TELEMETRY AND WIRELESS COMMUNICATIONS AT STATIONS CONSIDERATIONS FOR TELEMETRY

Mike Pugh
Technical Specialist
Intermountain Gas Company

Introduction

Supervisory Control and Data Acquisition (SCADA) is a system architecture that employs computers, communications equipment, and peripheral devices to interface the outside world with the digital world. Often, the word telemetry is used in place of SCADA. Telemetry is a broad term defined as “any device for recording or measuring a distant event and transmitting the data to a receiver or observer.” As such, a person could be used as telemetry. For the purposes of this presentation, the term SCADA will be used.

Purpose/Goal

One of the first considerations in pursuing the installation of a SCADA system is defining the purpose of the system. What are we trying to accomplish? Are there tasks that can or should be automated? Will this be a complete data acquisition and control system, or will it be used simply to collect data from the field? Who will need or want access to the system and/or the data collected? This is by no means a complete list of considerations. However, once questions like this are answered, the organization should have a better understanding of the goals. It is more important to know where we are heading than where we have been.

A complete SCADA system will incorporate at least some of the following items: a computer system to act as the central processing center, a communications system (such as a licensed radio system or a cellular system using a mobile private network), field devices such as remote terminal units (RTUs) or programmable logic controllers (PLCs), and measurement devices (such as pressure or temperature sensors). Not all systems will contain each of these items. The choices will depend on the decisions made at the beginning of the process.

Equipment

RTU/PLC/Flow Computer

The terms RTU and PLC are generally used interchangeably; though there are differences, they mostly do the same function. Their function is to interface the physical world with the digital world. This includes reading inputs such as pressure and temperature as well as controlling outputs such as relays and connected devices. RTUs and PLCs are generally less expensive and aim to appeal to a wider target in terms of functionality than flow computers.

Flow computers are specialized PLCs which have been purposely optimized to accurately measure gas flow using AGA standards. While these devices must be able to accept inputs such as pressure and temperature signals, they are generally more expensive that RTUs and PLCs. This makes them less than ideal for anything other than gas measurement calculations.

It is important to choose the correct device for the intended purpose. For example, XYZ Utility Co wants to monitor a regulator station that has two pressures. While a flow computer can certainly measure these two points, it would be considered excessive in terms of money and resources. The better option would be an RTU or PLC with sufficient inputs to accomplish the objective. In addition, it is recommended to select a device or family of devices that can fill the need for the entire system. While there may be some common functionality between manufacturers and types of devices, many RTUs, PLCs, and flow computers utilize a proprietary means of communication. Having too many different types of devices means the I.T. department has to manage each of those devices differently, thereby creating a more complicated system.

Transmitters

The decision regarding equipment is based on several considerations. Some of the considerations for pressure and temperature measurements include accuracy, output signals, temperature ranges, power requirements, features, and ease of use.

Higher accuracy units and those with additional features will command a higher price. For situations where accuracy is less of a concern, considerable sums of money can be saved by choosing more economical models. Another consideration with transmitters is the rated ambient temperature ranges. It does little good to save money with a pressure transmitter that has a lower range of 32°F if that unit is being installed where temperatures could reach -20°F in the winter months. However, if the transmitter is installed inside a climate-controlled facility, temperature range is less of a consideration.

Communications

Communications is a broad topic that can, for the purposes of SCADA, be narrowed down to two main areas: methods and protocols. Communication method refers to the way in which the data from the field makes its way back to the server. This can include, but is not limited to, licensed radio, license-free radio, cellular, landline, and cloud-based systems. Each of these systems has its advantages and disadvantages. The system chosen will depend on many factors not the least of which is data security. Other factors to consider include terrain, the availability or access to the Internet, the organization’s tolerance for risk, and capital versus operation and maintenance budget dollars. Machine to machine (or M2M) systems based on cellular technology have been gaining ground recently while landline-based systems have been falling out of favor.

Communication protocol refers to the format of the messages which contain the required data. One of the oldest and most common protocols is Modbus which was developed in 1979 by engineers at Modicon. There are many other protocols such as Distributed Network Protocol (DNP3), DF1, Foundation fieldbus, Process Field Bus (Profibus), and Highway Addressable Remote Transducer (HART). The use of HART has been on the rise due to the ability of the protocol to use existing 4-20 mA loops to superimpose a digital signal containing additional data. This eliminates the need to re-install sometimes hundreds of feet of wire in a plant setting.

Who needs the data?

Internal Customers

Among the group of people who may want or needs access to the data in the SCADA system is the Engineering department. These employees can use the data for functions such as comparing actual gate flows to the modeled flows, using pressure data to validate model results, and for monitoring the system for high or low-pressure events. The Gas Control department can use the data to monitor the current condition of the distribution system. Decisions to dispatch personnel to locations based on the data originate in the Gas Control department. The Gas Supply department can use the SCADA data to keep nominations in balance with actual use. Historical and current data along with weather forecasts can be used to determine how much gas will be needed in the future. This information is passed on to the marketer for the company to ensure the pipeline company has enough gas available for consumption.

External Customers

Large Volume / Transport / Industrial Customers

Some local distribution companies (LDCs) have contract customers that purchase their natural gas on the open market. The LDC delivers the natural gas to the customer's location with the existing infrastructure. Since these customers are usually contracted to purchase a certain amount of gas, many desire to monitor their usage daily. This is where your SCADA system comes into the picture. Providing timely and accurate data will assist these customers in maintaining compliance with their contractual obligations.

Gas Suppliers / Marketers

Likewise, Gas Suppliers and Marketers may also wish to monitor the usage of the customers they work with under contract. As mentioned above, contracts are usually signed with specific levels of consumption. Suppliers and marketers use SCADA data to ensure compliance with contracts.

Operational Costs

Initial Outlay

The largest expenditure when it comes to SCADA is the initial deployment of equipment. While costs will need to be carefully considered, this should not be the only factor in selecting the necessary RTUs/PLCs, measurement devices, communication devices, or software packages. With that in mind, however, the selection process should take all relevant factors into account. For example, selection of a pressure transmitter may also consider accuracy needed, extra features that may or may not be necessary, and previous experience with a brand or model. If Brand X costs more but has a longer life expectancy and Brand Y costs less but requires replacement more often, the wiser choice would probably be to spend the money initially and defer maintenance costs.

Maintenance

While many of today's electronic devices are not field-maintainable, there are still maintenance costs involved with a SCADA system. Battery changes are an ever-present function. This includes DC UPS systems as well as battery operated wireless devices. Every SCADA system field installation should include barriers and/or surge protection devices as appropriate for the type of protection required. Fuses and circuit breakers are also common in many installations. These items will require replacement at some point in time.

Calibrations

Calibrations ensuring accuracy of the data being measured and reported. Calibrations also cost money to complete. Along with the manhours needed, there are expendables such as filters and calibration gas as well as bottles that require periodic testing. These expenses should be considered when budgeting for ongoing SCADA costs.

Communication Methods

Backhaul Methods

Licensed Radio

Licensed radios are a group of devices that communicate with other devices and the SCADA server using pre-determined radio frequency bands. These radio frequencies are assigned by the Federal Communication Commission (FCC) and are managed to ensure interference free operation in a geographic area. One of the advantages of this method is that once an organization has received a set of frequencies, they can keep these for as long as they want. One of the disadvantages is that to maintain access to these frequencies, a license fee must be paid to the FCC. Additionally, a site rental fee will usually be required as the setup and maintenance of a tower can be a costly venture. Tower owners take on the cost of operating the tower and will rent out space to users to recoup those costs at a lower fee than owning it outright. These licensed radios can use serial, Ethernet, USB, and/or Wi-Fi connections for end devices, depending on the make and model.

Unlicensed Radio

Much like their licensed counterpart, unlicensed radios use radio frequency bands to communicate with other devices as well as the SCADA server. They also can use different physical communications ports to connect to end devices. However, unlicensed radios do not have a managed set of frequencies in which to operate. Unlicensed radios operate in the ISM (industrial, scientific, and medical) bands. These bands are a preset range of frequencies that do not require a license to operate within. While not having a license reduces costs, it also introduces the very real possibility of interference. Since the FCC does not regulate these bands, there is no recourse for another entity interfering with the organizations operations.

Cellular

Numerous studies have shown that the use of cellular for the machine to machine (M2M) arena has been and is currently on the rise. Cellular networks operate much like the radio-based systems for SCADA. A communication device – in this case a cellular modem – is connected to an end device to transmit data to the SCADA server. As the name implies, these devices use the cellular networks instead of radio frequencies. Otherwise, the operation is very similar in nature.

Landline

In conjunction with cellular use on the rise, landline use has been on a steady decline. Following the same trends as seen in a report from the Centers for Disease Control, National Center for Health Statistics, which shows that the number of cell phone only homes passed the 50% mark in the second half of 2016, the use of landlines for SCADA networks has also been on the decline. Cellular modems and SCADA radio systems offer a much more attractive package with more options, increased security features, lower overall costs, and greater reliability than landlines. The use of landlines for SCADA should be carefully considered before going down this path.

Local Methods

There are times when communication at the local level will become necessary or even advantageous. There are a few other methods that have not yet been discussed which can be used in these situations. These methods use low-powered radio signals. As such, they are only suitable in situations where devices are within relative proximity. As an example, the Rosemount 702 wireless transmitter which uses wireless HART has an optional high gain remote antenna rated at only 40 mW maximum power.

Mesh Network

One method for local communications is the mesh network. Mesh networks are configured so that each unit communicates with every other unit within range. In this way, if one path becomes blocked or otherwise fails to work, communication will still happen but through another path using other units. Most of the time the protocol is specific to the manufacturer, though this is not always the case. One example of mesh network technology is Wireless HART. Wireless HART uses the proven HART protocol in the 2.4 GHz ISM band instead of utilizing a wired 4-20 mA loop.

Wi-Fi / Bluetooth

Another form of localized communication involves the use of Wi-Fi and/or Bluetooth. Wi-Fi enabled devices communicate in much the same way your devices at home communicate with your Wi-Fi router. Devices must be configured to communicate within the group that they are intended to occupy. For example, a set of devices on wellheads near each other may belong to the "wellhead" group. Another set of devices may belong to the "gathering" group, and so forth. Bluetooth devices must be setup to pair with each other the same way your Bluetooth speaker pairs with your smartphone.

Security Techniques

GE Grid Solutions recommends three areas to focus on when it comes to securing your SCADA network. Area one is securing the device. Area two is securing user access. Area three is securing the network. Securing the device means making sure that the device itself cannot be tampered with or changed in any way outside of authorized users. This can be accomplished by using tamper seals or by disabling physical ports. Securing user access requires employing user authentication techniques such as usernames and passwords as well as using secure management services such as HTTPS or SNMPv3. Securing the network means using 128-bit or 256-bit AES encryption, utilizing firewalls, and maintaining device certificates. By focusing on all three areas, an organization is well on their way to protecting not only the data, but also access to their network.