Wireless Data Communications for SCADA Systems
Advanced SCADA Features

Networking
(Communication Anywhere to Anywhere)

Data Reliability
(No Communication Errors)

Data Security
(Immune to Intrusion)
“Open” Communication Solutions

**SCADA**
- Wonderware
- Intellution
- Factorylink
- etc.

**Applications**
- Pressure/Flow
- Maintenance
- Leak detection
- etc.

**Versatile IEDs**
- Pressure Control
- Flow calculations
- Pumps Start
- etc.

**SCADA**
- Wonderware
- Intellution
- Factorylink
- etc.

**Applications**
- Pressure/Flow
- Maintenance
- Leak detection
- etc.

**Versatile IEDs**
- Pressure Control
- Flow calculations
- Pumps Start
- etc.

**PLC Interface**
- Allen Bradley
- Modicon
- Etc.

**Versatile Interface**
- MODBUS
- DNP 3.0
- OPC
- MDLC over TCP/IP
- etc.

**Versatile Media**
- 900 Mhz Conventional
- 900MHz S.Spectrum
- Analog Trunking
- VHF / UHF Conventional
- UHF-900 MHz MAS System
- Telco Network
- GSM/GPRS
- Satellite
- Microwave…….

Wireless Communications for SCADA Systems BCWWA 2008
A powerful combination of two functions:

- Programmable Logic Controller
- Communication Modem
A Communication Oriented RTU  2/3

Store and Forward Repeater F1-F1

Reporting By Event

Node Linking two Media

Local Control of Remote Sites

Protocol Converter for PLC Links

RTU

Time Synchroniz ation

Wireless Communications for SCADA Systems BCWWA 2008
A Communication Oriented RTU  3/3

Polling via radio
Report by Event

Local Process
++
+

Network Comm.
-
+++
“Store and Forward” Links

All radio links may use the same frequency!
Backup Links Enhance Reliability

Wireless Communications for SCADA Systems BCWWA 2008
Wide Area SCADA-Data Network

Primary Water SCADA

ToolBox
IP Gateway
Ethernet

Secondary MCC
IP

Line Based network

RTU and Comm. Node

S&F Repeater
RTU for Pumping Station
RTU for Reservoir

Ethernet

S&F Repeater
Complex SCADA System

Wireless Communications for SCADA Systems BCWWA 2008
Reporting in Wireless SCADA Systems

- Cyclic Polling of RTUs
  - Complete Polling - “Tell me about all your conditions”
    - Time consuming process not suitable for wireless media
  - Report by Exception - “Tell me about only what changed”
    - Change of state that does not require immediate attention
  - Cyclic Health Check - “Indicate shortly that you are alive”
    - To minimize the health check cycle (leave time gaps for alarms)

- Initiating Unsolicited Messages
  - Report By Event - Predefined Alarm conditions
    - Must get immediate attention of the operator (critical alarms)

- Group Calls
  - Burst messages - “Everyone Accept this Message”
    - No acknowledgement is expected (“all keep quite for 5 minutes”)
Using the 7-Layer protocol sites may be configured for single frequency F3.
Wireless IP Connection with SCADA

Master Control Center

Programming ToolBox

IP Gateway

IP Network

Wireless IP Infrastructure

900 MHz – 5.7 GHz

RTU

IP Con.

IP Con.

RTU

IP Con.

IP Con.

RTU

IP Con.

Ethernet

Programming STS

Wireless Communications for SCADA Systems BCWWA 2008
Wireless GSM/GPRS Network

Site 1
- RTU
- Voice
- SCADA

Site 2
- RTU
- Voice
- Micro Wave Back Bone

Site 3
- RTU
- Voice

Site 4
- RTU
- Voice
Combined PLC and I/Os with RTU

Customer Site

I/O Control

Installed PLC or IED

RTU With radio

STS ToolBox

PLC or IED with Native protocol

Wireless Network
SCADA Security Incident Trends

Something Big Changes Here

Source: Eric Byres
Combined Set of Solutions May Help

- **Physical Security**
  - Provide adequate security to remote sites

- **Firewalls**
  - Protecting the corporate network

- **Use of private data network**
  - Public networks are often vulnerable

- **Use of “complex” protocol structure**
  - Need for specific analyzer

- **Communications Security**
  - Combined Encryption and Authentication
  - Multiple passwords across the system, etc.
Cost Saving Analysis  1/2

- Calculate the overall Economic factors:
  - Cost of lost potable water due to bursts and leakages
  - Cost of electric energy during designated period
  - Cost for repairs and replacement of equipment
  - Cost travel to remote sites for periodic checkup
  - Cost of system supervision and manual data collection

\[
\text{Cost (without SCADA)} - \text{Cost (with SCADA)}
\]

\[
\text{Saving} = \frac{\text{Cost (without SCADA)} - \text{Cost (with SCADA)}}{\text{Cost (without SCADA)}} \times 100 \%
\]
Cost Saving Analysis 2/2

Without SCADA

With SCADA

- Cost of lost potable water due to bursts and leakages
- Cost of electric energy during designated period
- Cost for repairs and replacement of equipment
- Cost travel to remote sites for periodic checkup
- Cost of manual data collection
- Total Cost
System Programming Tasks

**With Simple Protocol**
- Network Addressing
- Error Detection
  & Message Retry
- Diagnostics
- Data Security

**With Layered Protocol**
- Built In
- Built In
- Built In
- Built In

**Main Application**