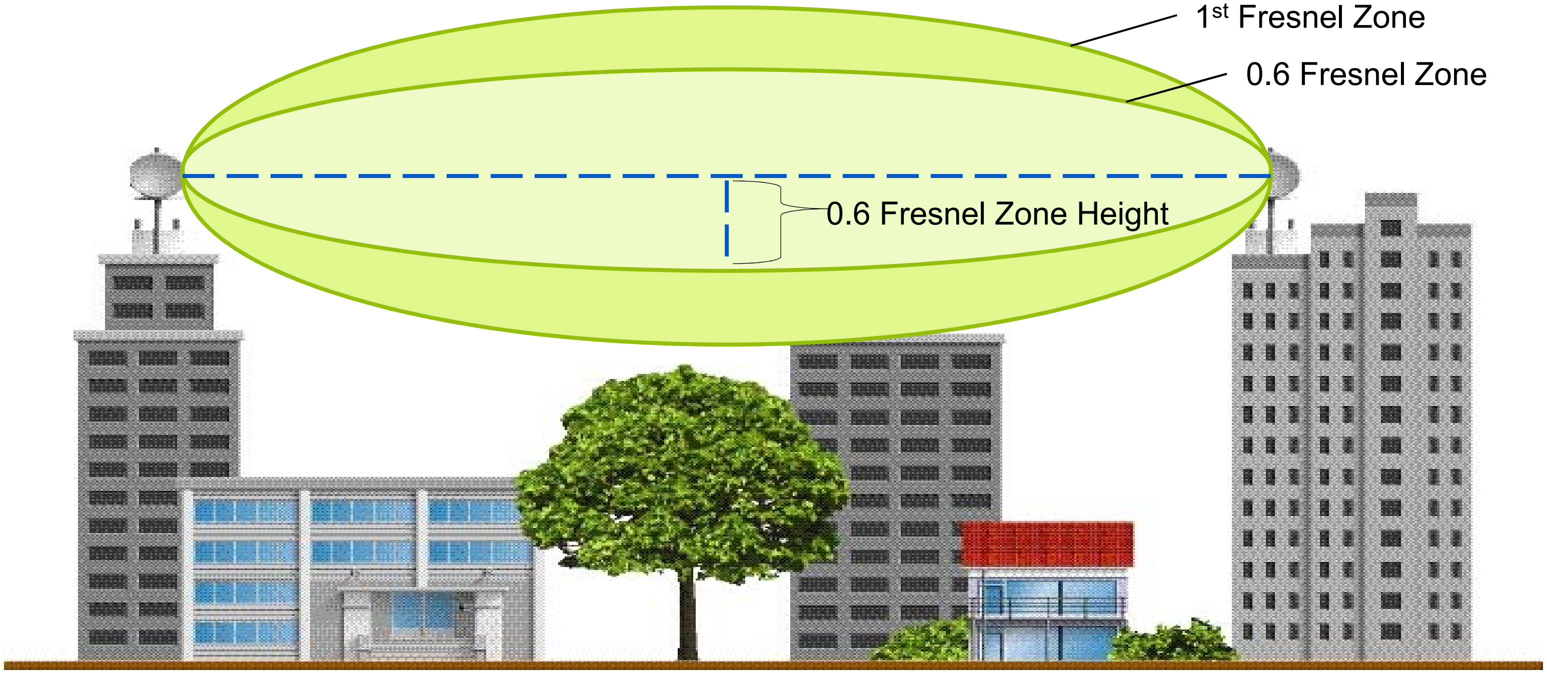


for proper UV protection, electrical tape should then be wrapped over the vulcanizing tape



Antenna height

the 0.6 Fresnel zone should be free of obstructions



$$H_{0.6Fresnel}=25.98*\sqrt{}[D_{miles}/(f_{GHz}*4)]$$

WirelessHART

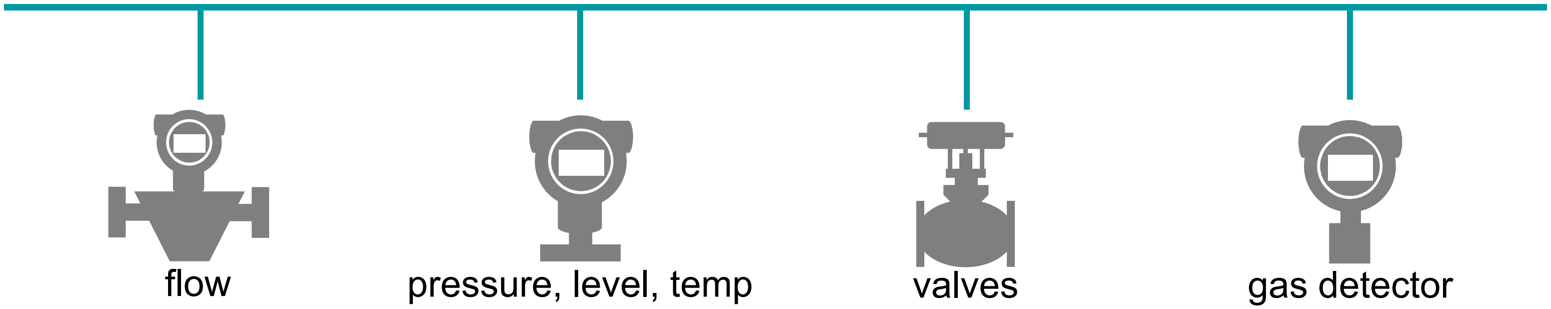
2.4
GHz

250
kbps

800
feet

DSSS

Wireless Sensors



flow

pressure, level, temp

valves

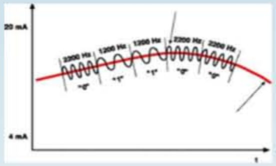
gas detector

WirelessHART

We make HART accessible

HART technology

the world’s most broadly supported protocol for the process industry



1986

HART became an open standard.

HART COMMUNICATION FOUNDATION

1993

The HART Communication Foundation was formed to manage the standard.

OPC OLE for Process Control

1999

The *HART Server*, an easy-to-use, OPC-compliant software application for accessing real-time process and diagnostic information was released.

HART

2001

HART 6 was released, including features to enable AMS (Asset Management System) integration:

WirelessHART

2007

HART 7 was released, and included the WirelessHART standard.

HART-IP

2012

HART 7 was enhanced with additional functionality, including HART IP.

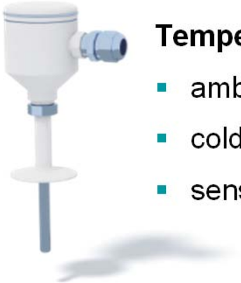
HART technology can help you

- **Leverage intelligent device capabilities**
  - use unified tools for device configuration
  - gain operational improvements by reducing troubleshooting time
- **Increase system availability**
  - detect device or process connection problems real time
  - avoid the high cost of unscheduled shutdowns
- **Decrease Maintenance costs**
  - use remote diagnostics to reduce field checks
  - capture performance trend data for predictive maintenance
- **Improve regulatory compliance**
  - enable automated record keeping of compliance data
  - take advantage of multivariable devices for more thorough reporting

Unlock your data

Level

- sensor status
- high and low alarm setpoints

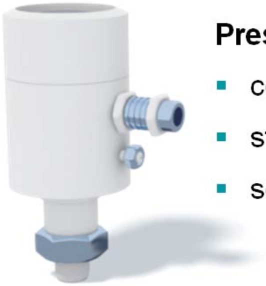


Temperature

- ambient temperature
- cold junction temperature
- sensor breakage

Valve Positioner

- actual valve position feedback
- adjust for mechanical wear
- sensor status

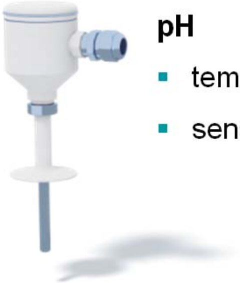


Pressure

- cell temperature
- static pressure
- sensor status

Flow

- process media density
- absolute pressure and temperature
- totalized flow



pH

- temperature measurement
- sensor health

WLAN

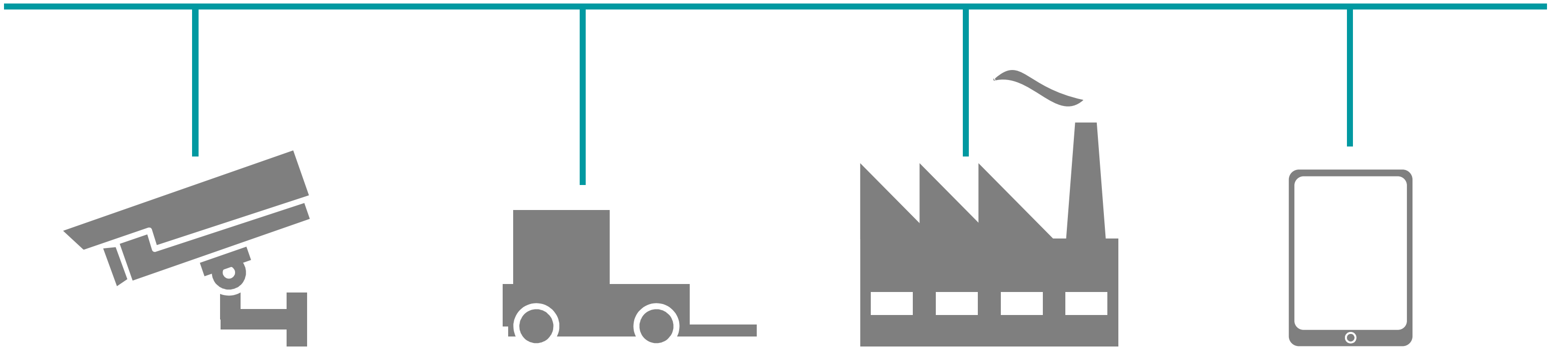
2.4/5
GHz

300+
Mbps

1,000
feet

DSSS
OFDM

Wireless LAN



security cameras

AGVs

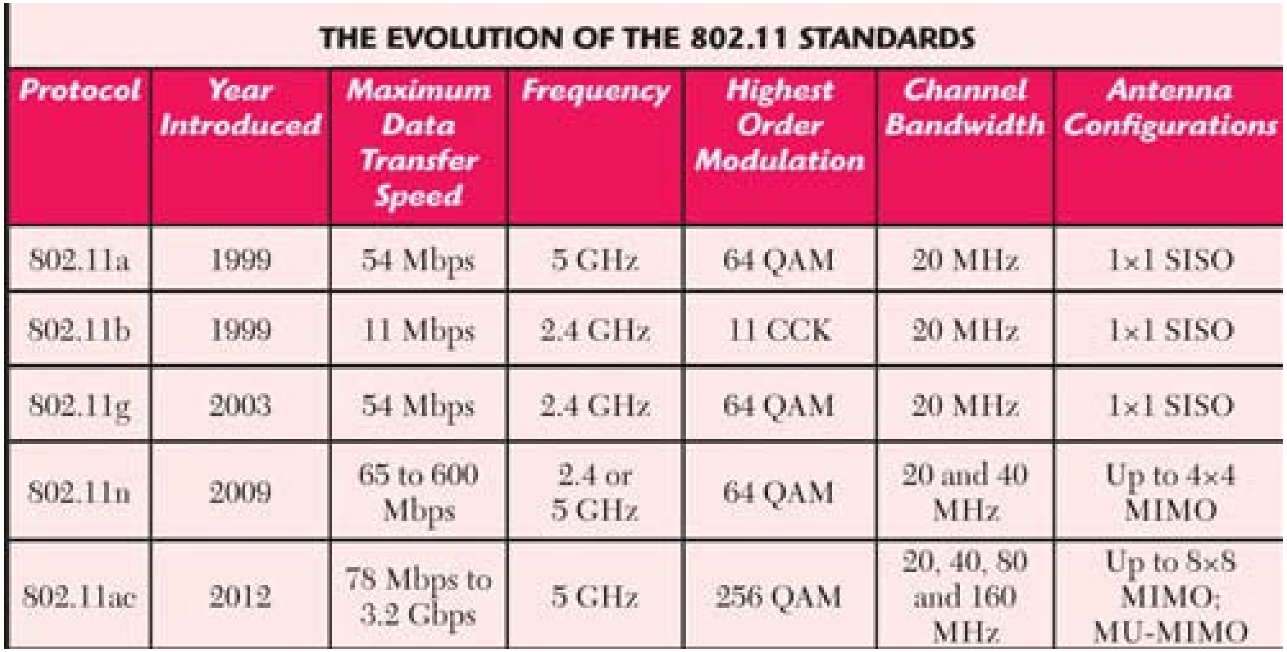
plant networking

mobile devices

What makes it Industrial?

- Temperature Specification
- Din Rail or panel mounts
- 24 Vdc Power
- Shock, Vibration, EMC rating
- Higher Transmit power (100/200 mW vs 25 mW)
- UL and Hazardous approval markings
- Advanced setting options

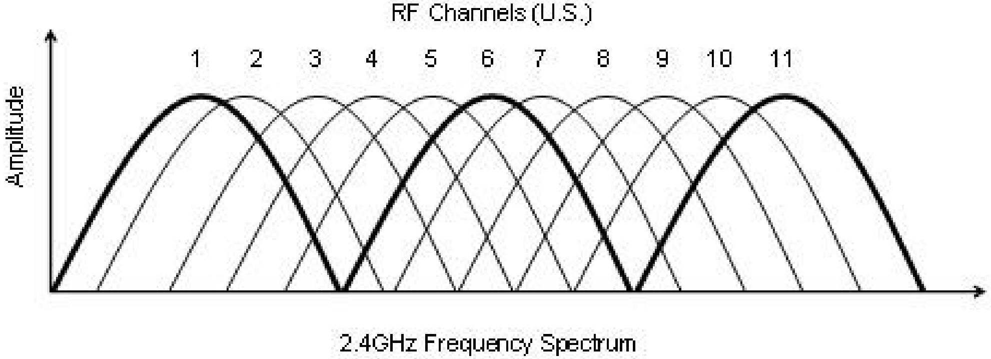
802.11 Standards

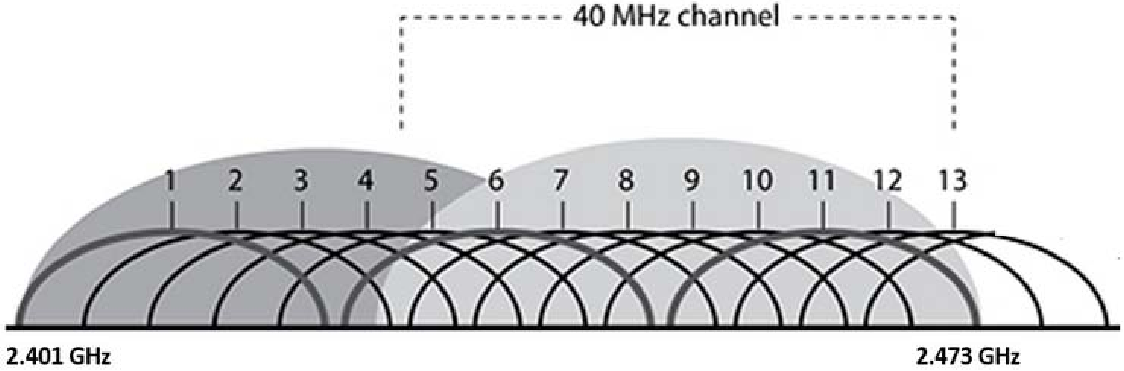


THE EVOLUTION OF THE 802.11 STANDARDS

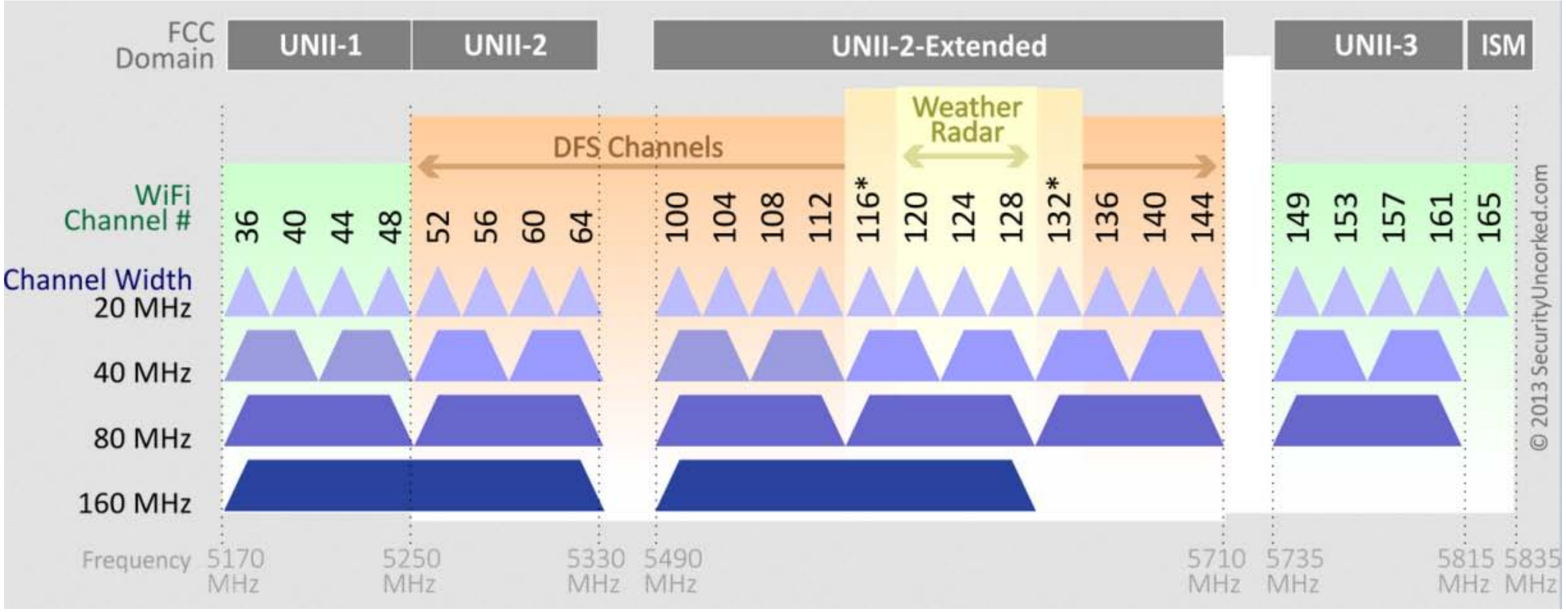
Protocol	Year Introduced	Maximum Data Transfer Speed	Frequency	Highest Order Modulation	Channel Bandwidth	Antenna Configurations
802.11a	1999	54 Mbps	5 GHz	64 QAM	20 MHz	1×1 SISO
802.11b	1999	11 Mbps	2.4 GHz	11 CCK	20 MHz	1×1 SISO
802.11g	2003	54 Mbps	2.4 GHz	64 QAM	20 MHz	1×1 SISO
802.11n	2009	65 to 600 Mbps	2.4 or 5 GHz	64 QAM	20 and 40 MHz	Up to 4×4 MIMO
802.11ac	2012	78 Mbps to 3.2 Gbps	5 GHz	256 QAM	20, 40, 80 and 160 MHz	Up to 8×8 MIMO; MU-MIMO

2.4 GHz Frequencies





5 GHz Frequencies



Trusted Wireless

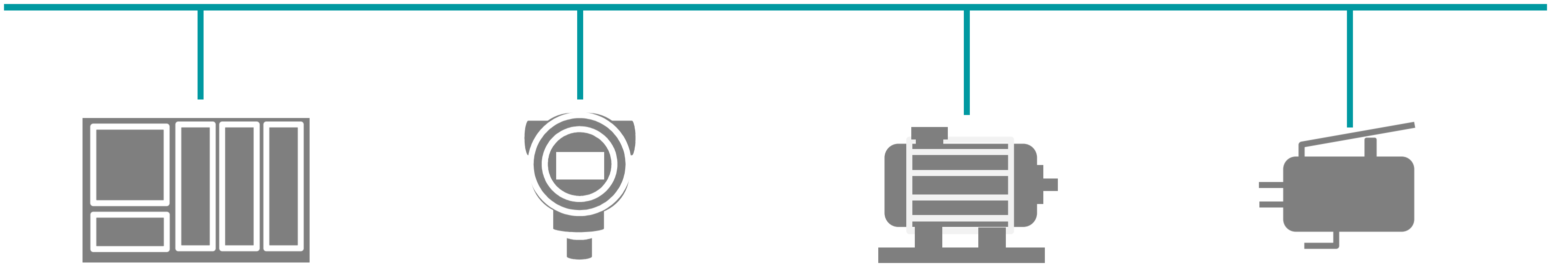
900 MHz

<1Mbps

20+ miles

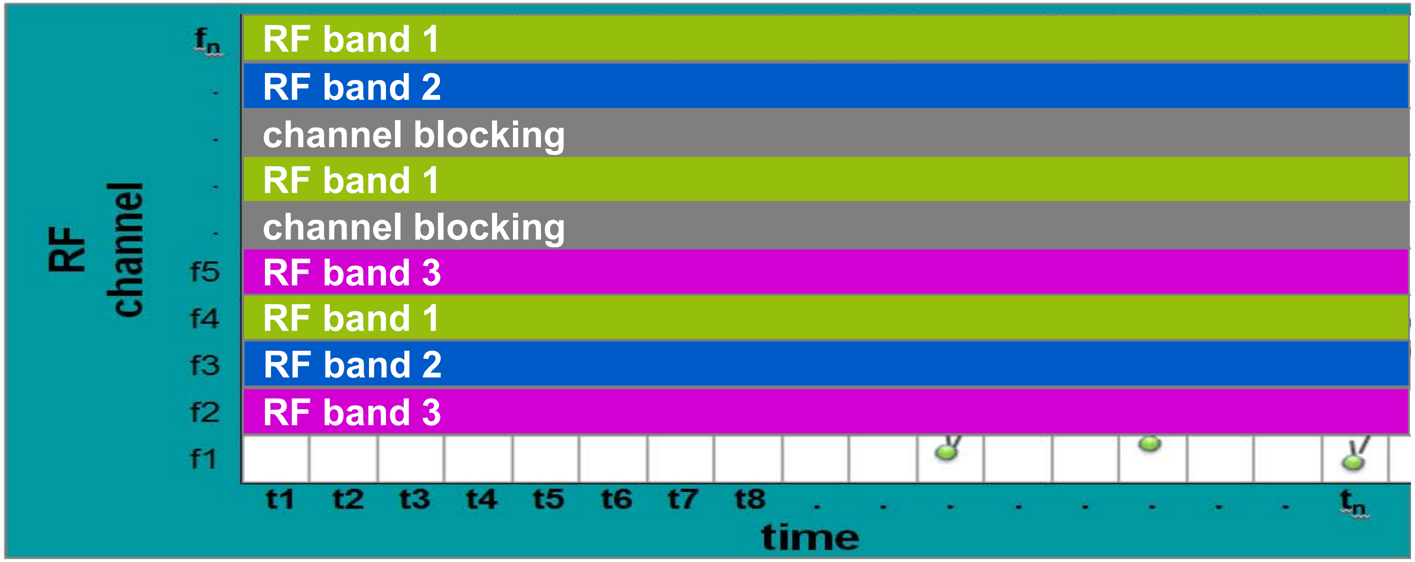
FHSS

Wireless I/O



Robust

technology for harsh industrial environments



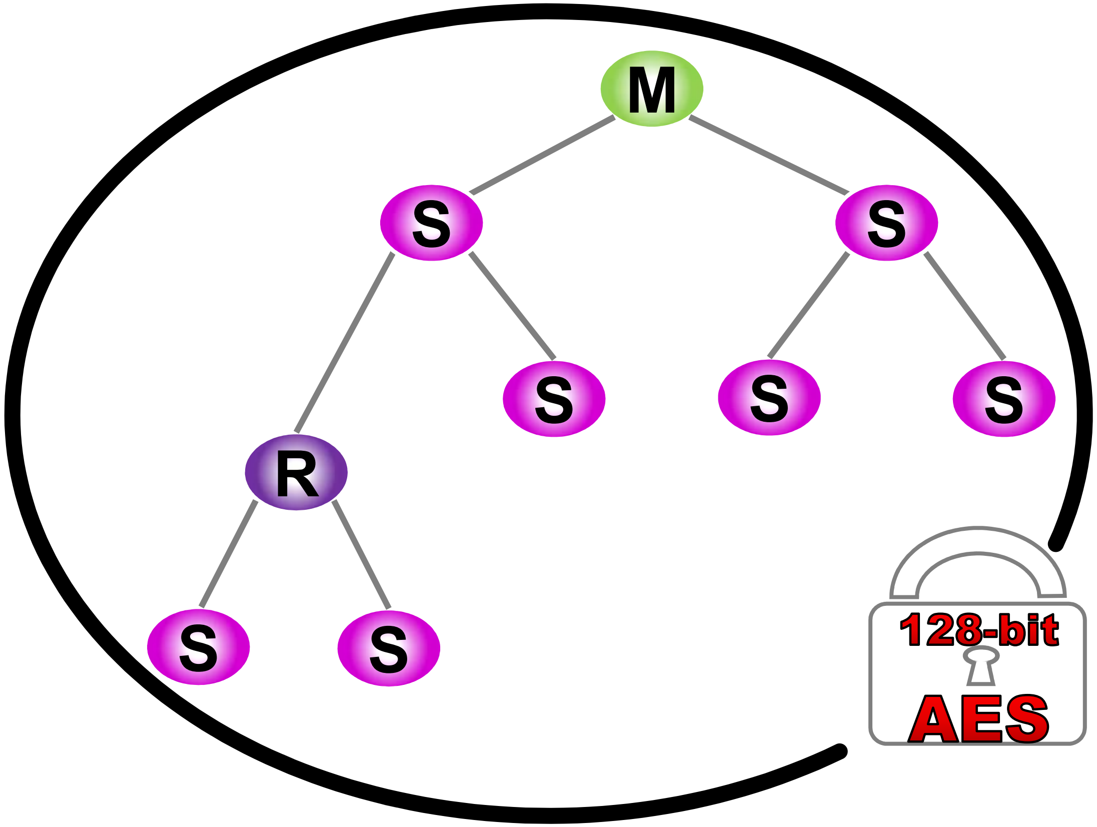
frequency hopping
tolerate interference over long distances

channel blocking
remove bad channels from use

Multiple RF bands
interleaved sets of frequencies for coexistence

Secure

using 128-bit AES-CCM for encryption and authentication



1. listen
2. synchronize
3. follow hop sequence
4. send join request
5. receive join acknowledge

Cellular

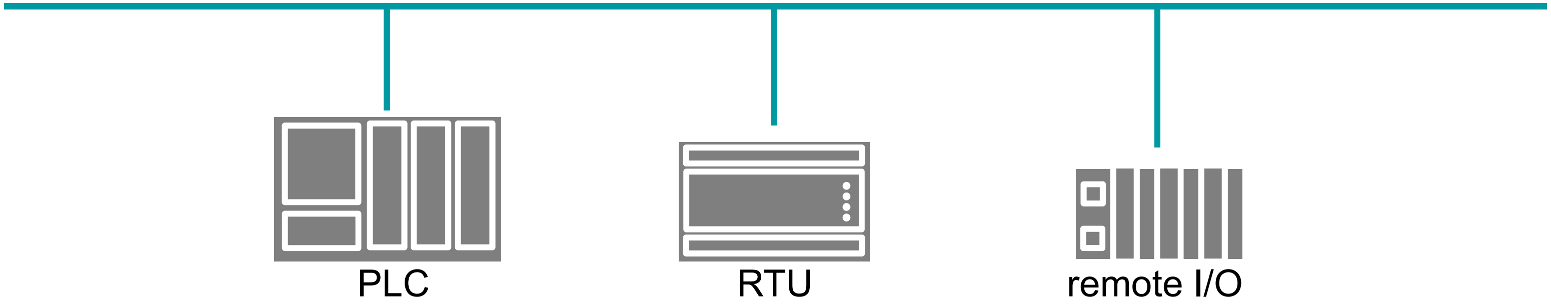
900 MHz

<1Mbps

15+ miles

1-5 watts

SCADA



PLC

RTU

remote I/O

What is SCADA?

Supervisory **C**ontrol **A**nd **D**ata **A**cquisition

the monitoring and control of remote equipment, often over many square miles

- long range (15+ miles)
- low data rate (< 1MB)
- high reliability (data gets through)

PHŒNIX CONTACT

900Mhz Wireless Ethernet Technology

- Proprietary wireless system
  - Inherently secure
  - AES 256-Bit
- FHSS
- 1Watt, 900MHz ISM band (US-Market)
  - Typical: 1-2 Miles
  - Max: 15 Miles +
- Designed for long distance Ethernet connections. Ideal for SCADA systems, remote programming, and data gathering

Cellular

- **GSM/EDGE/UMTS** is commonly known as "cell phone" technology
- Requires a SIM card and service plan to operate
- A GSM/EDGE(2G) is older technology used mostly for SMS/Voice and IP based data
- EDGE/UMTS(3G) is used for higher data transfer
- AT&T & T-Mobile

GSM®
GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

GSM/GPRS	
Frequency	850, 900, 1700, 1800, 1900, 2100MHz
Transmission	TDMA
Data Rate(2G)	85.6kbps (GPRS) 150kbps(EDGE)
Data Rate(3G)	7.2Mbps Download
Topology	Point to Point
Typical Range	Uses cellular infrastructure

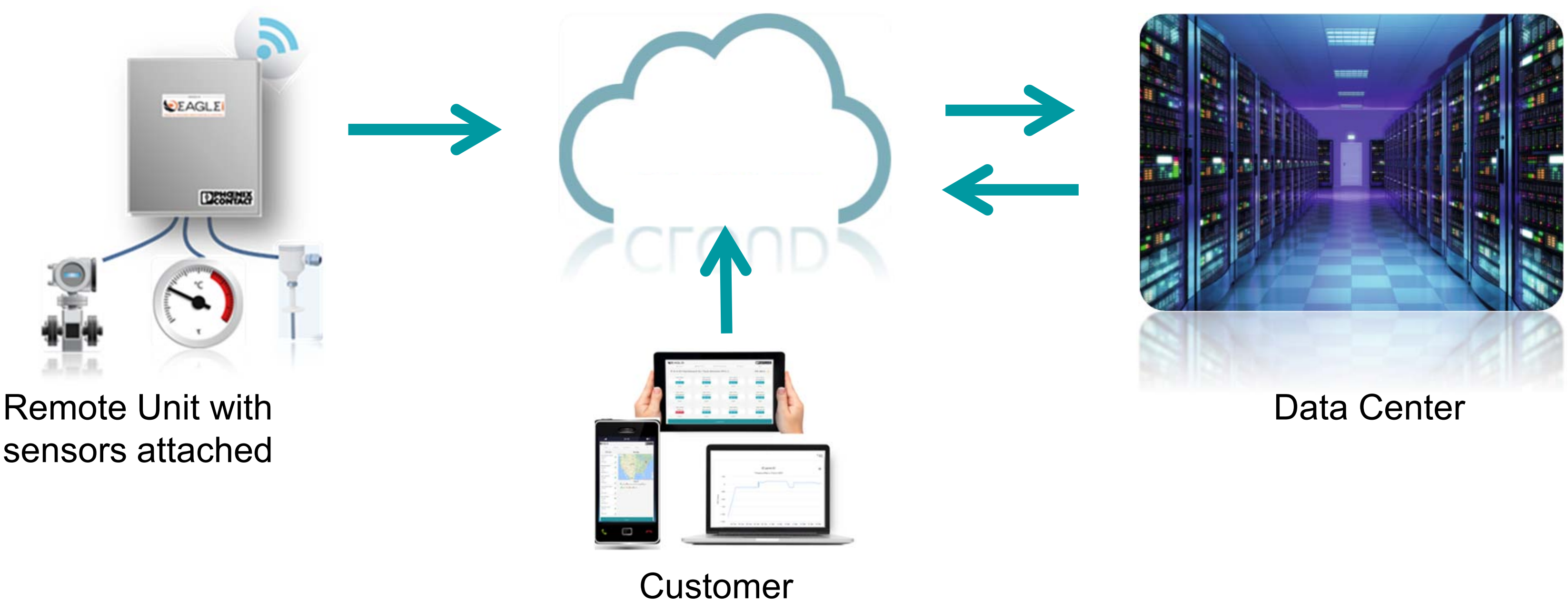
Cellular

- **CDMA** is another commonly known “cell phone” technology
- **Does not** use a SIM card
- Carrier Registration with IMEI #
- CDMA/CDMA2000(2G) is older technology used mostly for SMS/Voice and IP based data
- CDMA2000 EVDO(3G) is used for higher data transfer
- Verizon & Sprint

CDMA/EV-DO	
Frequency	800, 850, 900, 1900MHz
Transmission	CDMA
Data Rate(3G)	2.4Mbps download 3.1Mbps Upload
Topology	Point to Point
Typical Range	Uses cellular infrastructure

Cellular Data Overview

Understanding Cellular Data Transfer



Remote Unit with sensors attached

Data Center

Customer

Wireless Overview

- Wireless Applications:
  - Mobile Access
  - Remote PLC to PLC
  - Remote I/O

Mobile Access - Application

- Location – Plant facility
- Need – Wireless access to assets and/or process conditions

Wireless Overview

- Wireless Applications:
  - Mobile Access
  - Remote PLC to PLC
  - Remote I/O

Remote PLC to PLC - Application

Location – Reservoir booster pump station
Need – Wireless PLC to PLC communication to Plant SCADA

Wireless Overview

- Wireless Applications:
  - Mobile Access
  - Remote PLC to PLC
  - Remote I/O

Remote I/O - Application Overview

- Location – Open Channel Flow Meter
- Need – Wireless control/monitoring of remote I/O data

Practical wireless

- use the lowest practical RF data rate
- mount the antenna clear of obstructions
- weatherize connectors
- use surge protection
- maintain earth grounds