Annual Spring Conference

May 5, 2011

Lessons Learned Implementing Multi-Media for Telemetry and SCADA

By:

Terry M. Stulc, P.E.

Trindera ENGINEERING

COEUR D'ALENE, IDAHO

www.trindera.com

Introduction – Topics Covered

- Brief discussion of typical telemetry and SCADA systems
  - Typical communication options
  - Typical hardware and software options
- Brief discussion of Ethernet based systems
  - Network layout and design issues
  - Communication protocols
- Discussion of implementation issues
  - Discussion of infrastructure planning and design issues
  - Discussion of hardware / component issues
  - Discussion of software development issues
  - Discussion of commissioning issues
- Case studies / example applications
- Questions & Answers Period

Introduction – Topics Covered

- Discussion focus is on:
  1. Design and implementation related issues
  2. Lessons learned from recent projects

- Discussion focus is not on:
  1. Ethernet as a technology
  2. Hardware specific issues

Common Vocabulary

- SCADA = Supervisory Control and Data Acquisition
- PLC = Programmable Logic Controller
- RTU = Remote Telemetry Unit
- MTU = Master Telemetry Unit
- HMI = Human Machine Interface
- GUI = Graphical User Interface
- OIT = Operator Interface Terminal
- I/O = Inputs/Outputs
- VHF = Very High Frequency (30MHz to 300MHz)
- UHF = Ultra High Frequency (300MHz to 3GHZ)

Starting Point For Discussions

- Audience Poll:
  - How many are familiar with Telemetry and SCADA systems?
    - RTU or PLC based system?
    - SCADA software packages?
  - What type of communication media is being used?
    - Leased line telephone?
      - Owner's communication line?
    - Radio?
      - Licensed Frequency?
      - Unlicensed Frequency (Spread Spectrum)?
    - Ethernet?
      - Fiber Based?
      - Wireless?

Typical Telemetry System Components

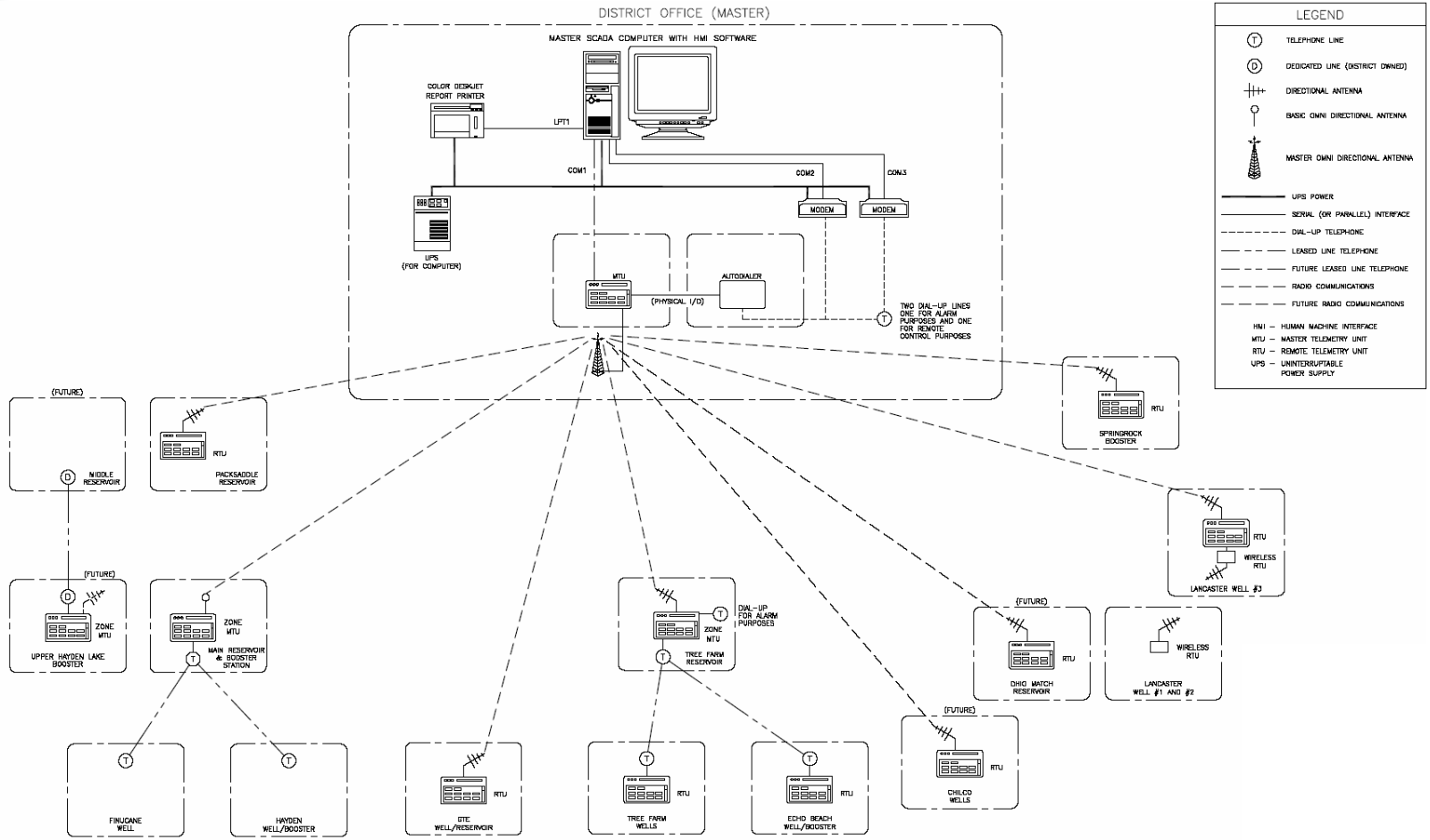
- 1. Hardware
  - Programmable Logic Controls (PLCs)
  - Remote Telemetry Units (RTUs)
  - Operator Interface Terminal (OIT)
- 2. Communication Media
  - Leased line telephone lines or dedicated line
  - Radios – FCC licensed or unlicensed
  - Wireless Ethernet
  - Other (cellular, optical fiber, power line modem, cable modem, etc.)
- 3. SCADA Software
  - Computer based Graphical User Interface (GUI)

Trindera ENGINEERING

Typical Telemetry System Communications Options

- Leased line telephone lines
  - Requires support from the phone company
    - (Initially when implementing a system, and ongoing after installation)
  - Buried lines are often dug up or damaged
  - Must rely on others for repair or reconnection
- Radios
  - Sometimes not an option based on terrain/signal limitations
  - FCC licensed radios require interaction with FCC
  - Unlicensed radios are typically lower power, and line of sight
  - Other – weather, towers, etc.

Example Network Block Diagram Combination Telephone Lines / Radios



Radio Based Communications

- Licensed Frequency Radios:
  - 2-5 watt power output depending on the input voltage
  - Analog Radios
    - VHF: 130-150, 150-174 MHz
    - UHF: 406-430, 450-470 MHz
  - Digital Radios
    - VHF: 132-174 MHz
    - UHF: 380-512 MHz
- Unlicensed Frequency Radios:
  - Spread spectrum (above 900MHz or 2.4GHz)

Spread Spectrum Radios

- AKA Unlicensed, License Free radios, or Frequency Hopping radios
- Nikola Tesla first patented the concept of frequency hopping in July 1900
  - Tesla came up with the idea after demonstrating the world's first radio-controlled submersible boat in 1898, when it became apparent the wireless signals controlling the boat needed to be secure from "being disturbed, intercepted, or interfered with in any way."
- Concept: “spread" the radio signal over a wide frequency range several magnitudes higher than minimum requirement. The core principle of spread spectrum is the use of noise-like carrier waves, and, as the name implies, bandwidths much wider than that required for simple point-to-point communication at the same data rate
- Initial commercial use of spread spectrum began in the 1980s
- In 1985 FCC decided to permit unlicensed use of spread spectrum in 3 bands at powers up to 1 Watt (for Wi-Fi, Bluetooth, cordless phones, etc.) under 47 CFR 15.247

Spread Spectrum Radios

- Not all spread spectrum radios are alike:
  - Frequency-hopping spread spectrum (FHSS),
  - Direct-sequence spread spectrum (DSSS),
  - Time-hopping spread spectrum (THSS),
  - Chirp spread spectrum (CSS),
  - Combinations of these techniques are forms of spread spectrum.
- Each of these spread spectrum techniques employs pseudo-random number sequences - to determine and control the spreading pattern of the signal across the allotted bandwidth
  - Some use the entire allotted bandwidth all the time (DSSS)
  - Some use the allotted bandwidth on a periodic basis (FHSS, THSS)
- Wireless Ethernet standard IEEE 802.11 uses either FHSS or DSSS in its radio interface

Spread Spectrum Radios

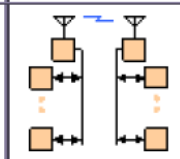
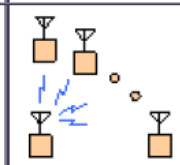
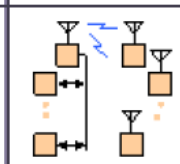
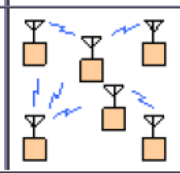
- **Frequency-hopping spread spectrum (FHSS)**
  - A method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both the transmitter and receiver.
- **Direct-sequence spread spectrum (DSSS)**
  - Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal (i.e. code it) at one end, then un-code it at the other yet.
  - The transmitted signal takes up more bandwidth than the information signal that is being modulated. The name 'spread spectrum' comes from the fact that the carrier signals occur over the full bandwidth (spectrum) of a device's transmitting frequency.
  - 802.11b wireless modems use DSSS signaling.
- **Time-Hopping Spread Spectrum (THSS)**
  - The carrier frequency is turned on and off by a pseudorandom code sequence.
- **Combinations of the above**

Spread Spectrum Radios

- Resistance to interference
  - DS is better at resisting continuous-time narrowband interference
  - FH is better at resisting pulse interference
- Encryption (resistance to eavesdropping)
  - The spreading code (in DS systems) or the frequency-hopping pattern (in FH systems) is often unknown by anyone for whom the signal is unintended, in which case it "encrypts" the signal and reduces the chance of an adversary's making sense of it
  - However, for mission-critical applications, particularly those employing commercially available radios, spread-spectrum radios do not intrinsically provide adequate security; "...just using spread-spectrum radio itself is not sufficient for communications security“
- Multiple access capability
  - Multiple users can transmit simultaneously on the same frequency (range) as long as they use different spreading codes

Wireless RTUs

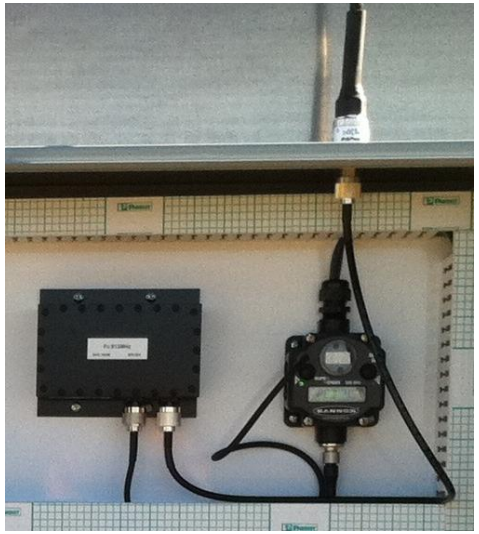
- Combination RTU and Ethernet Radio
- 900 MHz and 2.4 GHz Spread Spectrum
- Configured, not programmed
- Applications well suited for include:
  - Limited I/O applications
  - Reservoir monitoring
- Not so well suited for:
  - Applications requiring more I/o
  - Applications requiring programming
  - Wells/Booster Stations with multiple pumps and instrumentation

Wireless I/O Network	Block Diagram	Description
Point to point		2-way I/O between 2 locations
Point to point (expandable I/O count)		2-way high I/O count between 2 locations
Point to multipoint		Control of many locations from a central Host
Point to multipoint with expandable Host I/O count		2-way I/O between many locations and a central Host
Distributed I/O - expandable I/O count mesh network		2-way I/O between many locations (mesh network)

Trindera ENGINEERING

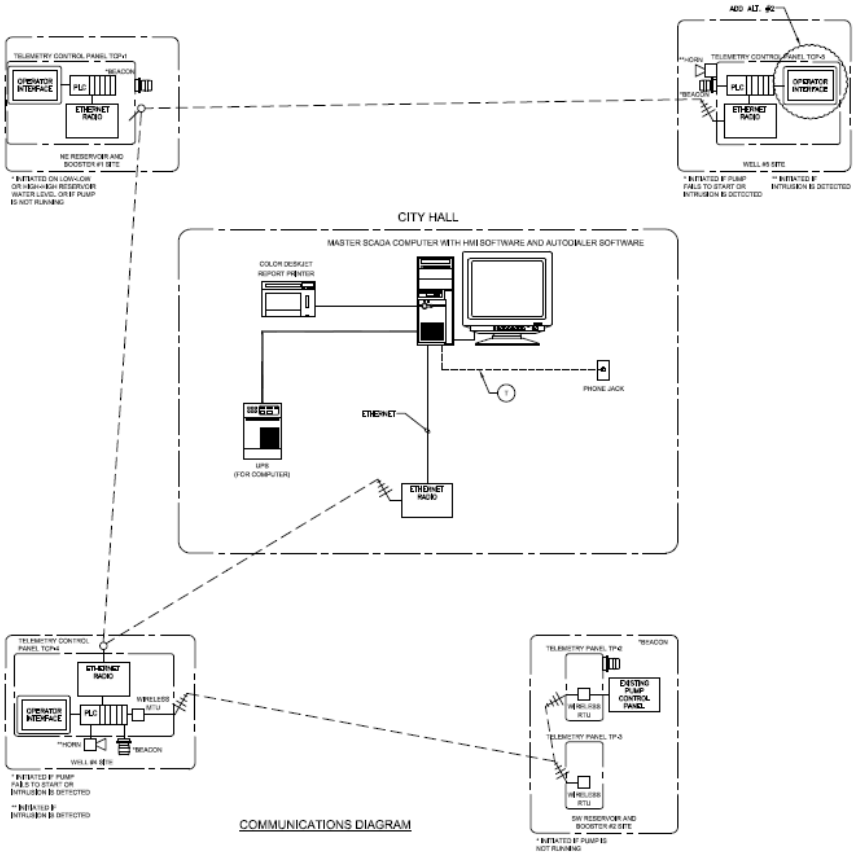
Case Study:
Troy, ID Water System Telemetry

- Radio based peer-to-peer telemetry system
  - Platform: Wireless RTU system
  - Problem: radio signal interference from adjacent system(s)
  - Solution: installed band pass filter to “filter out” noise



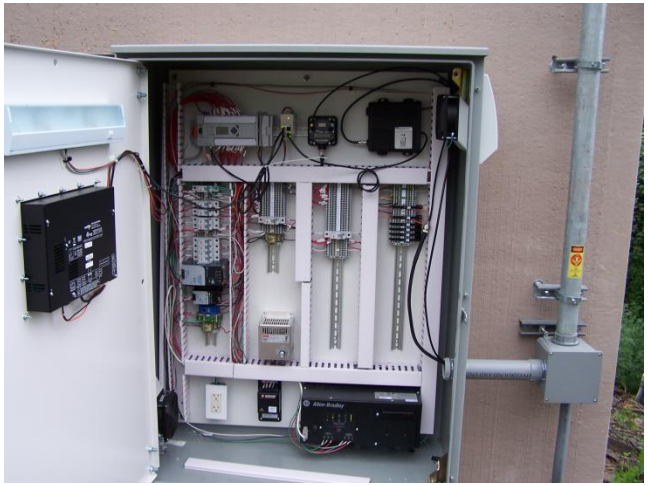
Case Study:
Rockford, WA Water System Telemetry

- Hybrid Radio System



Case Study:
Rockford, WA Water System Telemetry

- Hybrid Radio System
  - Platform: PLC with Ethernet Radio (Spread Spectrum) <u>AND</u> Wireless RTU (Spread Spectrum)
  - Issue: two different antenna needs
  - Problem: two different vendors (source of support)
  - Solution: engineer/contractor/vendor solution



FCC Licensing
Key Deadlines

- Beginning **January 1, 2011**, FCC will no longer accept applications for new or modifications of existing wideband 25KHz operations
  - (*i.e.* operating with only one voice/data path per 25 kHz of frequency spectrum)
- By **January 1, 2013**, Industrial/Business and Public Safety Radio system licensees must
  - operate on 12.5 kHz narrower channels, <u>or</u>
  - employ a technology that achieves the narrowband equivalent of one channel per 12.5KHz of channel bandwidth (voice) or 4800 bits per second per 6.25 kHz (data).

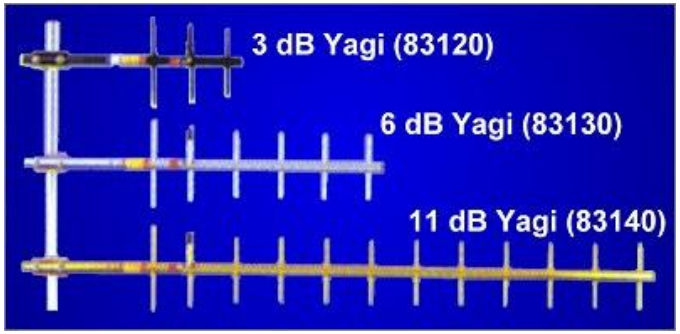
Case Study:
ESWD#1, Telemetry System Planning

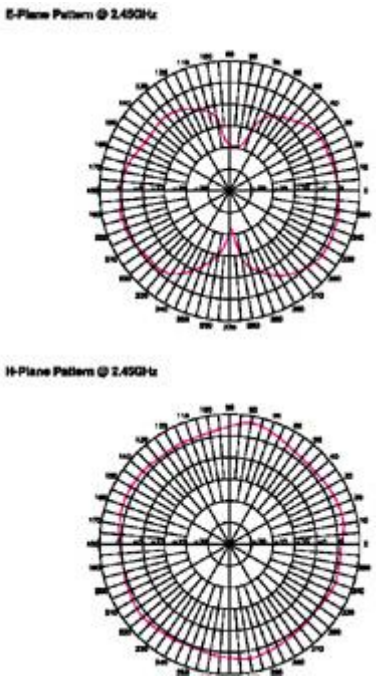
- Conventional RTU/Radio System
  - Platform: Older (obsolete) RTUs, with older (not-obsolete) licensed frequency radios
  - Issue: Upgrade just RTUs, or both RTUs and Radios
  - Problem: radios are licensed at older channel spacing (25KHZ)
  - Possible Solutions:
    - Replace radios with current technology (licensed frequency with 12.5KHZ channel spacing)
    - Replace radios with spread spectrum units (unlicensed)

      *District may not get license back in the future.

Trindera ENGINEERING

Telemetry Antennas Types





Direction Antenna

Omni-Directional Antenna

Combination Antenna

Telemetry Antennas and Grounding

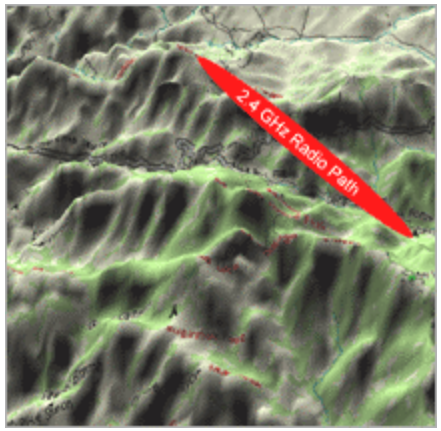
How to ground antenna?

Where ground antenna

How to mount antenna?

Lessons Learned – Radio Based Systems

- Designing a radio based telemetry system often requires expertise in the following:
  - Radio frequency interference analysis
  - Radiation exposure analysis
  - Site development plans
  - FCC licensing
  - Antenna supporting structures
  - Anomalous propagation analysis
  - Performance troubleshooting
  - Network security



Ethernet (and Industrial Ethernet)

Per Wikipedia:

- Ethernet was developed between 1973 and 1975
- Ethernet is a **family** of frame-based (packets) computer networking technologies for local area networks (LAN)
- It defines a number of wiring and signaling standards for the physical portion of the standard network model and the addressing format to be used on the physical network.
- **Internet Protocol** (**IP**) is the principal communications protocol used for relaying data packets across the network

Ethernet (Industrial Ethernet)

- Two original components of IP Protocol Suite:
  - Transmission Control Protocol (TCP)
  - Internet Protocol (IP)
  - Therefore the entire suite is commonly referred to as *TCP/IP*
- TCP/IP is composed of layers:
  - **IP** - is responsible for moving packet of data from node to node based on a destination address (the IP number)
  - **TCP** - is responsible for verifying the correct delivery of data from client to server. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received
    - TCP is the protocol that major Internet applications rely on
      - Applications such as the World Wide Web, e-mail, and file transfer
    - TCP provides a point-to-point channel where reliable communications is required
      - The Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP) are examples of applications that require a reliable communication channel

Ethernet for Industrial Applications

- TCP/IP designed to be robust and automatically recover from any node or phone line failure
- This design allows the construction of very large networks with less central management
- However, because of the automatic recovery, network problems can go undiagnosed and uncorrected for long periods of time
- Non-deterministic, therefore other industrial solutions have been implemented to address above
- **Industrial Ethernet (IE)** includes number of techniques are used to adapt Ethernet for the needs of industrial processes, which must provide ***real time*** behavior.
  - "By using standard Ethernet (Industrial Ethernet), automation systems from different manufacturers can be interconnected throughout a process plant" ☺

Trindera ENGINEERING

Example Automation Network Protocols

- **Process automation protocols**
- **FOUNDATION fieldbus** - H1 & HSE
- **Profibus** - by PROFIBUS International.
- **PROFINET IO**
- **CC-Link Industrial Networks** - Supported by the CLPA
- **CIP (Common Industrial Protocol)** - Can be treated as application layer common to DeviceNet, CompoNet, ControlNet and EtherNet/IP
- **Controller Area Network** utilised in many network implementations, including CANopen and DeviceNet
- **ControlNet** - an implementation of CIP, originally by Allen-Bradley
- **DeviceNet** - an implementation of CIP, originally by Allen-Bradley
- **DirectNet** - Koyo / Automation Direct proprietary, yet documented PLC interface
- **EtherNet/IP** - IP stands for "Industrial Protocol". An implementation of CIP, originally created by Rockwell Automation
- **Ethernet Powerlink** - an open protocol managed by the Ethernet POWERLINK Standardization Group (EPSG).
- **EtherCAT**
- **Interbus**, Phoenix Contact's protocol for communication over serial links, now part of PROFINET IO
- **HART Protocol**
- **Modbus** RTU or ASCII or TCP
- **Modbus Plus**
- **Modbus PEMEX**
- **Ethernet Global Data (EGD)** - GE Fanuc PLCs (see also SRTP)
- **FINS**, Omron's protocol for communication over several networks, including ethernet.
- **HostLink Protocol**, Omron's protocol for communication over serial links.
- **MECHATROLINK** - open protocol originally developed by Yaskawa.
- **MelsecNet**, supported by Mitsubishi Electric.
- **Optomux** - Serial (RS-422/485) network protocol originally developed by Opto 22 in 1982.
- **Honeywell SDS** - Smart Distributed System - Originally developed by Honeywell. Currently supported by Holjeron.
- **SERCOS interface**, Open Protocol for hard real-time control of motion and I/O
- **SERCOS III**, Ethernet-based version of SERCOS real-time interface standard
- **GE SRTP** - GE Fanuc PLCs
- **Sinec H1** - Siemens
- **SynqNet** - Danaher
- **TTEthernet** - TTTech

Ethernet options

- Fiber optic based Ethernet
  - Must address issues similar to leased line telephone if fiber provided by utility
  - Must address issues similar to dedicated line telemetry if fiber provided by owner/end-user
- Wireless Ethernet
  - Must address issues similar to unlicensed radio based telemetry
    - Terrain
    - Installation requirements (towers, etc.)
    - Weather

Ethernet “Plug and Play”?

- What does all this mean?
- Is Ethernet “Plug and Play”?
  - Not all Ethernet is created equal!
  - One major PLC Vendor advertises:
    - “…PLC… platforms are ***Ethernet-ready*** and can be used to coordinate I/O or data transfer between a PLC and up to 64 cyclically scanned I/O devices, as well as up to 32 simultaneous *Modbus TCP/IP* server connections, satisfying the requirement for real-time access to diagnostics, system health or maintenance remotely or locally.”
  - Another major PLC Vendor implements Ethernet/IP (only)

Case Study:
City of Airway Heights, WA – SCADA

- AHWRP Ph1B – Plant SCADA
  - Design called for all one vendor for PLCs and OITs
  - Greenfield project, open bid process
    - No basis for sole source equipment
  - Ended up with one brand of PLCs and another brand of MCCs (VFDs, Power Monitors, etc.)
    - PLCs used one Ethernet protocol, the MCCs another
    - Required gateways, managed switches etc.

Ethernet Hardware Components

- Components used to connect devices to provide shared communication among PLCs and control devices may include:
  - Hubs
  - Switches
  - Managed Switches
  - Routers
  - Gateways and bridges
  - Cables

Ethernet Standards

- Wired
  - IEEE 802.3 is a collection of standards produced by the working group defining the physical layer and data link layer of wired Ethernet
- Wireless
  - IEEE 802.11 is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4GHz, 3.6GHz and 5 GHz frequency bands
  - FCC Part 15 Rules and Regulations

Case Study:
City of Airway Heights, WA – SCADA

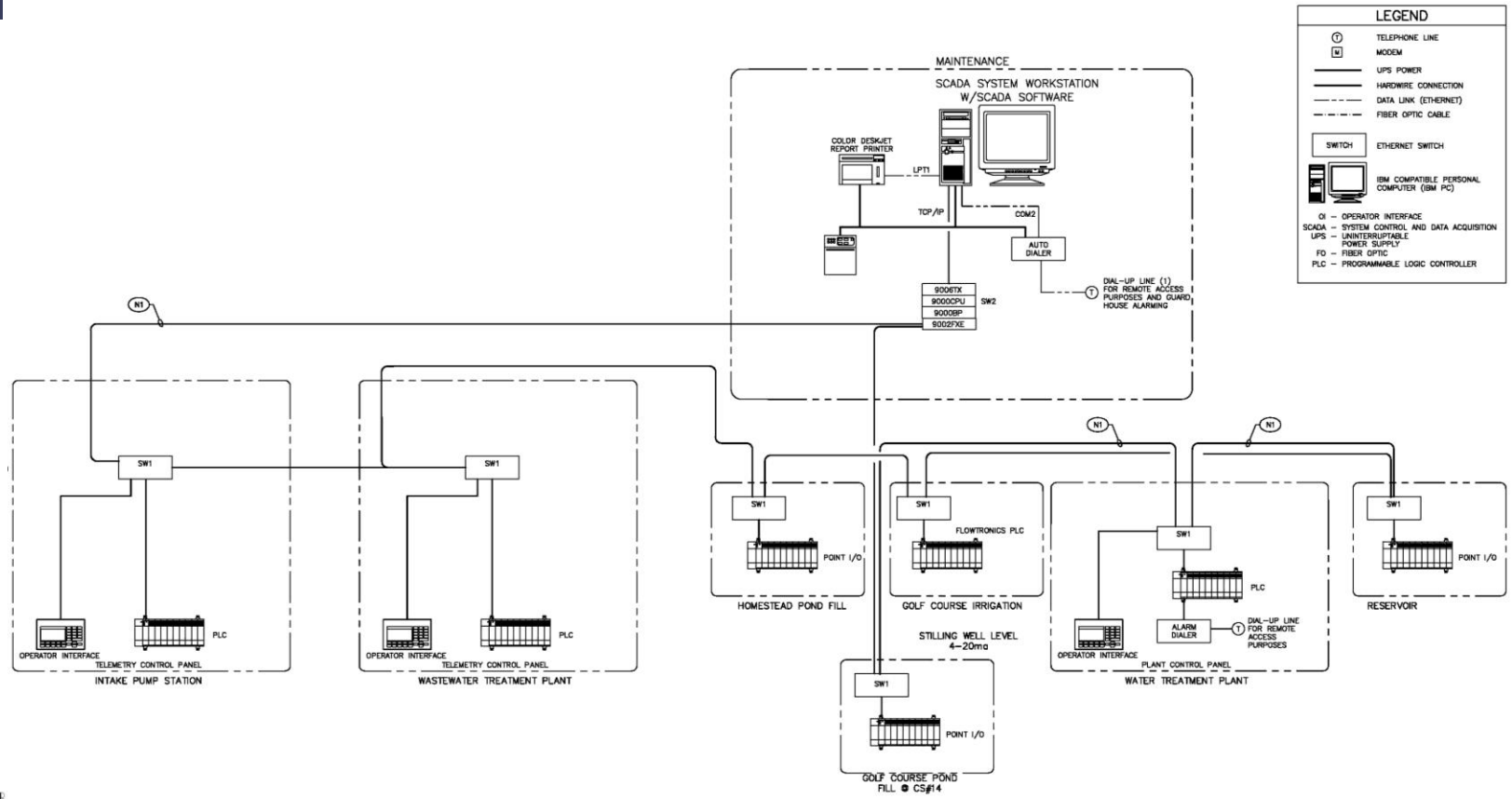
- AHWRP Ph1B – Telemetry Link to Plant SCADA
  - Design Intent vs. Operators' Desires
    - Planned for simple alarming/monitoring telemetry link. Specified licensed frequency radios with PLC control
    - Limited data, no graphics transmission, no video
    - Operators desired to see Plant SCADA at Lift Station and vice versa
      - Required more data to be transferred
      - Required SCADA Graphics to be transferred
      - Required more bandwidth
      - Ended up switch to license free Ethernet radios.

Other Example Ethernet based Telemetry/SCADA Systems

- Gozzer Ranch Golf and Lake Club, Coeur d'Alene, ID
  - Dedicated Owner installed fiber optic cable
- City of Cheney, WA
  - Combination wireless Ethernet (radio/modems) and City owned fiber optic cable
- Idaho Club, Sandpoint, ID
  - Dedicated Owner installed fiber optic cable

Trindera ENGINEERING

Gazer Ranch
Water/Wastewater System Telemetry System



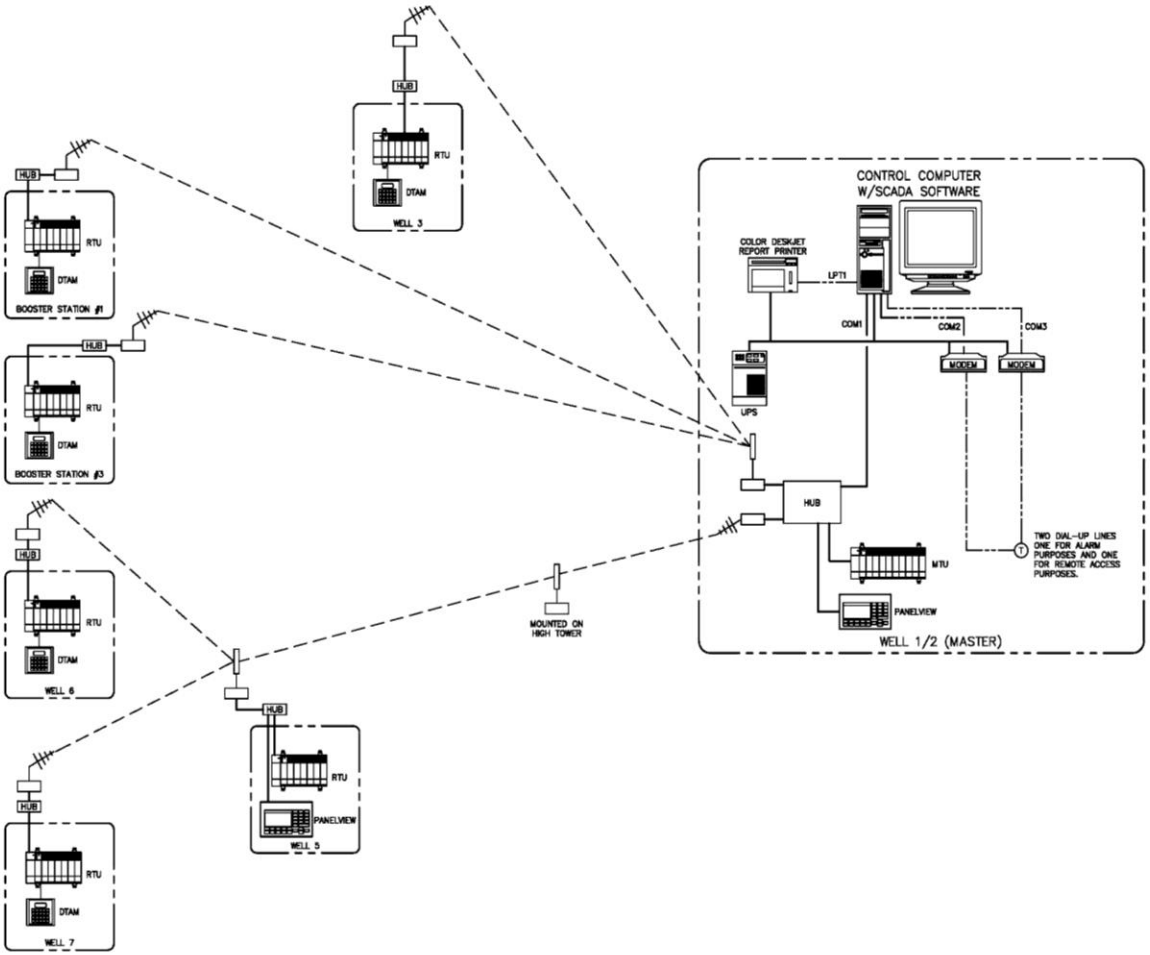
JUST ADD WATER
A Recipe for Life

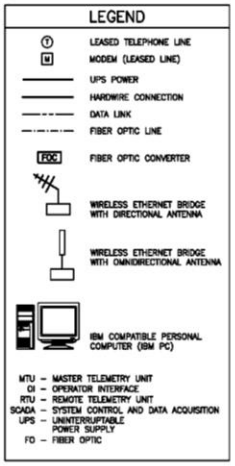
Trindera
ENGINEERING

Gazer Ranch
Water/Wastewater System Telemetry System

- Lessons Learned
  - Design of fiber infrastructure key to successful implementation
  - Need to ensure fiber infrastructure on standby power
  - Operator access locations can alter need for Master SCADA
  - Installation restraints - size, cooling requirements, aesthetics
- Positives
  - Peer-to-peer network
  - Ownership of infrastructure
  - Accessibility, flexibility, speed
- Opportunities for improvement
  - Software functional description - define prior to software development and deployment

City of Cheney
Water System Telemetry System





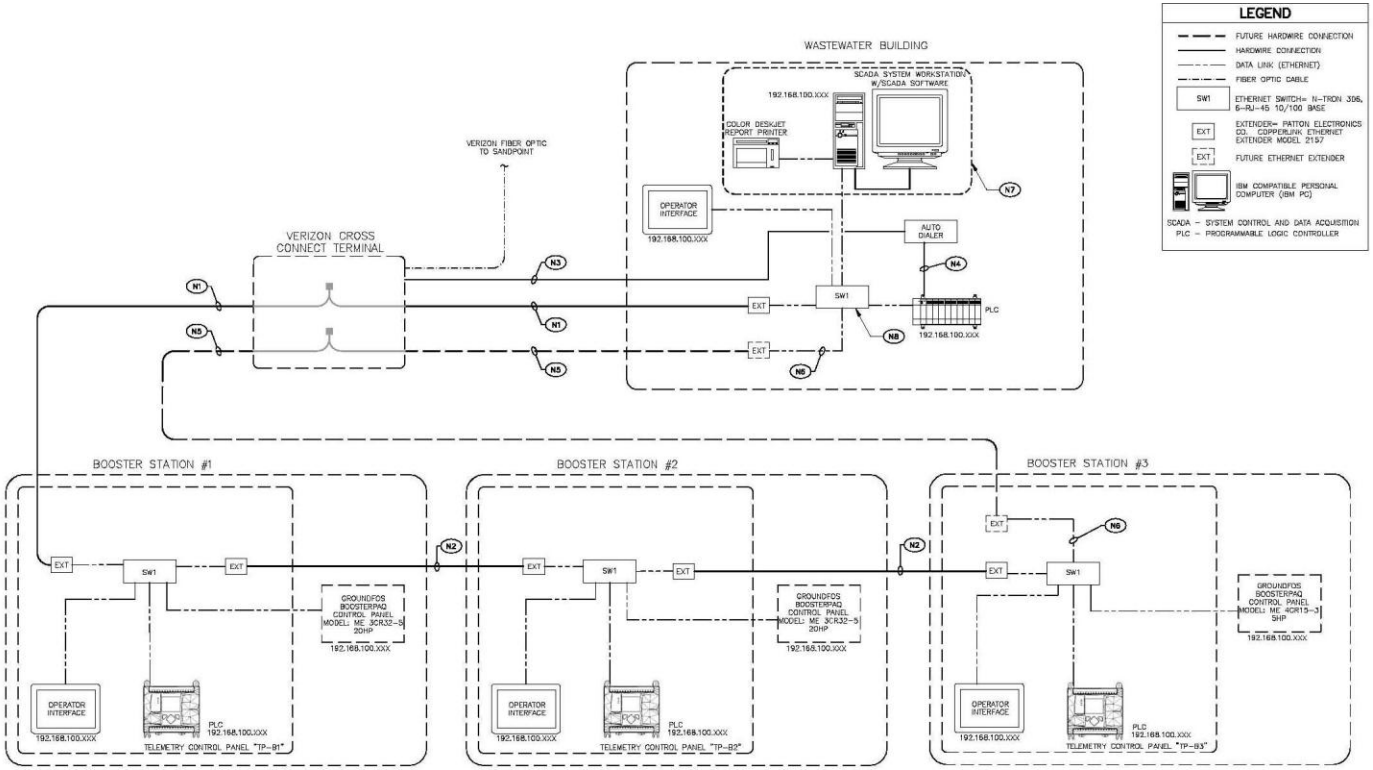
JUST ADD WATER
A Recipe for Life

Tringera ENGINEERING

City of Cheney
Water System Telemetry System

- Lessons Learned
  - City's plan for fiber optic cable infrastructure didn't extend to all locations where telemetry was required
  - Extending the fiber trunk to the wells, boosters and reservoirs was cost prohibitive
  - Extending the fiber drops to the wells, boosters and reservoirs was also cost prohibitive
  - Forced to alter plan and utilize wireless Ethernet radios
- Positives
  - Entirely City owned infrastructure
- Opportunities for improvement
  - Original plan not implemented
  - Hybrid communication network – communication system programming cumbersome

Idaho Club
Water/Wastewater System Telemetry System



JUST ADD WATER
A Recipe for Life

Trindera
ENGINEERING

Idaho Club
Water/Wastewater System Telemetry System

- Lessons Learned
  - Owner plans for infrastructure change frequency
  - Owner must commit to infrastructure options early in project
  - Utility must also commit to infrastructure options early in project
  - Operators must weigh in on required access locations and requirements for Master SCADA
- Positives
  - Peer-to-peer network
  - Accessibility, flexibility, speed
- Opportunities for improvement
  - Ownership of infrastructure
  - Decisions on required system functional requirements
  - Software functional description

Ethernet (Continued)

- Wired Ethernet
  - Twisted pair (copper)
  - Co-axial cable (copper)
  - Optical fiber cable (fiber optic)

Speed [Mbit/s]	Distance [meters]	Name	Standard / Year	Description
1	100 (nominal)	StarLAN	(pre) 802.3e 1986	Runs over four wires (two twisted pairs) on telephone twisted pair or Category 3 cable.
10	100 (nominal)	LattisNet	(pre) 802.3i 1987	Runs over four wires (two twisted pairs) on telephone twisted pair or Category 3 cable.
10	100 (nominal)	10BASE-T	802.3i 1990	Runs over four wires (two twisted pairs) on a Category 3 or Category 5 cable. Star topology with an active hub or switch sits in the middle and has a port for each node. This is also the configuration used for 100BASE-T and gigabit Ethernet.
100	100	100BASE-TX	802.3u 1995	Category 5 cable copper cabling with two twisted pairs.
1000	100	1000BASE-T	802.3ab 1999	Category 5 cable Category 5e strongly recommended copper cabling with four twisted pairs. (each pair is used in both directions simultaneously)
10 000	100	10GBASE-T	802.3an 2006	Uses Category 6a cable.

Case Study:
Hamilton, MT WWTP SCADA

- Hamilton, MT WWTP SCADA
  - Platform: Vendor provided PLC based control system (i.e. packaged system)
  - Issue: Vendor's PLC = Ethernet capable, let's integrate with Plantwide SCADA
  - Problem: City went out and bought/installed "Ethernet" cable
    - Bought and installed Cat3 cable
    - Required Cat5E due to speed and distance
  - Solution: Spent 8-10hours (over several days) during startup trying to make the Plant PLC talk to the Vendor's PLC

How Ethernet Networks Enhance Telemetry Systems

- Accessibility
  - Peer-to-Peer network topology, not Master-Slave
  - Operators can access all site, and all information from all sites, if software is properly developed
- Flexibility
  - Can easily add, remove or revise data points across the network
  - Alarm generation and logging
    - At local OIT and also at Master SCADA
  - Historical and real-time data logging and trending
    - At local OIT and also at Master SCADA
- Maintenance and support access via Internet

How Ethernet Networks Enhance Telemetry Systems

- Since, telemetry means to bring data to a central location, and since SCADA has three basic functions (control, monitoring and data archiving (trending and reporting), then Ethernet enhance telemetry system by;
  - Allowing more data to be transmitted and accessed easier,
  - Allowing operators a better view of what is happening in the field,
  - Allowing operators to manipulate alarms and set points from both central and remote locations.

Design Issues

- Due to increased accessibility to data points, operator interface displays must be more clearly defined
- Local access versus centralized access must be more clearly defined
- Flexibility leads to security issues
- Must address Internet security issues if allowing remote access
- Need to loop system if possible
- Need to ensure head-end network is on standby power, not just remote sites

Summary

- Discussion of telemetry and SCADA system components
- Discussion of radio or leased line telemetry versus Ethernet based telemetry
- Discussion of planning and design issues
- Discussion of implementation issues

Summary

- **<u>Questions and Answers</u>**

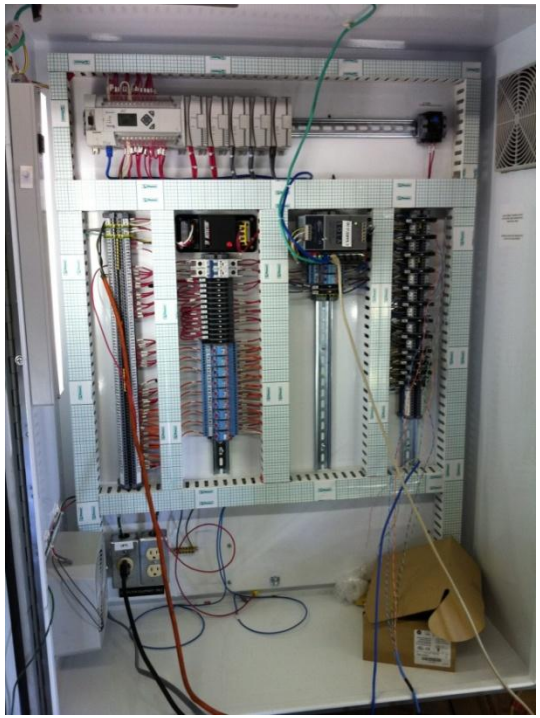
Trindera
ENGINEERING

Other Considerations

- **<u>Other Design and Implement Issues</u>**

Programming terminal connection

- Operator safety
- External connections versus internal (to panel)



Grounding Issues

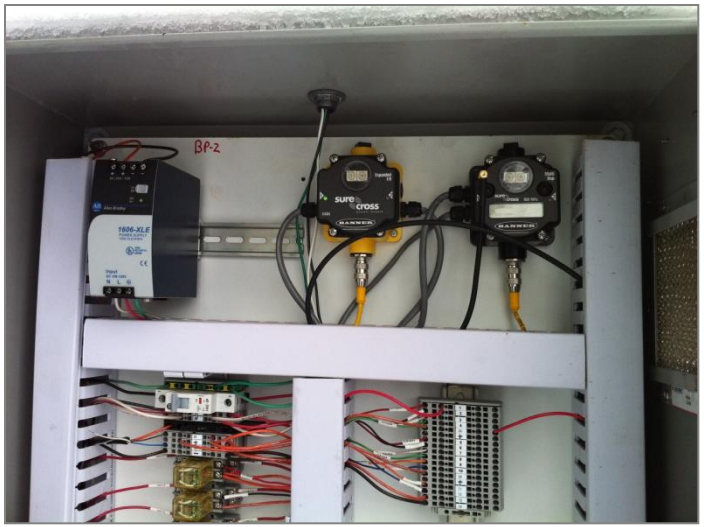
- Ground rods – type, size and installation

Grounding Issues

- Where to ground
- How to route ground conductor

Grounding Issues

- Where to ground
- How to route ground conductor

Installation Details

- Conduit penetrations and sealing