Above and Beyond SCADA: Expanding Horizons through Technology

Brian M. Hunter

Supervisory Control And Data Acquisition (SCADA) systems have been around for as long as most can remember. The need to monitor and control remote systems has resulted in a succession of SCADA evolutions over many decades. Until recently, the vast majority of these were simple monitoring systems with limited control. The advent of the microcomputer and Programmable Logic Controller (PLC) has allowed a quantum leap forward, giving utilities the means to monitor and control an unlimited amount of "points," store and transmit huge volumes of data, and graphically represent all this information to the system operator. While this capability has been around for a quite a few years, the ability to rapidly transport the information has been somewhat lacking. New technologies developed primarily for the Internet are now available to remedy this shortcoming.

Communications Bottlenecks

While PLCs and PCs can handle and transmit the necessary data, many times the existing SCADA communications links are not capable of handling it because of bandwidth limitations. Examples of information requirements of modern utilities include:

- Plant flow(s), Pressure(s), and Level(s)
- Pump status
- Power Conditions
- Alarms
- Regulatory data
- Security Information

The facility local computer system may be capable of monitoring and storing these data points because even older systems have the Input/Output (IO) capacity to do so. However, in many instances the data must be transcribed or printed locally if there is no efficient way to transmit it back to a central site for processing.

SCADA systems are traditionally a combination of "evolutions" that have been integrated in steps over time. Each step is driven by a need for increased information capacity (generally of operational nature). Where an existing communication link exists, little attention is paid to the need for getting the data back in a fast, economical, and reliable manner, often resulting in a system that is slow and frustrating to the owner. Additionally, it may result in a mistrust of the data that is presented.

In the case of Orange County and many other utilities, radio links were utilized to transmit SCADA information back and forth between remote facilities and the central site. As facilities were added, there was a corresponding increase in data transmission needs. Each new facility also meant a new radio link, further increasing maintenance burdens and reliance on an already complex and fragile system. Eventually, a communications bottleneck occurred. And you thought you were alone?

Horrible Truths About Radio

The advent of radio presented the world with a new and fantastic tool that completely revolutionized communication. With radio, news and data could be transmitted at nearly the speed of light, the world over. It was a natural and logical step to apply this new tool to utility remote control and monitoring systems such as SCADA.

In this day, the available radio spectrum for communications has been allocated to a vast number of uses. The Federal Communications Commission was established to oversee the use of various bands and to ensure that radio would stay a viable medium for years to come. This monumental task was doomed to eventual failure by human factor and equipment limitations.

As more and more radio users jammed the airways, the signal "noise" on all radio bands increased exponentially. The need for inexpensive equipment increased interference with adjacent users due to poor filtering, over modulation, and frequency drift. Also, users who are interfered with tend to "boost" their signals with amplifiers, causing their signals to interfere with other users located hundreds of miles away. This is commonly referred to as "skip."

Radio-based systems located in large metropolitan areas are especially susceptible to these types of interference because of the large concentration of systems in the area. Examples of problems associated with dense usage areas include:

- Adjacent frequency splatter.
- Outright use of the licensed frequency by another (illegal).
- Extraneous noise generated by lighting and power line leakage.
- Very near transmitters (including mobile users).
- RF leakage from large numbers of computing systems.

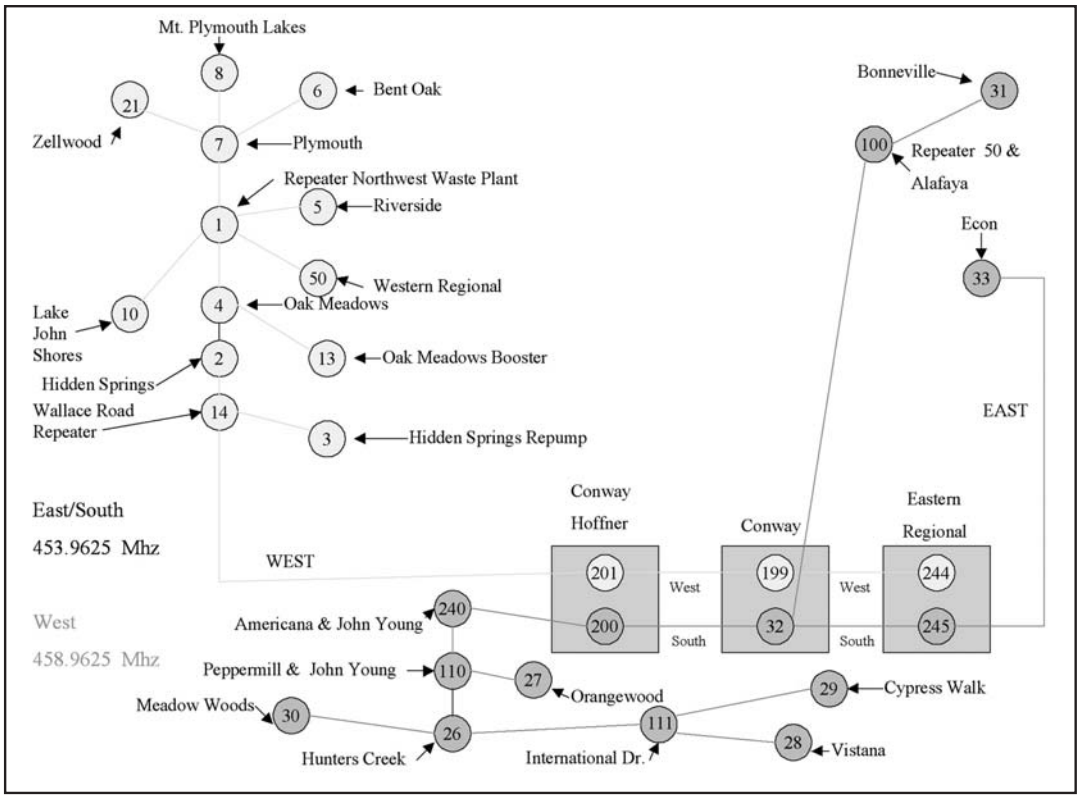
All these factors tend to make radio noise that can appear on a SCADA frequency at any time. The fact that most SCADA transmitters are limited to less than 5 watts of power means that a SCADA radio signal may not be heard through the hail of noise, splatter and stray signals in the area.

Orange County Utilities previously utilized two licensed frequencies in the 450 MHZ range. This system provided the SCADA data communications for 18 facilities. As with most systems, additions over the years had required the use of repeater sites and a combination of series and parallel branches to achieve the required links. A diagram of the original architecture is shown on page 39.

As one can see, any failure at a sequential repeater site would cause a loss of communications with sites located ahead of that point. This type of system is extremely vulnerable to interference, lightning strikes, thermal overload, and equipment failure. Additionally, the radio equipment was custom made and required specialized training and test equipment to calibrate and repair.

Adjacent radio users included the designation of "land mobile". This includes taxi service, trucking dispatch and the like. Users of this equipment tend to purchase inexpensive transceivers that are subject to the conditions mentioned previously, often resulting in communications failures that were sporadic or lengthy, depending on the type of interference.

Brian M. Hunter, CSM, CPM, is a utility supervisor in the Water Division of Orange County Utilities.



Original SCADA Radio Links

All these factors, coupled with the slow response of the communications (data bottleneck), made the former radio-based system less than desirable.

Technology to the Rescue

An evaluation was made to determine what technologies were available to remedy this situation. A criterion was developed to formulate an approach. What did OCU need and expect from the system, currently and in the future? The major requirements considered were:

- Sufficient bandwidth to support current and future needs.
- Enhanced reliability.
- Reduced maintenance and training burden.
- Commercially available.
- Non-proprietary.
- Ease of expansion/contraction.
- Enhanced capabilities.
- Cost (initial and recurring).

Enhanced radio was evaluated. This included Spread Spectrum systems that transmit data over many frequencies to alleviate interference problems. These were deemed to have insufficient bandwidth to provide for current and future needs. Also, the "line of sight" and low power aspects were considered undesirable in a metropolitan setting.

Fiber optic was evaluated as well. The extreme distances involved and the number of sites made this alternative fiscally unacceptable due to the high capital outlay involved. (However, utilities should examine installing FO wherever a new water or sewer main is being placed. This allows the utility to eventually "grow" a wide area network at a vastly reduced cost).

Integrated Services Digital Networking (ISDN) and Frame Relay transport was identified as a viable technology that could meet the challenge.

What is ISDN/Frame Relay?

ISDN is simply a sophisticated, digital phone line that is capable of transmitting voice, data, and video simultaneously. Standard analog telephone (POTS) is capable of doing this, but only at very slow rates through an analog modem. The ISDN technology is generally a 64-kilobit-per-second (kbs) connection that allows easy digital interface with many transmission protocols. This flexibility allows the utility to interface with a myriad of PLCs, RTUs, and computing devices. ISDN is widely available from most local providers and generally can be connected using an existing phone cable to the facility. The ISDN line represents the physical connection to each facility to be placed on the SCADA system. These lines transport the data back and forth to the Frame Relay network.

The Frame Relay system is a large network of computers or "switches" which route data packets from one address to another. Frame Relay was developed to handle the anticipated traffic requirements of the e-commerce revolution. As most are aware, the explosive growth did not occur and many dot-com companies disappeared into oblivion. Large providers invested heavily into the construction of infrastructure to meet these demands that never materialized. A progressive utility may now reap the benefit by negotiating cost and seeking competition between providers, eager to "re-purpose" their Frame Relay systems.

Frame Relay examines the address that is "framed" around the data and routes it through the network of switches to its final destination, without regard to what is contained within. The contents of each frame may be voice, video, or other types of data packets. The Frame Relay is only concerned with getting each frame to its designated recipient, allowing the combination of ISDN and Frame Relay to be much more flexible than any radio link available to SCADA users.

The combination of these technologies is used in hundreds of networks throughout the world to connect LAN, Internet, and voice applications. Frame Relay systems can provide worldwide control networks for very large institutions and utilities. Such systems may be comprised of many networks bridged together, using satellite and transoceanic fiber optic as part of their communications physical layer. For the most part, a municipal utility will be utilizing a local system within its geographical area; however, in the event that it is necessary to send data to far destinations, the local provider could easily do so through its bridge or portal.

Frame Relay service, like ISDN, is available from a local provider and constitutes nothing proprietary in nature. The Orange County Water Production Section currently operates 19 separate facilities from the Eastern Regional. Each facility PLC is connected through the system to the control room SCADA system (see the basic system diagram).

As illustrated in the diagram, a router is installed at each remote facility that

Continued on page 40

Continued from page 39

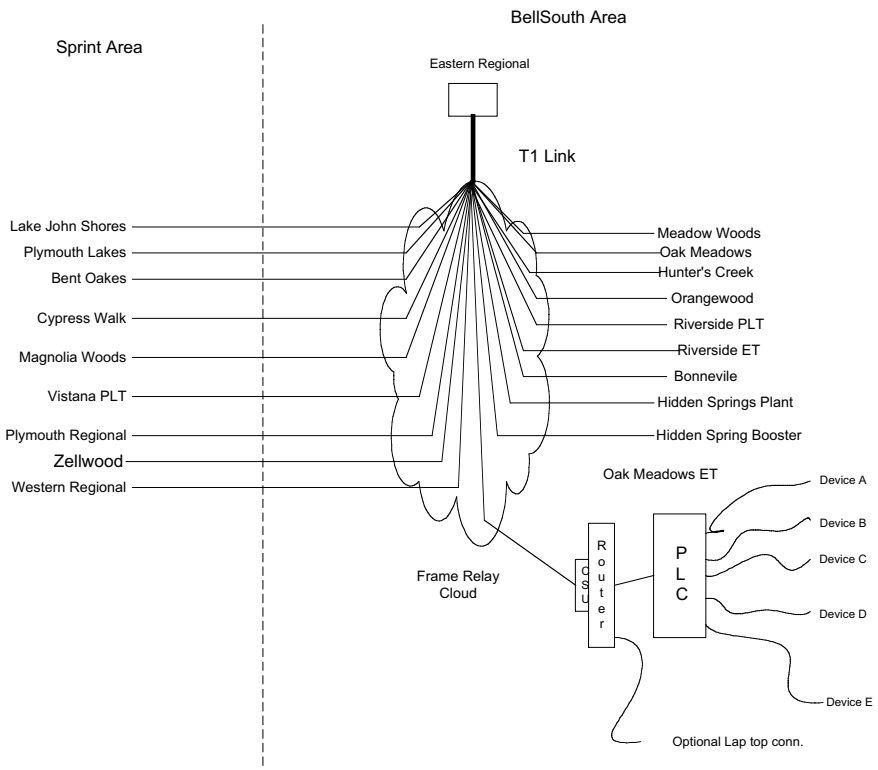
"frames" the PLC word (data) into a TCP/IP packet and transmits it over the ISDN line to the Frame Relay. The Frame Relay then routes the data to the appropriate exit node connected to the Central Site destination router. All routers have a unique address or set of addresses, much as your phone number is the only one like it in the world. This ensures that the data arrives only at the address it was intended for.

The destination router then sends the data packets over an Ethernet network to the SCADA Human Machine Interface (HMI). The data is interpreted by the HMI application and manipulated for display to the operator. Data (commands) are issued to the remote facility PLC in the reverse, but like order. Note that the connection between the Frame Relay and the control center is a full T-1 line. This is necessary to provide bandwidth for the combined data sent and received at the Eastern Regional. (T-1 is a 5.44-million-bit-per-second connection).

This architecture is very reliable when compared to radio. First, the Frame Relay is a "self healing" system that will route data frames around any roadblocks or point failures in the system. Second, each remote facility is connected in a star configuration. Failure of any ISDN line does not affect the other facilities. Frame Relay systems are operated by large entities and carry data that represents significant value, both economically and socially. Most carry information for banks, hospitals, or retail chains. Loss of communication places the provider in a liable situation; therefore, great care is taken in the maintenance and operation of the system. Generally these networks are monitored continuously and maintenance is immediately available 24 hours daily.

Migration to Frame Relay can greatly alleviate the utility of the maintenance burden associated with radio-based systems. When needed, repair and maintenance is performed by the provider, freeing up resources for the user to concentrate elsewhere. Some providers will even supply and support the router(s) located at each facility. There are initial installation and set-up fees associated with the migration to this type of system, as well as monthly lease fees for each line and the Frame Relay service. In Orange County, these costs roughly equal those of maintaining the radio system. Labor that was previously expended on radio system maintenance has been redirected to core utility needs.

Orange County Water Production
ISDN / Frame Relay SCADA Architecture *(Simplified)*



The Good Stuff

In this day of "doing more with less" and the jumble of regulatory burdens, the modern utility is driven to find ways to increase and enhance services. Additionally, competition forces us to optimize treatment and labor costs wherever possible. Moving above and beyond SCADA is possible with an enhanced system.

Given the fact that the ISDN/Frame Relay system allows the utility to collect vast, real-time data and transmit other forms of intelligence, the utility can begin to explore ways to enhance and optimize its effort. By coupling the system to a network of servers and workstations, it is possible to collect, store, and disseminate an unlimited amount of useful information. Some examples are:

- Chemical usage.
- Water withdrawals / usage.
- Raw and finished water quality.
- Pressure and flow.
- Energy Consumption.

By manipulating this data through trending and comparison on a real-time basis, the utility gets the benefit of a more representative set of data. This information may then be used to formulate operational strategies to optimize processes and plan for upgrades and modifications. Operational parameters can be stored by placing the collected data into a "historian" server. Regulatory reports can then be generated automatically by populating spreadsheets from this database. The Orange County Utilities Water Production Section is currently utilizing these enhancements.

The Future

Someone once said, "If you can imagine it, you can do it!" How true. Given the fact that this system is compatible with most all types of intelligent transmission, it is easy to begin thinking in future terms. This SCADA network is not intended to merely transport simple commands and ship static data. A basic rule: "If you can do it on the Internet, then you can do it with ISDN/Frame Relay." The possibilities abound:

- Video – Monitor your remote facilities for increased security.
- Work Order Systems – Mobile Workforce Management.
- Maintenance Documents – Schematics, manuals, and drawings.
- Automatic Meter Reads – Forward to Customer Service.

Continued on page 47

Continued from page 40

- Interdepartmental Services – GIS, Collections, Reclamation, etc.

The addition of a hub to the router at each remote facility means that many different devices can be supported. For instance, a wireless Ethernet connection can be used to allow technicians to use a laptop computer over the SCADA network to access information such as drawings and work orders. These can reside on a specific O&M system server that acts as a central repository for all such information. An electronic O&M system has major advantages over the traditional paper system, even more so when instantly available to any employee at any facility.

The simple addition of a handset allows the transmission of voice directly over the network to the central site. This is known as "voice-over IP" and can effectively alleviate the radio snarl encountered by many utilities forced to share communications with other groups.

Data can be shared by different departments with such a system. A fundamental service may be the monitoring of lift stations or reuse pump systems close enough to be tied into the connected facility. Automatic Meter Reading systems may be wholly or partially fed into the system to transport the information across the network. There are many possibilities; specifics depend upon the particular needs of each utility.

Summary

The Orange County Utilities Water Production Section has greatly enhanced its ability to collect, compile, and disseminate information. The ability to view system parameters in real time has led to the development of new operational strategies and expedited process troubleshooting activities. The SCADA system has become more than a simple monitor and command system; it is now a productive utility management tool as well.

Utilities managers who wish to move in this direction should evaluate where they are now and where they want to be in the years ahead. By examining all necessary elements and with careful planning, they can install and configure a new digital network with little or no impact on current operations.

With a high-speed Frame Relay network integrated into the communications structure, the utility can progress in ways never possible with radio. In fact, SCADA may become just one of the services "sharing" the network. As technologies progress, it is safe to assume that ISDN/Frame Relay will be compatible for many years to come. Simply put, the next-generation SCADA system will resemble the traditional system only in the most basic of ways.

Utilities Security Seminar May 23

The Florida Section of the American Water Works Association will hold a free EPA/AWWA seminar on counter terrorism May 23 in Kissimmee. Titled "Counter Terrorism and Security in the Water Industry: A Manager's Guide to Keeping Your Utility Safe," the session will be held from 7:30 a.m.-5 p.m. in the Kissimmee Civic Center.

Space is limited to the first 80 registrants. A $10 lunch charge will be payable at the door by cash or check. The seminar is approved for six CEUs or six PDHs. For details contact Dave Prah at **PrahDJ@cdm.com** or 407-660-2552.