Utilization of SCADA Communication Networks for Video Surveillance by Water Companies

Donald A. Simoneau

Abstract

Our nation’s water supply distribution network comprises hundreds of thousands of miles of pipes, with a corresponding number of above-ground facilities. Since 9/11/2001, various agencies and associations involved with these vital systems have recognized the need to provide a much higher level of protection against sabotage and attack.

Only a fraction of water supply facilities use security measures beyond locked doors and fencing. Operators of these vital systems have identified video surveillance as a key method for improving security and reducing vulnerability. Until now, adding video surveillance to remote facilities required a new, separate, and expensive communications network to incorporate available technology.

This paper will outline a new technological development that allows the transmission of video images utilizing low bandwidth networks. Unlike traditional stand-alone security systems that use closed-circuit or broadband networks for video transmission, this technology enables the use of existing low-bandwidth communications to transmit video and integrates with existing supervisory control systems.

Water System Computing Environment

Typically, wells, tanks, reservoirs, pumping stations, and associated infrastructure are automatically and remotely monitored and controlled by small, rugged programmable logic controllers located at the remote facility. These programmable logic controllers (PLC’s) are tied back to a central control room (usually a pump station or water treatment facility) using low-speed communications such as licensed wireless radios or leased telephone lines. The data retrieved from the PLC’s are then managed, displayed, and stored by supervisory control and data acquisition systems (SCADA).

When these remote PLC’s have “security” systems added to them, they almost always consist of simple switches that can detect motion or the opening of a door, window or gate. This configuration leads to several problems:

- Wind, trees, animals or other natural events, may cause a false alarm. These devices cannot distinguish between a false alarm and an actual intrusion.

- This method provides much too limited “real time” information about an event. A delay of hours, even days, could occur between the event and the ability to properly characterize the event.

Once an intrusion event has been identified, the operator must definitively identify the nature of the threat or risk system-wide contamination. Detailed and time-consuming analysis must be made requiring visits to remote facilities to guarantee the safety of the water supply. Video surveillance is widely recognized as the best tool to accelerate the
determination of whether an intrusion is harmless or one that warrants additional response action.

In some security installations, a digital video recorder (DVR) and cameras are used to monitor remote premises. These units store days of video on a disk drive for later review. They are generally not connected back to a central station because the bandwidth required is not available at the remote site. Fiber optic cables, leased T1 lines, or a DSL line are too expensive for the water company to afford. If an intrusion occurs, this video can be examined to see if the event was real (for example, not an animal) and if so, to help identify the perpetrator. The main shortcoming of this application is the delay in hours or days that may occur before the video is reviewed.

Water treatment facilities are often manned facilities allowing for monitoring and control of the entire system. Located closer to roads, telephone and broadband lines, and clean power, these facilities can support more data gathering and processing. In a typical configuration, a “master” PLC is used to periodically collect and send information from the multitude of “slave” PLC’s located at the wells, pumping stations, water storage and other remote facilities. Information from the central station can be transmitted via high-speed paths (e.g. broadband cable, DSL) to other users such as weekend-on-call technicians, police and fire dispatchers, etc.

Remote Facilities

Water distribution facilities (pumps, wells, holding tanks) are frequently located in remote locations, far from high-speed and economical communications networks. Until now, adding video surveillance to these remote facilities required a new, separate, and expensive communications network to incorporate currently available technology. Currently available video surveillance systems have been developed for applications where high bandwidth communications are available, even to remote facilities. In current security parlance, a remote site is simply a different building, but still highly accessible.

Video surveillance systems that claim to use “low bandwidth” connections cater to dial-up connections, which are rarely available at remote water supply facilities. In addition they offer a severely reduced set of features and limited integration capability into existing water monitoring, control, and notification systems.

Longwatch

The Longwatch Surveillance System was specifically designed to the security requirements of water systems that utilize SCADA systems. The system provides motion video over communication lines that already exist in thousands of remote water treatment sites.

The system:

- Enables a path for video data where one currently doesn’t exist
- Provides video data over the existing secure and reliable communication systems
• Eliminates the capital investment and incremental monthly access charges associated with implementing high-speed communications

• Avoids the difficulties that exist when using cell phone, telephone or cable across service boundaries

**Product & Technology**

A Longwatch system requires the following:

• Cameras and intrusion detection equipment (and respective enclosures if necessary)

• One or more Remote Video Engines (RVE) depending on the number of cameras being used and the number of remote sites being monitored

• One Video Control Center (VCC) and a network infrastructure (either wired and/or wireless.)

**Remote Video Engine (RVE)**

The Remote Video Engine (RVE) is a pre-packaged general purpose computer with a built-in video interface. The RVE can accept up to four camera inputs in either black and white or color and is equipped with four digital contact inputs that can be connected to items such as proximity switches, glass break detectors, motion detectors, etc. The software is pre-loaded on the hard drive in the RVE and operates under a pre-configured, Microsoft Windows XP Embedded (XPe) operating system. A simple configuration program is provided to the user to adjust (if needed) various operating parameters of the program. In addition to the security inputs to the RVE, the RVE has a bidirectional RS-232/RS-485 serial port (for connection to the programmable controller) and an Ethernet port (that can be used for local configuration of the RVE with a web browser, or for connection to broadband modems (when the RVE is used in a mixed-transmission system.)

The protocol generator is designed to work with Rockwell’s Allen-Bradley DF1, Group Schneider’s Modbus/RTU & Modbus/ASCII, TCP, UDP, and SIO. SIO is the native Longwatch Serial Protocol for use on dedicated serial networks.

If the network is temporarily unavailable to the RVE, video images are archived in the RVE on its local hard drive. When the network becomes available, the RVE automatically updates the Video Control Center with the archived images. Video compression is the key to the RVE application. A typical low-resolution color image of 160 by 120 requires 19,200 pixels. Each pixel is represented in the digital camera image by three 8-bit bytes. Therefore, 57,600 bytes or 460,800 bits are used to represent the picture. Using traditional communications of 9600 baud (960 bytes per second), it would take 60 seconds to transmit the image. Using state of the art compression, the first image transmitted by Longwatch contains 1400 bytes, representing a 97.6% reduction in size. Transmission time for this image is only 1.5 seconds. Subsequent images, that undergo minor changes, require only 200-400 bytes.

In addition to video compression, a key element of the RVE is its ability to use the existing supervisory control communications system present in the water facility. In the
case of the Allen-Bradley DF1 protocol, for example, it accomplishes this by using a “pass through” protocol available in the programmable logic controller (PLC.)

In typical applications the RVE shares the existing communication link with a local programmable controller (PLC) over a serial (RS-232 or RS-485) communications line. This local PLC is existing equipment and used for local supervisory control and monitoring of the water production equipment. The local PLC communicates to a master programmable controller at the main control and monitoring facility of the water supplier. This communication is performed over an existing connection consisting of either a wireless radio or a telephone line.

Additional features:

1. Transmission speeds and compression factors are user-configurable at each Remote Video Engine. This enables the user to “fine-tune” system performance.

2. The response rate and performance of each RVE is a function of the communications line provided. For example, if a 19.2K baud line is provided, performance will be twice that of a 9600 baud line.

The RVE is scalable and able to use broadband connections in addition to serial connections. In some cases a water supplier may have a resource (e.g. a well, storage tank or treatment facility) located near a subdivision or other area that has broadband cable or DSL available. Rather than connect via radio or low-speed telephone, the operator may elect to connect that resource’s RVE via the high-speed network using TCP or UDP protocol. Performance will increase accordingly. At the Video Control Center, all images and alarms are presented and processed in a similar way for ease of operation.

Remote Video Engine modes:

- **Alarm video clip mode**
  When an alarm event occurs (detected either by an event contact closure or image analysis trigger) the system captures a short segment of motion video from each camera attached to that RVE (typically two frames a second for about 15 seconds) for the period just before the event to just after the event. These images are then sent over the network to the Video Control Center for viewing and forwarding to designated cell phones.

- **Live-video mode**
  Low frame rate, low resolution video can be provided either continuously or ‘on-demand’ for specific cameras. Frame rates and quality can be adjusted based on available bandwidth.

- **Continuous local recording**
  The RVE acts like a digital video recorder (DVR) and continuously records high resolution video images from each of the attached cameras. This recorded video may be retrieved locally by transfer to a laptop computer or a commercially-available USB disk drive in the event that high resolution video is needed for investigation and prosecution of vandals.
- **Guard Tour mode**
  In order to enable the system operator to view all cameras on one scrolling system overview screen, each RVE can send pictures from all cameras at a user-defined ‘background’ frequency.

The following illustration depicts a typical system deployment. The items shown in gray are supplied by Longwatch; all other items are pre-existing parts of the water system.

**Typical System Deployment**

Any number of remote (field) facilities are tied together with a private, low-speed network (in the diagram, this is a radio network.) Usually, one Remote Video Engine (RVE) will be installed at each field facility, and can support between 1 and 4 cameras. If the field facility has doors, windows or gates, smoke detectors, additional alarm contacts can be wired to the RVE to trigger “alarm video monitoring” if a switch trip occurs.

**Video Control Center (VCC)**

The “base operations” facility is typically located at a main water treatment plant and has a central control room. It is at the base operations facility that the Video Control Center (VCC) is installed. The VCC is a software application and can be installed on an existing Windows XP computer (often, there are multiple computers being used for SCADA purposes).
The VCC provides an alarm summary display application that presents video in customary monitoring system formats. It also provides an integrated industry standard database to maintain all alarms and video files, tools for overall system management, and an application software bridge that enables alarm, configuration and video integration with the SCADA system. The video can be viewed through any standard internet browser, or a video-capable cell phone, as long as personnel have access to the water department’s secure intranet enabling accurate and timely response to field events at any time of day or night. Easy access to remote video helps reduce or eliminate resource-consuming emergency response visits to remote field facilities.

**System Block Diagram**

- Event detection (contact closure) senses door/gate opening, etc.
- Image analyzer checks for suspicious motion in video
- Image scanner multiplexes up to four cameras per RVE
- System watchdog checks for availability of network. If unavailable, video stored in local archive.
- Alarm video recorder takes short, higher-resolution movie clips if an event is detected
- Protocol encoder enables compressed video to be transmitted over existing networks

The Longwatch Surveillance System is built to industry hardware and software standards including Web Windows XP/Embedded, Microsoft DirectX/DirectShow, MS Media Player, ActiveX and OPC interfaces.
About Longwatch

Longwatch was founded by a team of industry veterans with the goal of providing video over existing SCADA communication networks. The result was the development of the Longwatch Video Surveillance System. Advanced technology incorporated in the system allows SCADA system operators the ability to utilize video to monitor and verify alarms at remote sites utilizing the existing communications infrastructure. The system gives operators the ability to manage video alarms and control system alarms on the same system.

Longwatch
520 Providence Highway
Norwood, MA 02062
1-781-255-7400
info@longwatch.com
www.longwatch.com