

# **BENEFITS OF USING WIRELESS ETHERNET COMMUNICATIONS IN EXISTING OR NEW MUNICIPAL SCADA SYSTEMS**

Victor KL Wong, P.Eng  
Chief Engineer, SCADA Systems  
Dayton & Knight Ltd.  
West Vancouver, BC, Canada  
[vklwong@dayton-knight.com](mailto:vklwong@dayton-knight.com)

Thomas Dunn  
Chief Technologist, SCADA Systems  
Dayton & Knight Ltd.  
West Vancouver, BC, Canada  
[tdunn@dayton-knight.com](mailto:tdunn@dayton-knight.com)

## **KEYWORDS**

Wireless Ethernet, Spread Spectrum, Frequency Hopping, Radio, Communications, SCADA

## **ABSTRACT**

With the implementation of appropriate security measures receiving full attention in the water supply industry, many municipalities are faced with the challenge of not only monitoring their facilities through SCADA, but adding remote video surveillance and datalogging for security at remote sites. Most municipalities today already have SCADA systems in place, but those using radio communications as the primary backbone are limited to small bandwidths of less than 9600 bps. This leaves Municipalities with only minimal bandwidth for datalogging retrieval and remote surveillance applications.

Recently there has been an explosion in wireless products available on the market that will allow municipalities to leverage their existing infrastructure and available resources. These wireless products are based on the Ethernet communications media that is the underlying core in most office networking environments.

This paper will review fundamental concepts of wireless Ethernet communication, design considerations for implementation into new and existing Municipal SCADA systems, benefits of using wireless Ethernet versus conventional radio systems, and its application with datalogging retrieval and video surveillance systems.

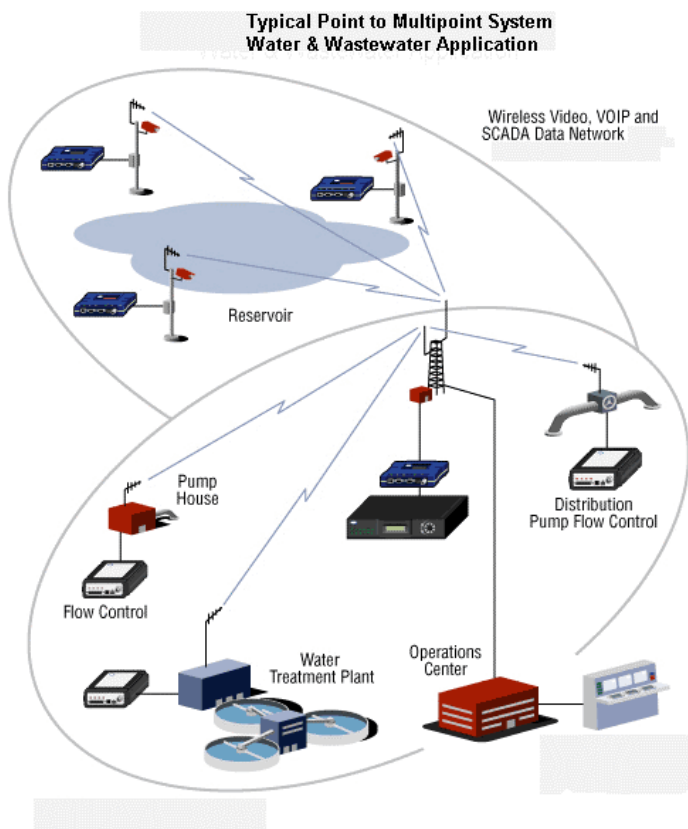
Also discussed is an actual case study on a successful design and implementation project using a wireless Ethernet SCADA system in a large municipality. The case study will examine integration into the Municipality's existing SCADA communications infrastructure, design criteria used, benefits realized, and future IT development potential.

## INTRODUCTION

In North America there are a large number of telemetry systems in use by various governments and municipalities operating distribution systems for fresh water, waste water, and storm water. In addition to these systems, managed traffic light control systems, security systems, irrigation systems, lane control systems, and vehicle location systems also utilize a combination of computer monitoring at central facilities and remote field devices (including RTU and PLC products). SCADA (Supervisory Control and Data Acquisition) systems have become very common among larger municipalities for monitoring remote water and sewer facilities. Even small towns now use basic remote telemetry devices to monitor alarms and provide call-out to operation personnel.

Wire line devices provided the communications between remote devices such as RTUs, PLCs, instrumentation systems, and the central monitoring services or on-call personnel. The communications devices such as data modems or auto-dial voice alarms were slow in communicating and provided a minimal number of data points that could be monitored and/or controlled. Advances in technology have improved the rates of communications, but still are limited to the amount of data that can be transmitted over telephone circuits.

The use of radio communications to move data from remote devices to a central computer has been an option since the early 1970's. Early radio communications used standard voice grade radios and data rates of 300 to 1200 bits per second. Radio frequencies were typically assigned in the VHF (136- 72 MHz.) or UHF (403-430 and 450-470 MHz.)



bands. In the early 1980's, data communication rates were moving to 2400 bits per second (bps) and soon reached 9600 bps using specially built data radios with internal modems.

Industry Canada or Federal Communications Commission (FCC) in the United States also designated the 900 MHz. bands for licensed communications of point to point data transmission and point to multipoint data transmission systems. The frequencies used were in the 928/952 MHz. and 932/941 MHz band. At the same time as communication equipment technology was changing, the RTU vendors (e.g. Bristol Babcock, Control Microsystems, Motorola, Fisher ROC, etc.) were developing newer versions of products that

could accept faster data rates that were becoming available. One of the disadvantages of faster data rates was the range between master and remote stations were reduced at the faster (9600 bps) data rates. To overcome this problem, RTU and radio vendors developed a technique called “store and forward” using custom protocols and hardware.

## **NEW COMMUNICATIONS SPECTRUM**

In the early 1990’s, a new radio frequency band located between 902 MHz. and 928 MHz. and a new modulation method became available and is known today as spread spectrum radio communications. Data rates in this new frequency band were typically operating around 19.2 kbps although 9.6 kbps was still used. At this time, RTU equipment were still operating through serial communications RS-232 data ports with a maximum speed of 57 kbps, and the limiting factors still reside with the data radio maximum throughputs.

The use of spread spectrum radio technology removed the requirement to license a frequency or pair of frequencies from Industry Canada (or Federal Communications Commission (FCC) in the United States) to the end user. The often-lengthy frequency coordination and assignment period from Industry Canada was no longer a barrier with the use of license-free spread spectrum products. Clients who once had significant delays in data communications on the licensed channels due to data traffic levels and number of remotes could now add additional remote stations without sacrificing system performance and reliability.

## **BENEFITS OF WIRELESS ETHERNET**

### **THE PROBLEM**

As the number of remote facilities in SCADA systems grew, so did the requirement to provide more information from the field for management systems analysis. Early RTU design incorporated 30 to 50 analog and digital points per remote location. Digital alarms were considered to be the most important data that was required at the central monitoring facility. Analog values were sampled periodically and transmitted back, but did not provide the resolution that local chart recorders incorporated due to bandwidth limitations. In order to provide the resolution of analog data necessary to support applications such as enhanced modeling of water and wastewater distribution systems, other means of providing more bandwidth were required.

With recent concerns about terrorism and the security of our water supply systems, now there was a need to enhance security for door and hatch entry alarming by adding video surveillance to better respond to potential threats to reservoirs and pumping stations. There is a need for more and faster information to be used by field personnel carrying notebook computers and handheld devices. These problems cannot be met without more bandwidth in SCADA system communications design.

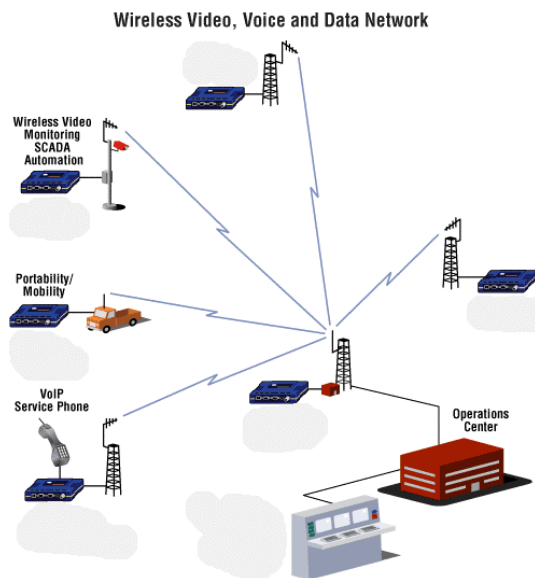
Within the office and factory floor, wired Ethernet networks operating at 10 and 100 mbps are common methods to move data between computers. Ethernet networks supply high bandwidth, data transmission using addressable packets of information to route data between locations, which are connected via network cable. This technology has been in existence for more than 30 years, but did not easily support long distance cable runs that would be necessary for field RTU use. Fibre-Optic cables can be used to move data over longer distances, but the costs are still too high for the amount of data that a SCADA system would typically transmit.

## **THE SOLUTIONS**

What the industry needed were more requirements to move data from remote locations to a central monitoring facility and to develop an Ethernet network environment that used radio instead of cable to provide network connectivity for field RTU locations. Recent announcements from several communications vendors have demonstrated Ethernet networks from 115 kbps up to 100 kbps using spread spectrum radios and the 900, 2400, and 5800 MHz. radio bands. Now industry can provide the enhanced bandwidth to address some of the new requirements that provide cost effective management of remote systems.

The new wireless Ethernet networks systems are both scalable and flexible ensuring network growth in any organization. This protects investments and provides lasting value. The solutions also provide easy-to-deploy and easy-to-manage networks that allow remote management and control of network devices to reduce the overall management and servicing costs. For SCADA systems, radio products for the 900 MHz band and data rates from 115 to 512 kbps are the most cost effective to utilize.

## **WIRELESS ETHERNET AND SITE SECURITY**



The use of wireless Ethernet in municipal applications opens up new possibilities for integrating data, voice and video into one single network. Applications could include a combination of traditional SCADA/telemetry services, remote video and surveillance monitoring, and emergency voice services while leveraging existing infrastructures. These applications are possible because of the larger bandwidths a wireless Ethernet system could provide over conventional radio systems.

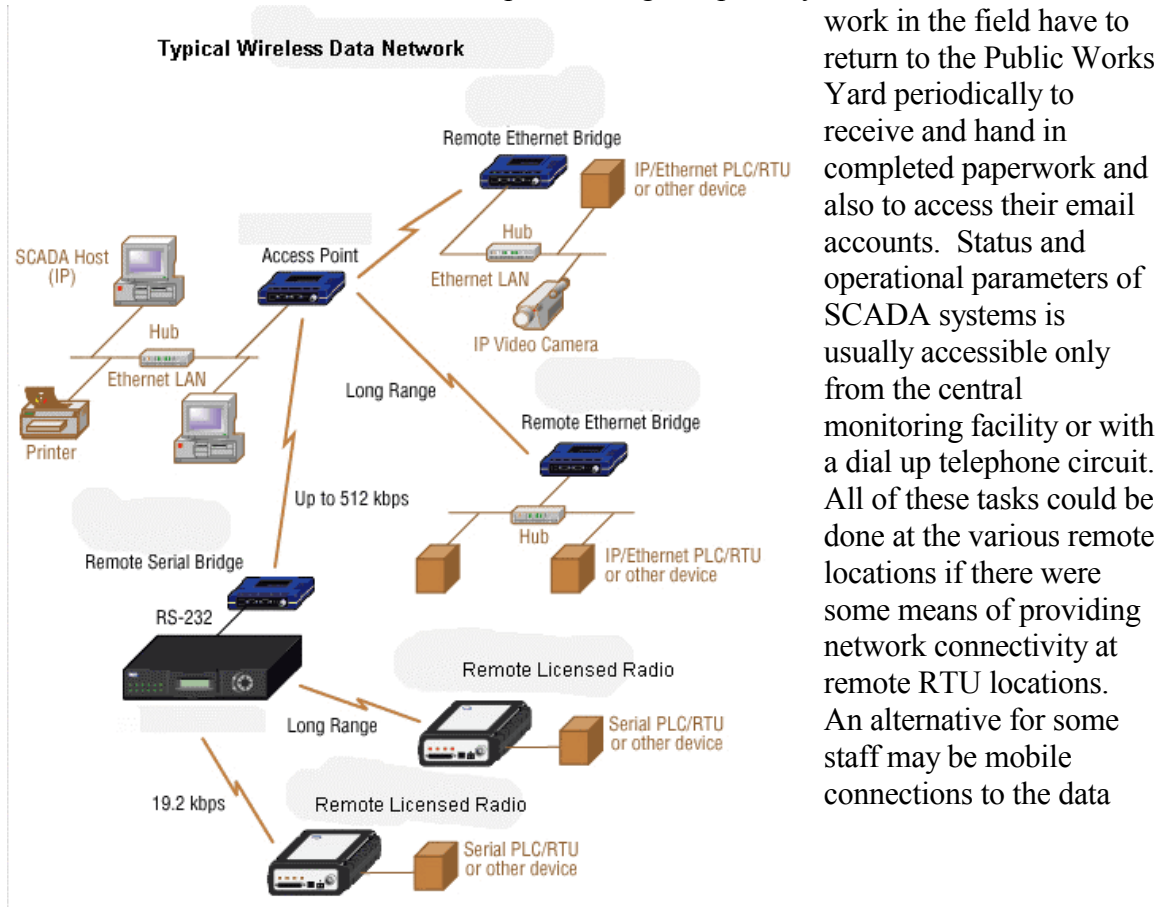
The ability to now view and record the unlawful activities while it is happening in a remote facility is critical. Many municipal agencies have re-assessed its security readiness and are now installing new or upgraded security and/or surveillance systems including wireless video to help enhance the security system. This is a first step in mitigating damage to a water supply system.

Because of its large bandwidth characteristics wireless Ethernet systems could also piggyback voice data over the radio network using a technology known as VOIP (voice over IP). This provides a cost-effective alternative to a traditional telephone network in municipal systems where traditional services are not available, or a temporary voice connection is required. Examples of this may be at water reservoirs or watersheds.

### WIRELESS ETHERNET AND DATA

To add resolution to analog data such as pressure, level, flow, pump run duration, and chlorine residuals, data can now be logged on site in the RTU's memory as frequently as once every second and these time stamped data log files now need to be sent back to the HMI (Human Machine Interface) computers over the same communications channels as the regular polling and report by exception data traffic.

The administration of municipal government and its employees have resulted in internal email for its staff and some of the manual processes such as work orders and maintenance schedules could now be issued and completed using computer systems. Personnel that



work in the field have to return to the Public Works Yard periodically to receive and hand in completed paperwork and also to access their email accounts. Status and operational parameters of SCADA systems is usually accessible only from the central monitoring facility or with a dial up telephone circuit. All of these tasks could be done at the various remote locations if there were some means of providing network connectivity at remote RTU locations. An alternative for some staff may be mobile connections to the data

cellular networks (e.g. Telus 1x data services, or Verizon in the United States), but this has a capital and a monthly cost associated with it.

One of the most exciting trends in wireless communication today involves the transmission of IP (Internet Packets) and industrial protocols over wireless Ethernet devices. Wireless Ethernet solutions provide the following benefits:

- Interoperability between hardware and software components;
- Reliability to perform in rugged conditions resulting in less downtime and fewer repairs;
- Scalability allows the reuse of existing networks thereby providing backward and future compatibility;
- Easy of use due to standards-based on Network Management System (NMS) allowing lower system maintenance costs;
- Multiple users and applications could all running on the same infrastructure;
- Secure solutions for wireless data, voice and video applications; and
- Easily deployable.

Wireless Ethernet network hardware solutions in the field at RTU locations have been recently announced (within the last year) from several vendors of radio and RTU products. Using a terminal or device server adapter, it is possible to make physical connections between a network and network capable radio modem and a serial port on an RTU, but this represented an additional cost in dollars and programming time. The announcement from several RTU vendors indicating product or products that now contain an RJ-45 Ethernet 10BASE-T communications port in addition to several RS-232 serial ports allows greater flexibility in the current design of conventional RTU SCADA systems and in future a new Ethernet based communications systems.

At the same time as some RTU vendors were incorporating network interfaces RTU products, the communication vendors had announced new lines of radio based products in the 902-928 MHz. and 2.4 GHz. bands utilizing license-free spread spectrum radios with data throughput from 115 kbps to 512 kbps. While data throughput rates are still below the 10 mbps rates supplied by wired Ethernet 10BASE-T systems, it represented a 10 to 40 fold improvement over what had been previously available in data radio communication systems. The new radio modem devices will now co-exist with existing equipment manufactured for these radio bands.

## **WIRELESS ETHERNET AND DATA SECURITY**



Spread spectrum technology is a method of taking data, which might normally be sent as one message on a single frequency and breaking it up into small packets (a series of bits containing data, control, and source and destination addresses information). These packets are then sent over many frequencies in the band. The most prevalent method

of using multiple frequencies is by hopping from one frequency to another every fraction of a second until the message is fully transmitted. Another method of transmission is called direct sequence, which transmits over the entire band at the same time. The spread spectrum techniques were first developed by Ms. Hedy Lamarr (famous actress during the 1930s) during the Second World War to prevent unauthorized interception of messages. While the military have been using spread spectrum in their bands for the past 60 years, commercial use of this technology has only become available in the last ten years.

This technology adds several layers of security to the transmission of information over a wireless circuit. In order to successfully intercept or send a data message, the interceptor would have to have the ability to discover the following information.

- The make and model of the radio equipment;
- The pseudo-random sequence of the hopping pattern;
- The system code word for the device;
- IP addresses assigned to each remote site and host site; and
- Any other security layer information such as VPN.

As all wireless data networks offer the opportunity for data interception and insertion, it is impossible to achieve and guarantee absolute security in a wireless or even a wired network. By providing layers of security to the wireless Ethernet network will minimize those risks.

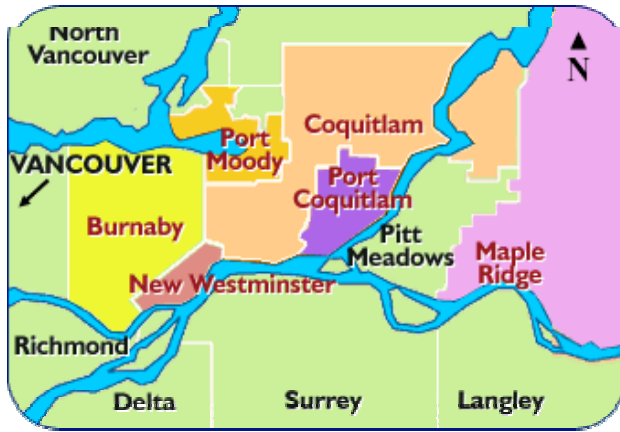
Adding several layers to the wireless Ethernet networks also provide the following protection:

- Accessing of data transmission using wireless packet sniffers
- Interception and insertion of wireless information
- Unauthorized/unauthenticated devices from joining the wireless network
- Denial of Service (DoS) attacks
- MAC IP spoofing
- Network Topology Discovery

The following case study best shows an example for the design of a SCADA system upgrade for the City of Coquitlam, which started in the Fall of 2001 and has just recently been commissioned.

## CASE STUDY – CITY OF COQUITLAM, BC, CANADA

The City of Coquitlam located in southwestern British Columbia near Vancouver, BC is



approx. 12, 934 Hectares (8.17 sq. miles) in area and has a population of 112,890 (2001 census). It is approx. 23 Km. in length from east to west and 20 Km. in length from northeast to southwest. The Operations group is responsible for 500 Km. of water mains, 400 Km. of sanitary mains and 450 Km. of drainage

The City of Coquitlam has operated their water and sewer distribution

systems using RTU's and radios since 1991. Original RTU equipment consisted of a Motorola Intrac unit that provided basic control and monitoring and was connected to an 800 MHz. trunking system operating at data rates of 600 bps that was operated by one of the major communications carriers.

The central monitoring facility in was running a DOS based HMI software package. After a six month trial, it was determined that the trunking radios introduced too long a delay in granting permission to transmit during peak periods and a new 928/952 MHz. frequency was required from Industry Canada. Upon receiving this new frequency, the old trunking radios were then exchanged for new ones to support a communications channel in the 928/952 MHz. bands.



Over several years, the number of remote SCADA facilities grew to approximately 30 and included water reservoirs, pump stations, flow monitoring stations, and 14 sewer lift stations. This system operated until 1997 when the City re-evaluated its telemetry system requirements. The evaluation indicated that an upgrade to a more intelligent RTU device was required. The intelligent RTU would provide local RTU programming, better analog resolution needed for historical collection and trending, faster data rates, dynamic store and forward routing of data, and better control strategy implementation between reservoirs and various pressure zones.

The decision to upgrade the HMI software package from a DOS-based to a Microsoft Windows-based system was also completed. After tendering, an Intelligent RTU vendor

was selected. The RTU required a third party radio to operate in a simplex 900 MHz. system running at 2400 bps instead of the duplex frequency system that was in use at that time. The RTU vendor also supplied a customize HMI software package. Due to the technical difficulties with the RTU vendor experienced by both the contractor and the client, the RTU vendor's product was abandoned in the 2001 SCADA expansion project.

The 2001 expansion included 7 flow monitoring stations, 10 sewer lift stations, 5 methane blower stations and 23 grinder pump stations. During this expansion, Dayton & Knight Ltd. (the consultant) recommended that no further sites be implemented using the existing RTU product. A subsequent technical evaluation was conducted to determine which RTU option met the specified design criteria required for future expansion. In order to retain the capital investment in what was relatively new RTU and radio equipment, it was recommended that the existing equipment be retained utilizing the client's existing licensed frequencies (928 and 952 MHz).

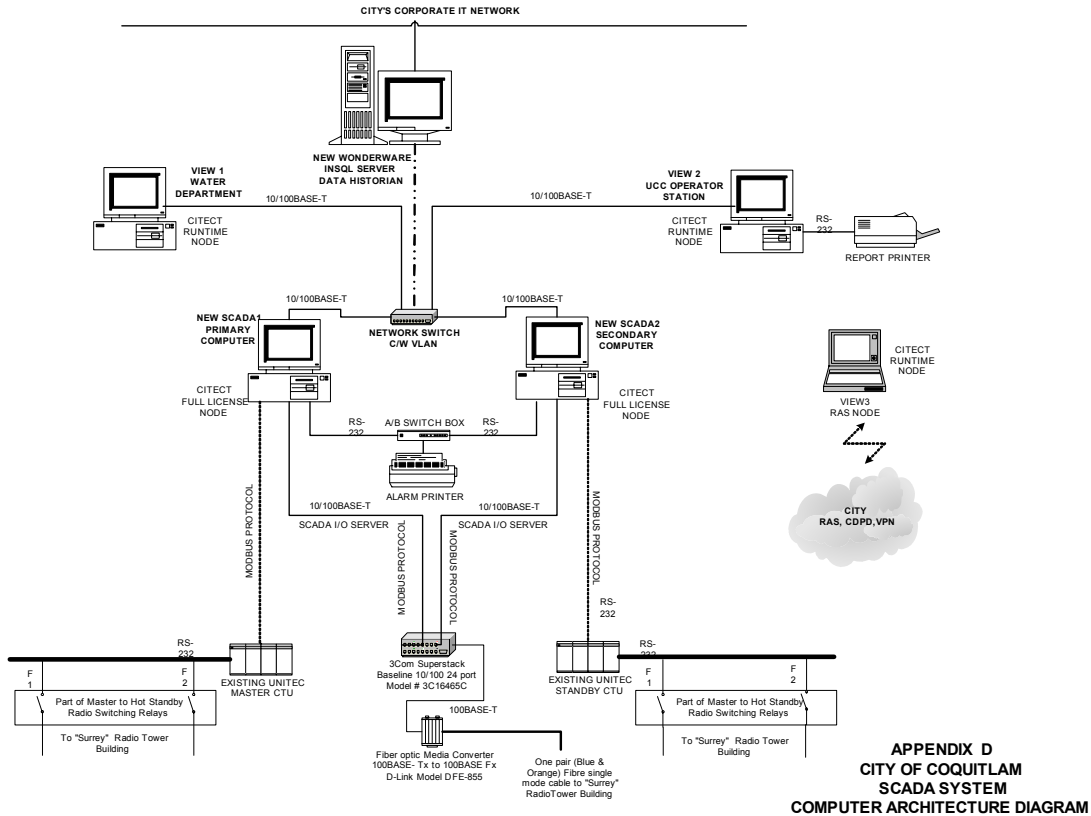
This necessitated evaluating other communications methods, as vendors did not recommend mixing protocols on the same RF channel. Fibre optic cable, a second licensed frequency, a license free spread spectrum channel, and cellular digital packet data (CDPD) were evaluated for communications systems on the new expansion. Initial discussions with Industry Canada were not successful in obtaining a second 928/952 Mhz. frequency pair. The City's fibre optic cable installation program had not yet matured to provide fibre to most RTU locations. Cellular packet CDPD services were considered to have too high an operating cost. Therefore it was recommended that the City consider a license-free spread spectrum solution for all new stations with the possible upgrade of the current communications system at a future date.

The process of gathering information on all new locations including latitude and longitude by GPS receiver, plus site inspections for near field obstructions and potential store and forward sites. Because propagation to the master station at the City's Utility Control Centre (UCC) was already known for a number of existing stations, theoretical path loss studies on all new and some original stations and were checked against known signal levels and fade margins at those original sites.

Seven new stations that were identified could not get a clear shot to the master radio site, consequently a bucket truck and RF service monitor was used to test each of the remote sites empirically including noise floors. At this stage, our design criteria for RTU and radio provided only serial connection to 19.2 kbps spread spectrum radio system. Radio sensitivity on this radio was very close to licensed products operating at 9600 bps. After completing the radio tests, two vendors, one an RTU vendor (Control Microsystems) and the other a radio vendor (Microwave Data Systems) announced new products that added Ethernet capability to their product lines.

The Control Microsystems products had been short listed because of their ability to do provide data logging functionality, which made them ideal for use at the 7 flow monitoring stations. The new products announced by Microwave Data Systems increased the data throughput of the spread spectrum product line from 19.2 kbps to either 256 kbps or 512

kpbs. As bandwidth requirement was a very important criterion, these products were specified after recalculation of fade margins and path losses for the new radio product conducted and verified. Two new store and forward (access points) locations were established to accommodate poor paths from 5 of 7 PRV sites and 4 sewer lift stations back to the UCC. Also identified were 20 sites with minimal I/O data points that would receive spread spectrum instrumentation loops instead of full RTU devices. Three RTU devices were installed in an industrial park area and communicated only three digital alarms (high level, power fail, and comm. fail) at each of 20 sites back to the three full RTU sites.



Major concerns found in the design phase of this project were lack of direct line of sight due to City's mountainous terrains and extensive foliage losses (trees were primarily of the evergreen type and 20 to 20 metres in height). In addition, homes were built in close proximity to sewer lift stations that blocked direct line of sight for some remote SCADA stations. Some of these problems were overcome by placing antenna support structures at more than 50 feet away from where radios and RTUs were located.



The City of Coquitlam had already started their video surveillance program using other wireless radio products before the new wireless Ethernet data network was proposed. However, some future use of video data on this new network is possible within the bandwidth limits. The future use of this network for remote access to email, and other operating paperwork will be evaluated once there are more water and sewer sites from the old system moved to the new Ethernet data system. It is anticipated that more store and forward repeater sites will be required when this expansion is slated to start. Access point radios will be integrated with new fibre optic cables to be installed in the next 2 to 5 years as part of a hybrid system. This client has already noted the improved data response time for alarms and analog information.

### **RECOMMENDATIONS FOR SUCCESSFUL IMPLEMENTATION**

1. Test components and download configurations in the shop before installation in the field;
2. Provide section in Tender electrical specifications that forces contractor to sweep antenna systems and produce graphs before system is accepted. This will add cost to tender but establish contractor responsibilities;
3. Stay away from Electrical Utility (BC Hydro) pole installations of RF antenna systems if possible. It can be done but it takes a long time to co-ordinate, and costs a lot if you want to be up above 30 feet and primary wires. Yearly service fees will be charged and Electrical Utility must install the antenna systems in some cases;
4. Try to get residents to buy into importance of radio system. Accommodating their visual concerns may produce poor RF paths to central monitoring facilities;
5. Be prepared to design more store and forward locations if situations warrant;
6. Vendors must provide more training on product to field integration staff;
7. Industry needs to move to single store and forward radio products not two separate radios. Microwave Data Systems is planning for this in future product releases; and,
8. If you plan on integrating serial legacy products into IP Ethernet radio products, then expect to require additional test equipment for field troubleshooting.