Environment, Communication,

A short guide to remote telemetry monitoring & control

By Grant Van Hemert

Water and wastewater utilities have a number of remote locations. Among these are pump stations, towers, valve boxes, sampling stations and septage systems. When automating these remote locations, three terms that may be confusing, but have direct ramifications on the reliability and longevity of the system, come up quickly: supervisory control and data acquisition (SCADA), programmable logic controller (PLC), and programmable automation controller (PAC).

Proper Terminology

SCADA is a term that often is misunderstood in water and wastewater. For many in the industry, it is limited to control and monitoring of remote applications. The term in its real definition is synonymous with the water and wastewater utility control system as a whole. This includes the communication with and control of the remote locations, as well as the main plant system. These systems are composed of SCADA software connected to either PLC/PACs or remote telemetry units (RTUs).

SCADA software comprises the interface mechanism between machine and human. This software is critical not only for control of the main facility, but in regard to the remote system. One of the other aspects is the ability to log events and generate alarms. All of this requires a timestamp, which will be discussed later in this article.

The PAC is an evolution from the PLC and includes some enhanced programming capability and Web services. PLCs and PACs are designed for plant and machine control, and are known for high-speed and reliability. These controllers have a presence in remote applications and often perform well. Remote control, however, is different from what occurs inside a facility. Thus, it can be argued that PLCs and PACs are not designed for remote applications.

Because of this, a different type of controller is designed for remote applications: an RTU. The main differences between an RTU and a PLC or PAC come down to three different areas: environment, communication and power.

A facility often has buildings and electrical rooms that might be isolated from the main process and usually are air conditioned. At remote facilities, however, the control panels often are outside and exposed to extreme temperatures and hazardous gases.

To address this, an RTU will have a higher temperature range than a PLC or PAC. The range should be 40°C to 70°C at minimum. An RTU also will have a conformal coating to help protect the unit from corrosive gases such as hydrogen sulfide.

In many cases, the RTU will be placed in a location that could be exposed to hazardous gases such as methane. Thus, the RTU should be suitable for Class 1, Division 2 Groups A to D, and be certified to UL Standard 1604 for U.S. locations, CSA Standard C22.2 Number C213-M1987 for Canadian locations, and also hold ATEX II 3G and IECEx certifications.

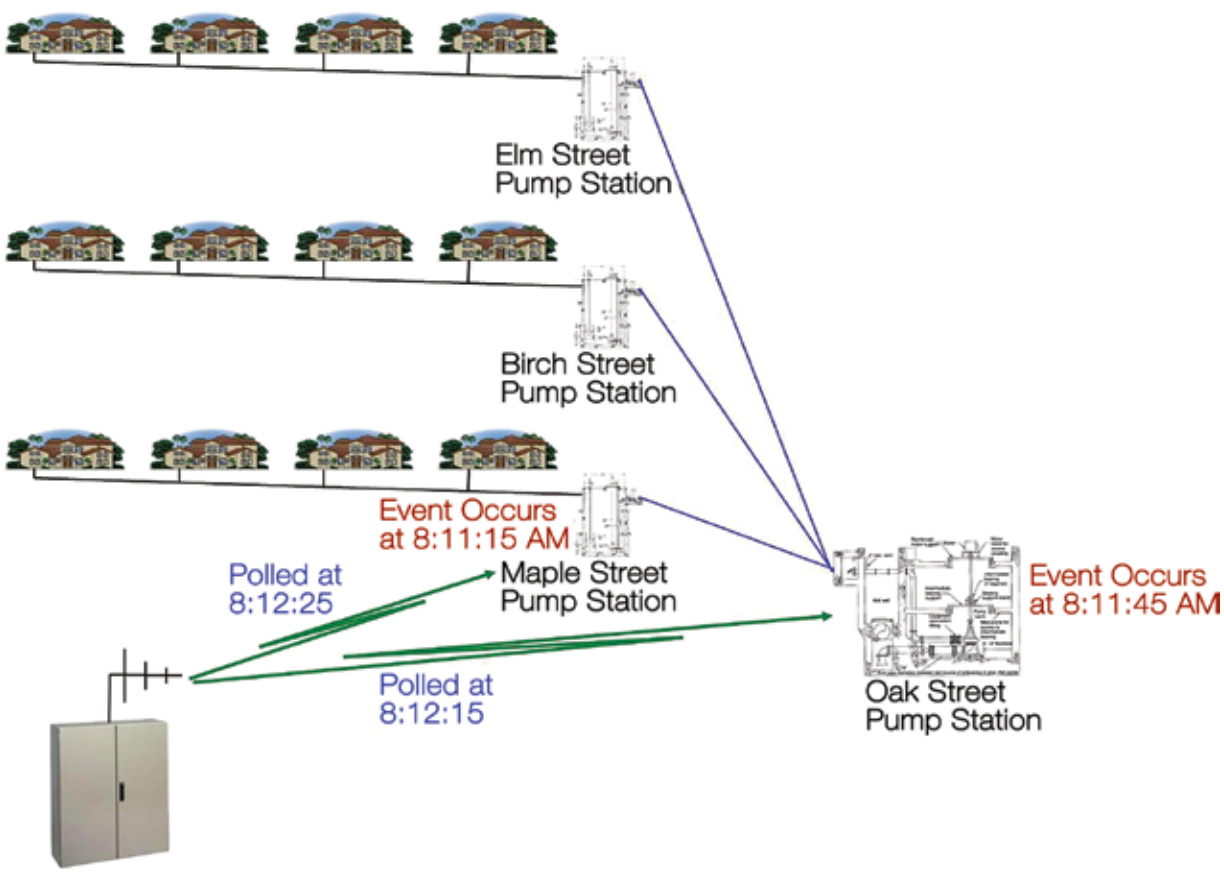
Communication Protocols

Communication to an RTU is different than to a plant-based PLC or PAC. In a plant, communication typically happens over a physical connection such as a wired cable or fiber optic cable. This wired technology is reliable, and many protocols were created for this environment. An RTU, however, is different. In this environment, the communication occurs over radio link, leased phone lines, cable modems, and public bandwidth such as global system for mobile communication (GSM) or general packet radio service (GPRS). This means that data transmission can be delayed or even interrupted and that a communication protocol for remote locations must be used to accommodate these differences.

Communication protocols come in three basic types. The first is a polled system in which a range of values is requested and sent back to the master. This is the method used when a customer employs Modbus or Modbus TCP. The second protocol features a master station that subscribes to data from the RTU, and only requested information is sent back. This method is used by a variety of protocols, such as EtherNet/IP and DeviceNet. Both of these protocols work well within a typical treatment facility where a physical connection exists. The third protocol uses both polled and unsolicited messaging back to the master station; an example of this third protocol is known as the DNP3. It can solve five challenges unique to remote communications.

The first challenge involves timestamping events when they are generated. The first two protocols assign a timestamp when the data enter the SCADA system. Due to the high data rate inside a plant, there is little chance of a discrepancy between what is registered in the SCADA software and the real event. In remote communication, however, this becomes a real possibility due to the time lapse between polls. Figure 1 depicts two interlinked stations. An event occurs at the Maple Street Pump Station; then a resulting event occurs at the Oak Street Pump Station. The master RTU station, however, polls Oak Street first, then 10 seconds later

Figure 1. Sequence of Events Misalignment



polls Maple Street. The result is that the events are polled in the opposite order from which they occurred. If one relied on a SCADA system to assign the timestamp, the events would be logged in reverse order. DNP3 generates the timestamp at the RTU; thus, the true sequence is preserved regardless of when the polling occurs.

The second challenge arises from the fact that data retention occurs during a communication loss. The first two protocol types were designed for hard-wired systems. Therefore, upon a communication loss, they simply stop working. Upon restoration, any events that occurred are lost. With DNP3, the events are stored with their timestamp inside the RTU. When communication is restored, a log of data is sent back to the master station, facilitating zero data loss. Because the timestamp exists on each data point, the event sequence also is preserved.

The third challenge that DNP3 solves is having the ability to optimize packet size by only sending the data that have changed since the last transmission. This preserves the data resolution without intensive system polling. This is critical when dial-up, GSM, GPRS or satellite is used. Not only does it decrease bandwidth, but it also minimizes the amount of data for which a utility is charged.

The fourth challenge is having the ability to change programs and firmware over the wireless network. Traditional networks assume that a technical staff member will be near the controller for firmware changes. In regard to program changes, they assume that the network will be at a high bandwidth, and changes can be handled easily. In a remote application, the network may be slower, and any changes need to accommodate that. By allowing remote changes and firmware uploading, DNP3 eliminates the need to visit the remote site for updates.

The final challenge is cyber security. There has been a lot of attention on this topic lately, and most water and wastewater facilities are either implementing or developing a cyber security program. The traditional networks are relatively secure because they are based on a physical connection. The main threat to these networks arises from the Internet and data sticks present in computers attached to the network. When dealing with remote systems that transmit over the airwaves, however, a physical connection does not exist and an additional threat is introduced: a person using the airwaves to monitor communications or take control of a lift station. To prevent this, DNP3 can have secure authentication and encryption capabilities embedded. Authentication prevents a faux master from controlling the network, and encryption prevents unauthorized users from accessing information.

The Power Factor

Power addresses both the actual wattage used as well as the voltage used. In most treatment plant control systems, 120VAC or 24VDC is available. Most water and wastewater locations have 120VAC as a control voltage derived from the 480VAC used to run motors. However, this may not be available in some installations, in which case it might be easier to use a solar panel to power the control panel. An example would be an RTU on a water tower that is only monitoring tower level. Unlike an RTU, most PLCs or PACs use too much power for solar applications—12VDC is more common in these applications because it is the voltage used in most batteries. PAC or PLC systems require 24VDC or 120VAC for their input and outputs. An RTU has a range of 12VDC inputs and outputs available.

A lot of confusion exists between the terms SCADA, PLC and RTU. Nevertheless, a deeper look reveals that these are not the same terms, but three distinct technologies that are designed to work in concert. WWD

Grant Van Hemert, P.E., is a product manager with Schneider Electric's Remote Terminal Units. Hemert can be reached at grant.vanhemert@schneider-electric.com or 919.217.6367.

For more information, write in 1105 on this issue's reader service form on page 41.

Write in 111

Write in 112