

# Uses of the New Types of Wireless Technologies for Distribution and Substation Automation

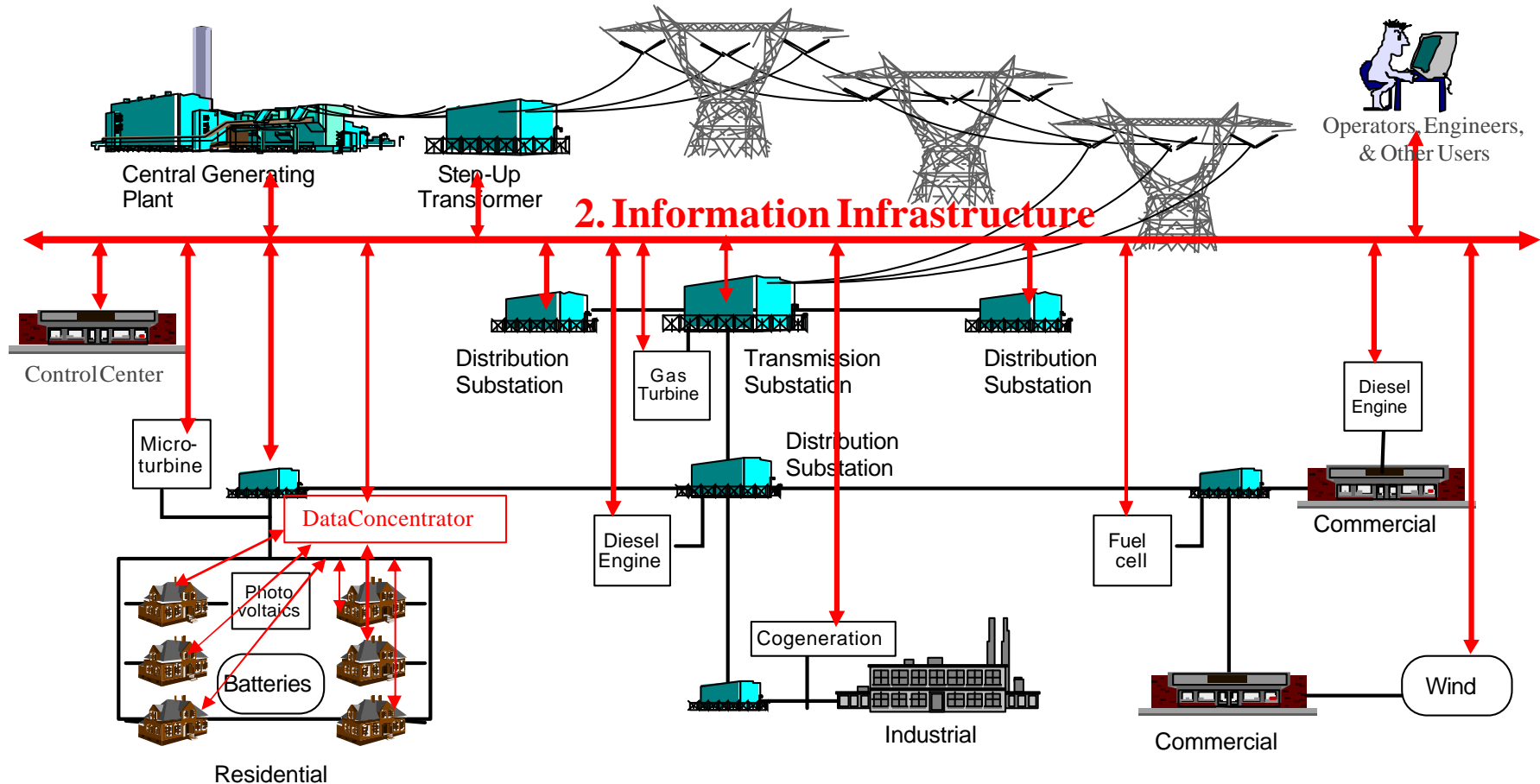
Frances Cleveland, Xanthus Consulting International

# Topics

- Wireless Communications: Devilish or Angelic?
- Types of Wireless Communications
- Reliability and Security Issues with Wireless Communications
- Examples of Wireless Communications
- Next Steps

# Two Infrastructures must be managed in the future, not just one...

## 1. Power Infrastructure



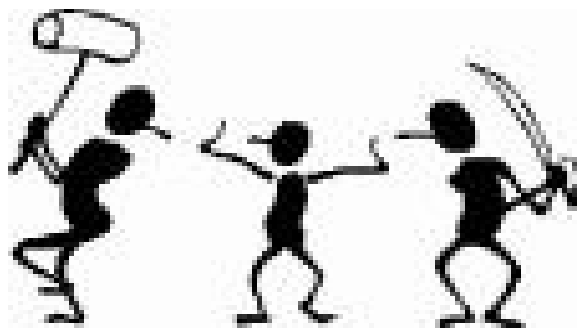
# Two Images of Wireless Communications in Substations

- Devilish:
  - Eavesdropping on data
  - Unauthorized control commands
  - Unreliable, disrupted communications in the noisy substation environment
  - Hackers, viruses, and worms
- Angelic:
  - **Low costs**
  - Rapid installations
  - Easy maintenance
  - Avoided ground potential rise problems
  - **Low costs**
  - Mobility
  - Safety due to remote operations
  - Warmth of a van outside a freezing substation
  - More data and additional capabilities
  - **Low costs – 7 times less in TVA's example**



# Where Does the Truth of Wireless Lie?

- Where is the truth in these two images?
- Should wireless communications be avoided completely in substations?
- Are there applications where wireless **could be** used?
- Are there applications where wireless **should or must be** used?
- Are there applications where wireless **should not be** used (yet)?
- What additional security and reliability requirements should be added to wireless systems to make them usable in substations?
- Bottom line: **Can utilities afford to ignore the significantly lower costs of wireless technologies?**



# Types of Wireless Systems #1

- **Older wireless systems:**
  - Microwave systems
  - Multiple address radio systems
  - Satellite, particularly VSAT
  - Spread spectrum radio, 928 MHz point-to-point
- **WiFi – IEEE 802.11:**
  - Currently WiFi is the most popular wireless standard for networking computer systems and other computer applications
  - IEEE 802.11b data rate is 11Mbps
  - IEEE 802.11g data rate is 54Mbps
  - Frequency band is the 2.4Ghz band
  - Range of 100-150 feet



# Additional Wireless Systems #2



- **Bluetooth™ – IEEE 802.15.1:**
  - Bluetooth is used in cellphones, Personal Digital Assistants (PDAs) and other mobile wireless devices, primarily for communicating with computers, Intelligent Electronic Devices (IEDs), headsets, hands-free systems, and other gadgets.
  - Very short range of only 33 feet (approx 10m)
  - Frequency band is the 2.4Ghz band.
  - Relatively low data rate of 1.5Mbps
  - Bluetooth is designed for low-traffic serial point-to-point links, which is why it's being used in devices like wireless mobile phone headsets.

## Additional Wireless Systems #3



- **Zigbee – IEEE 802.15.4:**
  - **IEEE 802.15.4** defines low-rate (<250 kbps), very low duty cycle, wireless personal area networks often termed “meshed networks” as opposed to point-to-point. Distances between devices is 30-300 feet.
  - **ZigBee** builds upon this 802.15.4 standard to define application profiles that can be shared among different manufacturers to provide system-to-system interoperability.
  - This effort is still a work in progress, although of great interest to industries (such as the power industry) that have extensive sensor networks.
- **WiMax – IEEE 802.16:**
  - Addresses the "first-mile/last-mile" connection for longer distances (5-30 miles) and faster rates (45-75 Mbps)
  - The main focus of the IEEE 802.16 standards is to enable a wireless alternative for cable, DSL, and T1 communication channels for consumer last-mile access to the Internet, including high-speed data, Voice over IP (VoIP), Video on Demand (VoD), and backhaul for IEEE 802.11 LANs.



# Additional Wireless Systems #4



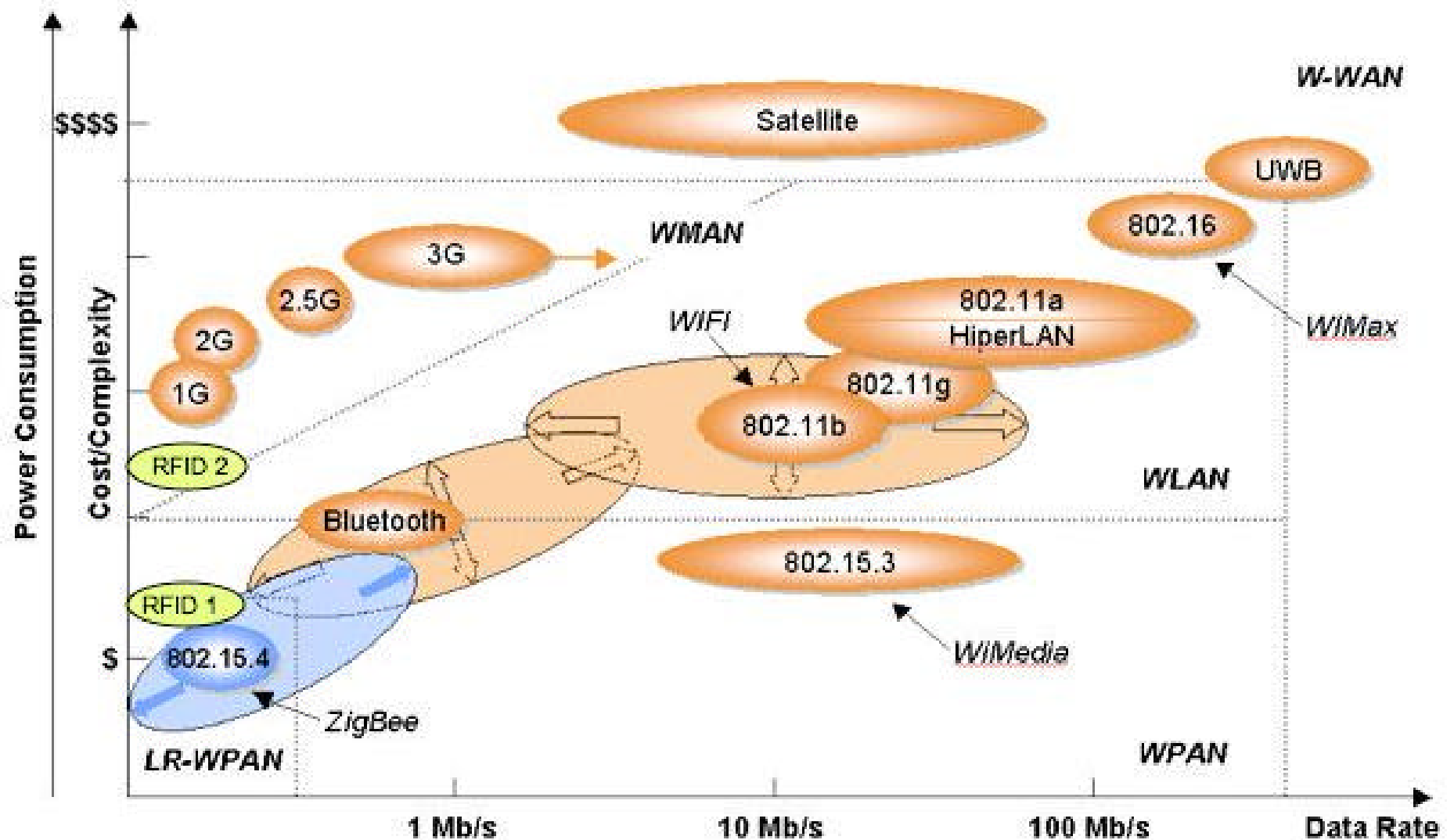
- **Cellphone – Group Spéciale Mobile(GSM):**
  - GSM was established to create a common European mobile telephone standard for a pan-European mobile cellular radio system (and now worldwide)
  - The resulting mobile telephone standard allows cellphone users to “roam” across many cellphone systems and between most countries world-wide.
  - New generations of cellphone technologies, termed 2.5G, 3G, and 4G are deployed in certain countries or are still under development.
  - GPRS commonly used for data, with 30-80 kbps typical.
  - EDGE (enhancement to GPRS) provides 160-236 kbps
  - The range is wherever cellphone coverage is available!

# Additional Wireless Systems #5



- **Tetra – Terrestrial Trunked Radio standard**
  - Developed for Professional Mobile Radio (PMR)
  - Provides some data services
  - Different countries have different frequencies, e.g. 446 MHz in the UK, 380-430 MHz in Europe, and 800 MHz in other parts of the world

# Comparison of Different Wireless Technologies



# ***Benefits of Wireless Versus Wired***

- **Less expensive** because cabling does not need to be installed. While fiber optic cables cost about \$25k per mile, wireless media is “free”
- **More rapid implementation**, since no trenching through and around substation equipment is required.
- **Less experienced technicians** can often be used, because they do not need to be concerned with ground potential rise or have to run cables around HV equipment.
- **More mobile and portable** so that the same equipment with wireless communications can easily be moved from one spot to another, either continuously (e.g. in a truck) or periodically (e.g. for spot maintenance).
- **Additional wireless equipment can automatically interconnect** with only the appropriate security features enabled.
- **Less susceptible to ground potential rise** because no cabling is needed.
- **Failure location** in wireless systems can be easier, since only need to test the end devices.
- **New wireless applications may be feasible** that were not cost-effective with wired communications. These applications might improve power system reliability and efficiency, or provide increased personnel safety.

# Common Reliability and Security Concerns for Wired Media and Wireless Media

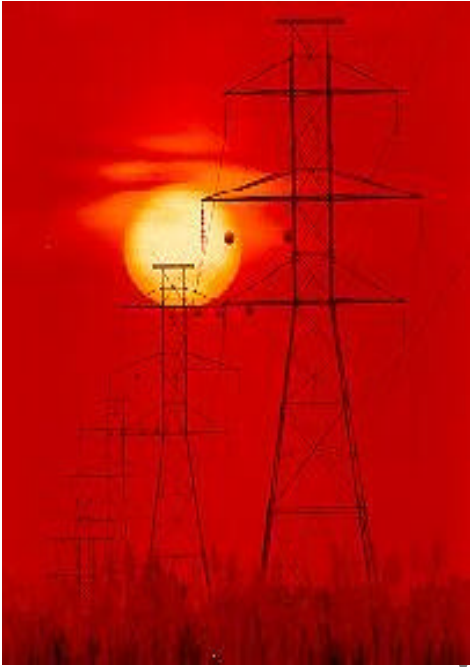
- ***Some reliability and security concerns/problems/issues are the same for both wired and wireless media. These need to be identified so that only the differences can be compared: apples to apples.***
  - **Data protocols.** Robustness and security of data are related to the actual protocol, not to the media it goes over. The security (or lack of security) of Modbus is the same whether it goes over fiber optic cable or a wireless system.
  - **Internethackers.** Hackers trying to access systems through the Internet do not care or even know about the media.
  - **Overloading of the communications network by the utility.** The data volume that a network can handle is related to the bit-per-second rate of the media, as well as configuration, response requirements, the degree of “bursty” data, and other network parameters. Again, this is media-independent.
  - **Single points of failure.** The network configuration, not the type of media, is responsible for possible single points of failure.
  - **Utility security policies.** If authorization procedures are not solid or are not followed, it does not matter what media you use. This includes not updating default passwords, vendor “backdoors” into their equipment, lost or stolen equipment, bypassing security checks, etc.

# Reliability and Security Concerns That Are More of an Issue for Wired Systems

- **Wired systems can have reliability and security issues that are not a factor in wireless systems**
  - **Cutting or breaking the cable.** Cables can always be cut or broken, whether by a backhoe, by corrosion, by repeated bending, or by a disgruntled employee with a large pair of wire cutters.
  - **Poorly connected wires or stressed wires.** Poor connections on wires can lead to noisy or intermittent communications and could potentially lead to breakage of the wire.
  - **Physical theft of wire.** Long stretches of wire in unsecured areas may pose a problem of physical theft of the cable, a rampant problem in many countries in the world.
  - **Eavesdropping on metallic wires.** If physical access is available, metallic wires can easily permit eavesdropping with very simple techniques.
  - **Ground potential rise on metallic wires.** Metallic wires are susceptible to ground potential rise in substations due to power equipment and lightning strikes
  - **Lack of mobility for additions, changes, upgrades, and movement of equipment.** Wired networks are more difficult to move or modify as new equipment is added and the configurations are changed, particularly if parts of the wiring are in inaccessible ducts or trenches.

# Reliability and Security Concerns That Are More of an Issue for Wireless Systems

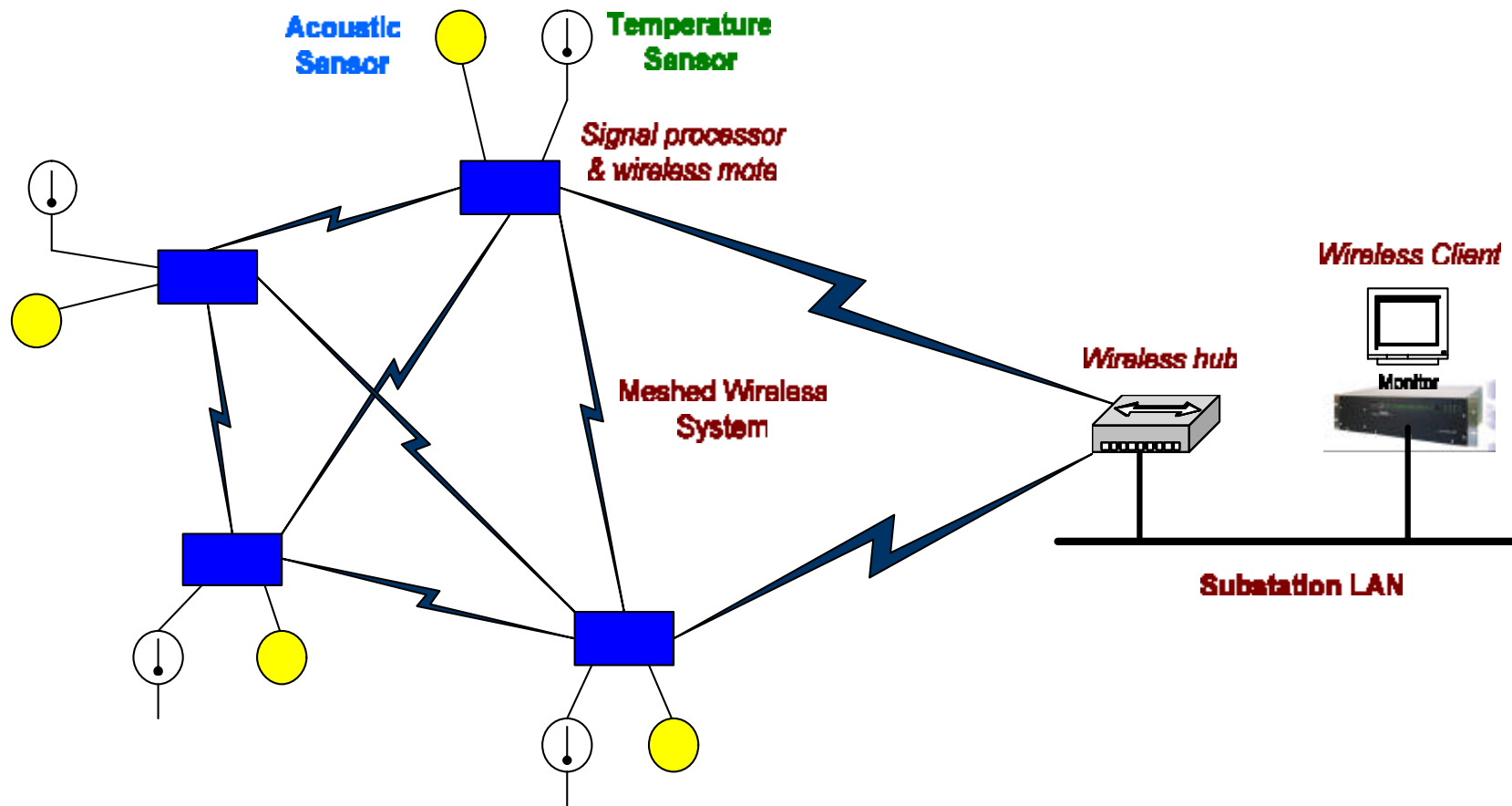
- **Wireless systems can have reliability and security issues that are not a factor in wired systems. These are often associated with denial-of-service and/or the unreliability of time-sensitive interactions.**
  - **Eavesdropping on non-secured channels.** Since wireless signals can be received by users outside the immediate environment, their data can be listened to, and if not encrypted, can be understood. **However, if the data is adequately encrypted (IEEE 802.11i) or authenticated (SHA-1), then the information does remain secure.**
  - **Disruption of the wireless signal due to electromagnetic interference (EMI).** Substations and power plants are very electrically noisy environments, particularly during breaker operations and other equipment actions.
  - **Faded signals.** Many factors can cause the wireless signal to fade, including too long a distance between wireless transmitter and receivers, atmospheric conditions, metallic surfaces that reflect the wireless radio waves, obstacles in the line-of-sight, and other factors.
  - **Overloading of bandwidth.** Nearby users can overload the available bandwidth in the frequencies being used in the substation, thus causing delays and the potential need to retransmit data.
  - **Immaturity of wireless lower layer protocols.** Wireless lower layer protocols (as opposed to data protocols like Modbus and DNP) have only been developed recently and are still undergoing significant upgrades, modifications, and testing.



## Examples of Wireless Systems

# Acoustic Sensing of Arcing in Gas-Insulated Substations

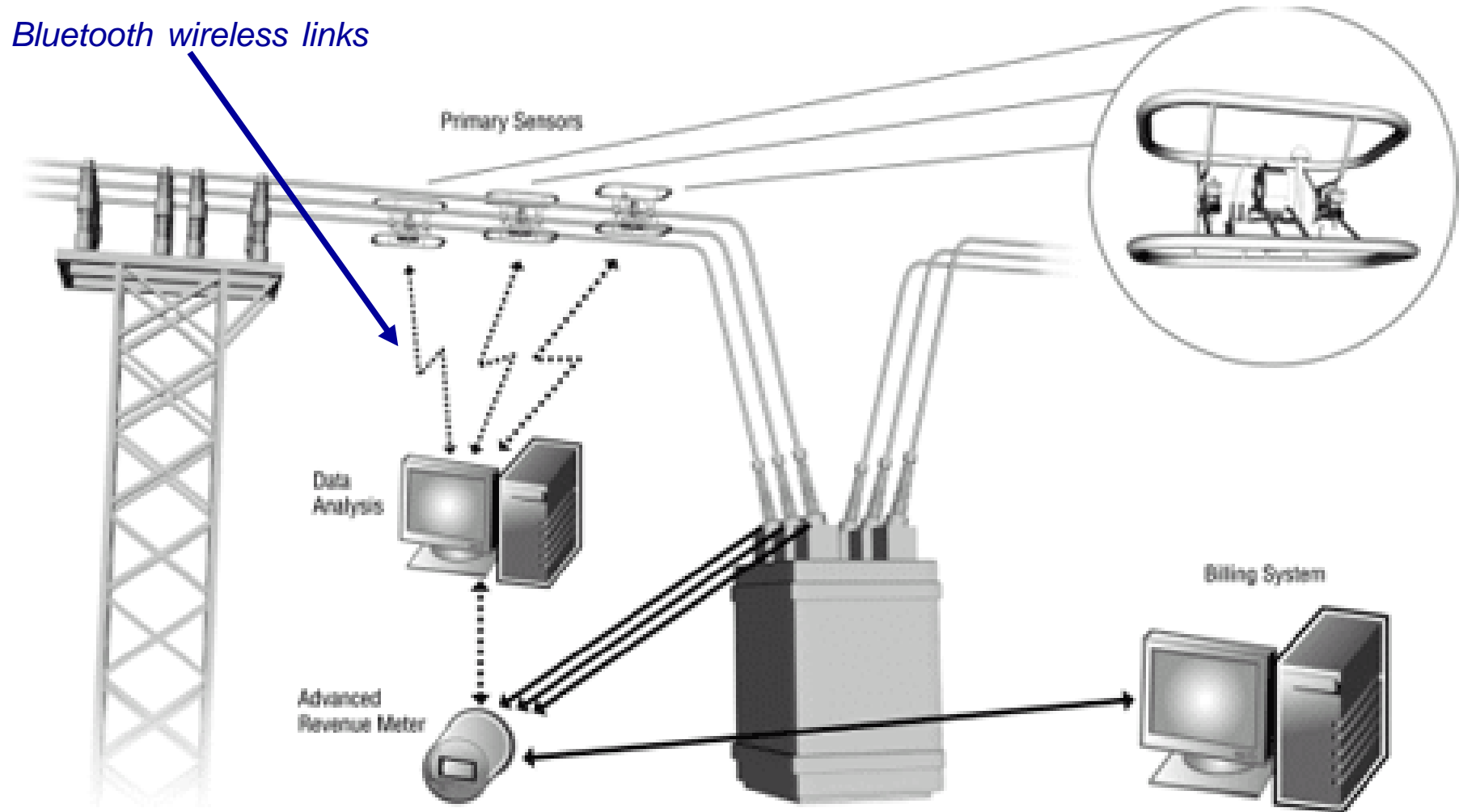
## Initial Demonstration - Meshed Wireless Acoustic and Temperature Sensors



# Specifications for Acoustic Sensing of Arcing in Gas-Insulated Substations

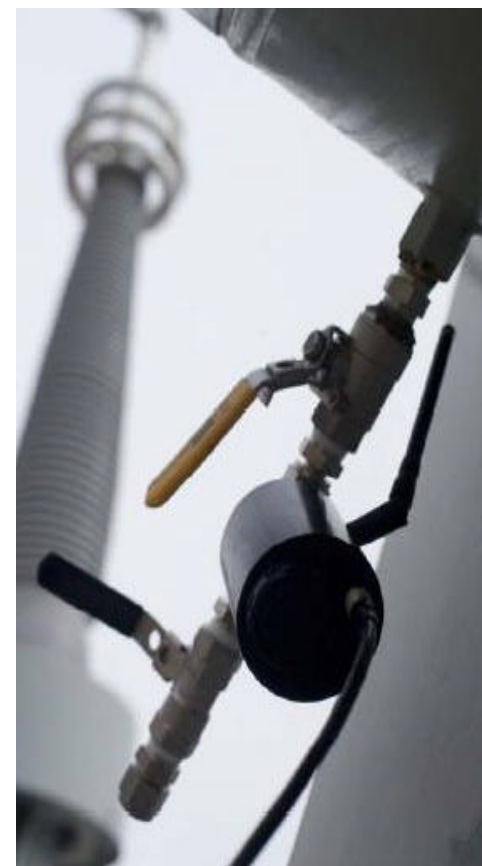
- 4 acoustic sensors:
  - Acoustic sensor R15I-AST to be provided by Physical Acoustics Corporation (PAC)
  - Resonant frequency: 150kHz
  - Analog signal output: 20 volts peak-to-peak maximum; however expected signal will be about one (1) volt of sub-second duration
- 4 temperature sensors
- Signal processors with A/D converters and basic data processing capability to capture acoustic RMS values and temperature
- Wireless mesh motes based on IEEE 802.15.4 Zigbee-like technology as a cluster
- Gateway wireless processor to interface to each cluster
- Human-Machine Interface (HMI) (PC for demo) interfaced to or part of gateway

# Sensors for Accurate Calibration of CTs for Reuse in Revenue Metering



# SF<sub>6</sub> Monitoring by Avistar – Mosaic

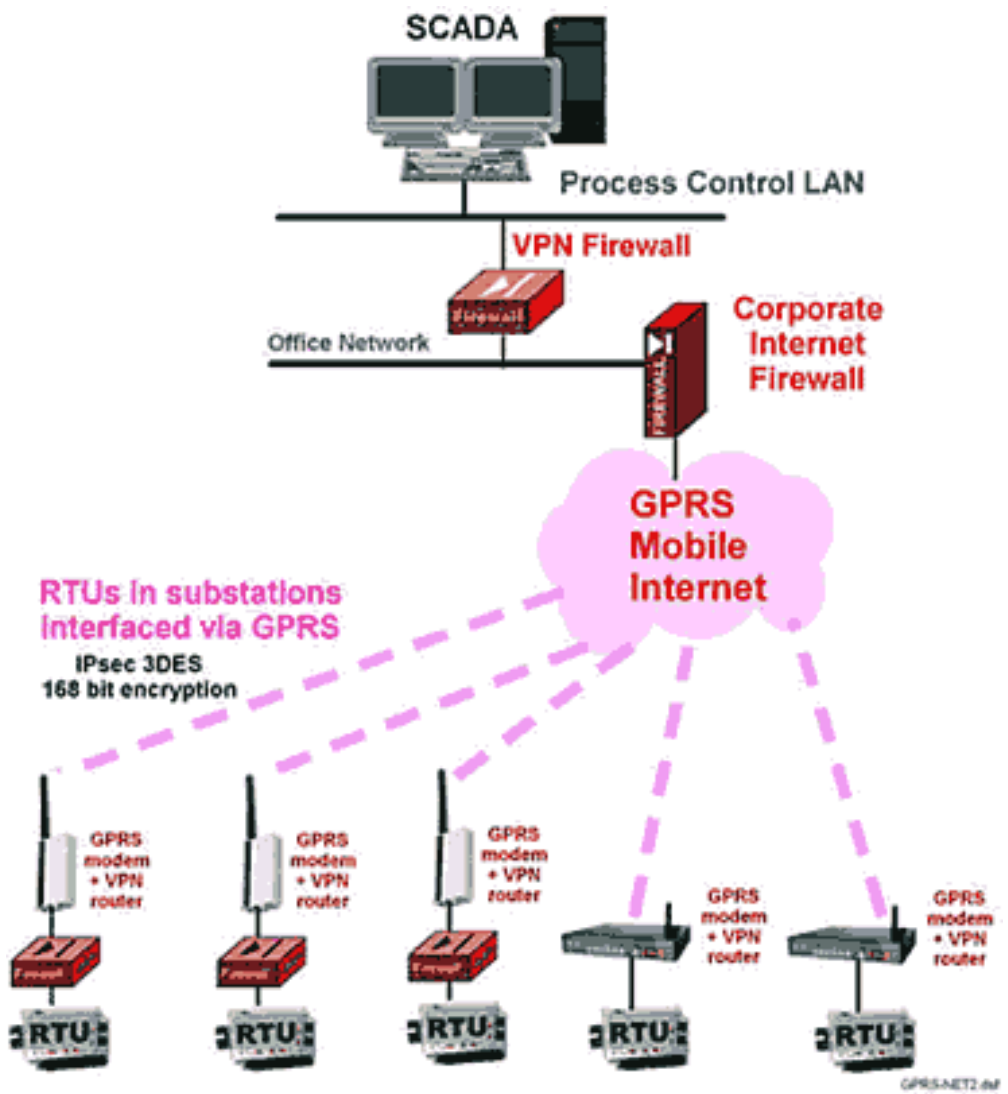
- Meshed network of wireless “motes” from Crossbow, one of a handful of meshed wireless vendors
- Small wireless monitors on circuit breakers with long-lived battery power
- Lower maintenance costs by avoiding truck rolls
- As we learned yesterday, also beneficial for environmental monitoring of the powerful SF<sub>6</sub> greenhouse emissions



# Beckwith Load Tap Changer Wireless Modules



# Cellphones: GPRS for SCADA and Maintenance Data from Small, Distant Substations or Poletops

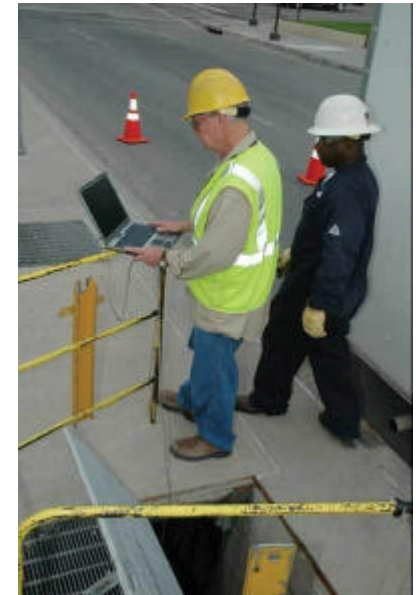


# Wireless for Safety in Underground Vaults

- Underground networks pose additional maintenance challenges. These include:
  - Checking the status of network protectors in underground vaults, often accessed via commercial buildings whose security procedures can hinder timely entry to the vaults.
  - Opening network protectors before performing switching operations, including the validation that the network protectors are truly open
  - Switching of operational network circuits for routine maintenance, with safety procedures requiring this to be performed with the crews outside the vault
  - Entering vaults in order to collect data from equipment, check network protector status, and modify/verify relay set points
- Vaults can also be dangerous during switching operations:
  - Possibility of sparks igniting a buildup of flammable gasses.
  - Crawling through cramped quarters, climbing ladders, and walking across wet floors near high voltage lines.
- **Wireless communications can be used by field crews just from laptops in their vans, thus making access to vault data much easier, safer, and in shorter time.**

# Example of GPRS for Underground Network Monitoring

- In 2003 and 2004, Kansas City Power & Light's (KCP&L's) network customers experienced several outages, jeopardizing the utility's goal to maintain great customer relations and a high quality of service. In addition, concern arose when three KCP&L underground network crew members narrowly escaped injury when a network protector faulted while the workers were inside the vault. KCP&L executives tasked the company's distribution automation engineers to provide a solution to these issues as soon as possible.
- The project was driven by safety concerns, escalating costs and increasing performance issues with the utility's aging underground network systems. It developed products to reduce costs and improve efficiencies for electric utilities that use network protectors. KCP&L worked with Telemetric and Richards/ETI to develop an economical solution for network automation using commercial cellular networks along with cost-effective hardware and software. This project proved that digital GPRS (general packet radio service) could be used as a reliable and secure way to enable distribution automation in underground vault installations-a solution previously thought to be too difficult or costly to implement using private spread-spectrum radios.

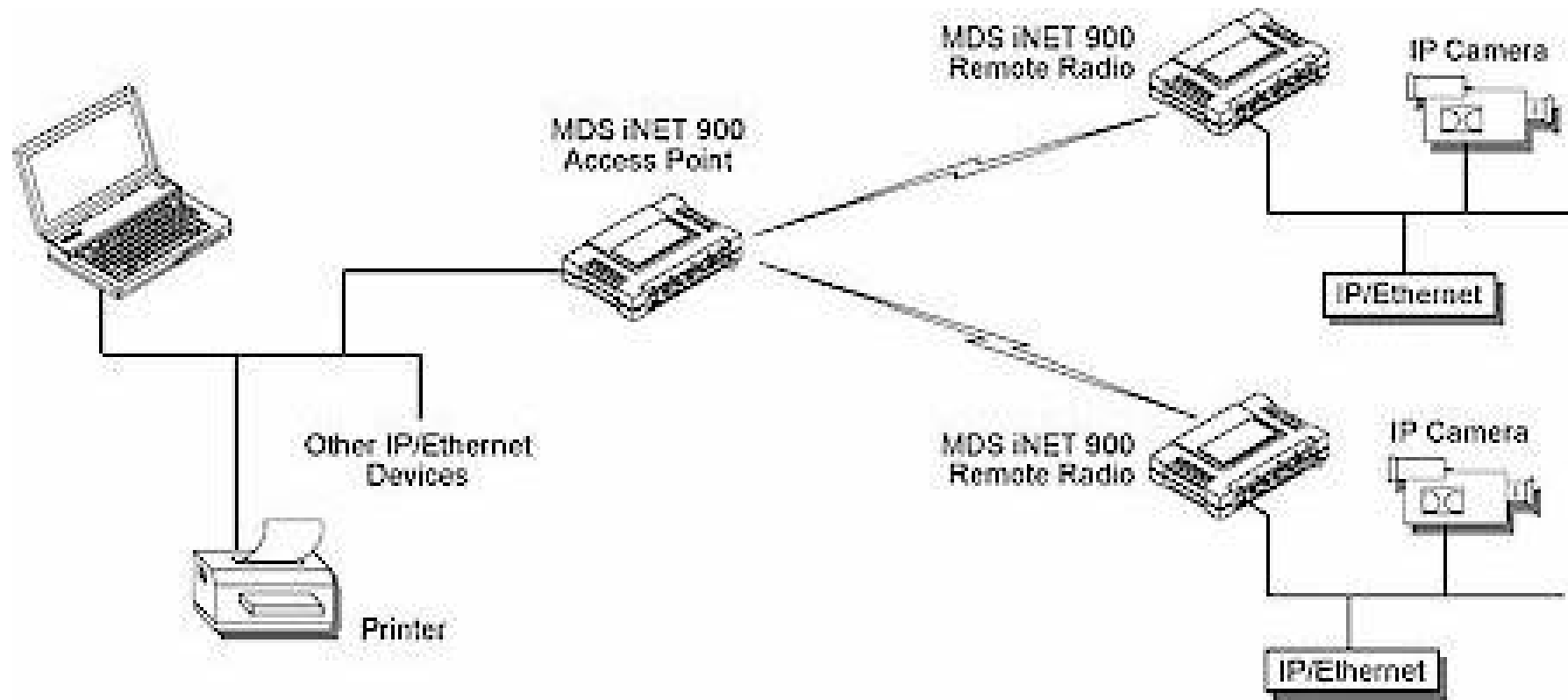


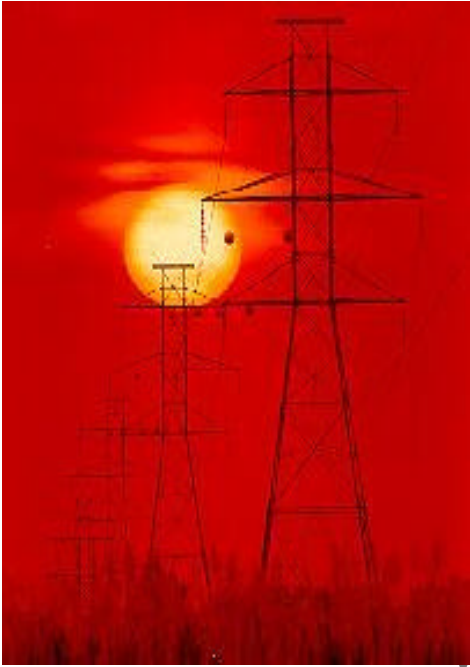
# Maintenance from Inside the Truck, Outside the Substation Fence or Below the Poletop

- Private wireless network with high security
- Improve safety and security
- Stay warm or cool or safe in truck



# Wireless Monitoring with Security Video Cameras – MDS Wireless System





**Conclusions??**

# When Wireless Can or Should Be Used

- **Data being transmitted is not very time-sensitive, and can tolerate delays.**
  - Data can be lost for the length of the delay, or
  - Systems on either side “buffer” the data until communications become available again, and the data can be resent
- **Data would be very expensive or difficult to retrieve using “wired” communications.**
  - Difficulty and cost of installing wiring across substation yards
  - Ground potential rise and other safety/security issues of running wires from within a substation to outside equipment
- **Wireless communications are temporary**
  - Due to short-term need or emergency situation
  - Wireless communications systems are for backup or redundancy
  - Infrequent usage where possible delays are acceptable
- **Data is received from and/or transmitted to mobile equipment**
- **Data is transmitted and received via cellphones and/or mobile data terminals by utility users**
- **Obviously, when new functions can be cost justified by using inexpensive wireless communications**



# Next Steps – EPRI and the Power Industry

- Develop Use Cases for wireless applications – IEEE P1777 has been established to request such Use Cases for many different power industry applications
- Specify the reliability, security, and other performance requirements for different types of distribution automation and other power industry functions
- Develop and test the performance of wireless technologies in different environments, pushing vendors to provide “industrial strength” wireless products
- Expand the sensor data processing capabilities in chips and microprocessors at the local sites so that only “information” needs to be transmitted over the wireless networks
- Specify standardized testing procedures for wireless technologies used by functions
- Develop educational programs, guidelines, and presentations on wireless technologies – costs will come down and capabilities improve as more utilities implement wireless systems
- Work with standards organizations to enhance wireless standards to meet even more stringent utility security and reliability requirements



# Example P1777 Use Case: Predictive Maintenance Monitoring of Power Transformers

Topics	Description
<b>Person filling out Use Case:</b> Company, Name, Title	Xanthus, Frances Cleveland, Consultant
<b>Function name</b>	Predictive maintenance monitoring of power transformers in electric substations to help detect problems in a timely yet cost-effective manner before they cause possible transformer failures.
<b>Purpose:</b> Brief description of the purpose of the function	Monitor temperature, vibration, and oil pressure to detect out-of-range conditions and long term trends in order to determine more precisely when maintenance is or is not needed.
<b>Possible benefits</b> for using wireless technologies	<ul style="list-style-type: none"> <li>• Lower cost for installing sensors since no trenching needed</li> <li>• Avoid effort and disruption caused by trenching in substation yard</li> <li>• Low cost of wireless systems make purchasing the number of sensors needed for good predictive maintenance more cost-beneficial</li> <li>• Predictive maintenance will lower the number of truck rolls and unneeded dispatching of maintenance crews</li> <li>• Predictive maintenance will help avoid major transformer failures</li> <li>• Ease of installation</li> <li>• Mobility – can move sensors to other transformers</li> <li>• With more sensors, can do more predictive maintenance</li> </ul>
<b>Potential concerns</b> in using wireless technologies	<ul style="list-style-type: none"> <li>• Wireless equipment may not work well in an electrically noisy substation, so information from sensors will not be available</li> <li>• Wireless equipment may not survive in harsh substation environment</li> <li>• Industrial spies may be able to eavesdrop on transformer status information and somehow</li> </ul>