SCADA Primer

This document discusses the basics of SCADA systems. It serves as introduction for those who are not familiar with it, and as a reviewer for those who are already knowledgeable about the SCADA Systems.

1 - What is SCADA?

SCADA (Supervisory Control And Data Acquisition) system refers to the combination of telemetry and data acquisition. It consists of collecting information, transferring it back to a central site, carrying out necessary analysis and control, and then displaying this data on a number of operator screens. The SCADA system is used to monitor and control a plant or equipment. Control may be automatic or can be initiated by operator commands.

2 - What is telemetry?

Telemetry is usually associated with SCADA systems. It is a technique used in transmitting and receiving information or data over a medium. The information can be measurements, such as voltage, speed or flow. These data are transmitted to another location through a medium such as cable, telephone or radio. Information may come from multiple locations. A way of addressing these different sites is incorporated in the system.

3 - What is data acquisition?

Data acquisition refers to the method used to access and control information or data from the equipment being controlled and monitored. The data accessed are then forwarded onto a telemetry system ready for transfer to the different sites. They can be analog and digital information gathered by sensors, such as flowmeter, ammeter, etc. It can also be data to control equipment such as actuators, relays, valves, motors, etc.

4 - What are the differences between SCADA and DCS?

Similar to the SCADA systems are the Distributed Control Systems (DCS). The DCS is usually used in factories and located within a more confined area. It uses a high-speed communications medium, such as local area network (LAN). A significant amount of closed loop control is present on the system. The SCADA system covers larger geographical areas. It may rely on a variety of communication links such as radio and telephone. Closed loop control is not a high priority in this system.

5 - Components of SCADA System

A SCADA system is composed of the following:

1. Field Instrumentation;

2. Remote Stations;
3. Communications Network;
4. Central Monitoring Station.

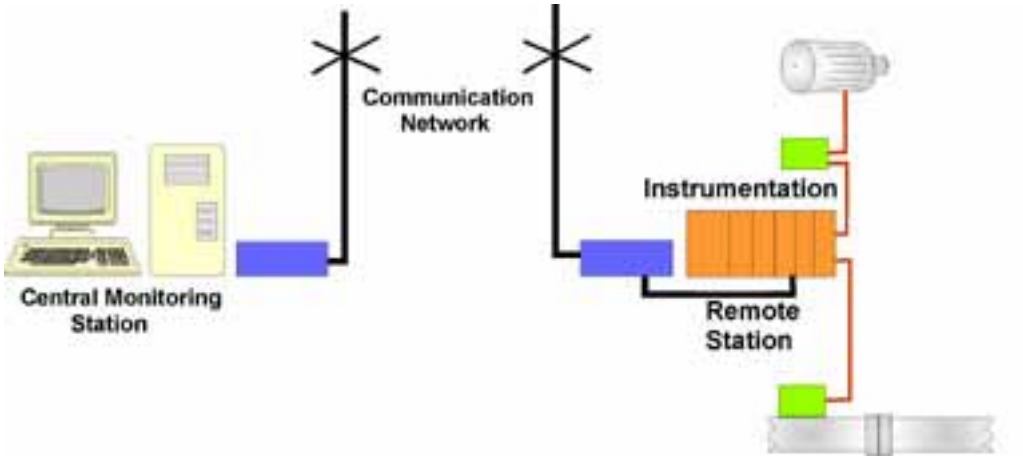

Fig. 1- Components of SCADA System

Field Instrumentation refers to the sensors and actuators that are directly interfaced to the plant or equipment. They generate the analog and digital signals that will be monitored by the Remote Station. Signals are also conditioned to make sure they are compatible with the inputs/outputs of the RTU or PLC at the Remote Station.

The Remote Station is installed at the remote plant or equipment being monitored and controlled by the central host computer. This can be a Remote Terminal Unit (RTU) or a Programmable Logic Controller (PLC).

The Communications Network is the medium for transferring information from one location to another. This can be via telephone line, radio or cable. The Central Monitoring Station (CMS) refers to the location of the master or host computer. Several workstations may be configured on the CMS, if necessary. It uses a Man Machine Interface (MMI) program to monitor various types data needed for the operation. The following is a sample configuration of a SCADA system for water distribution.

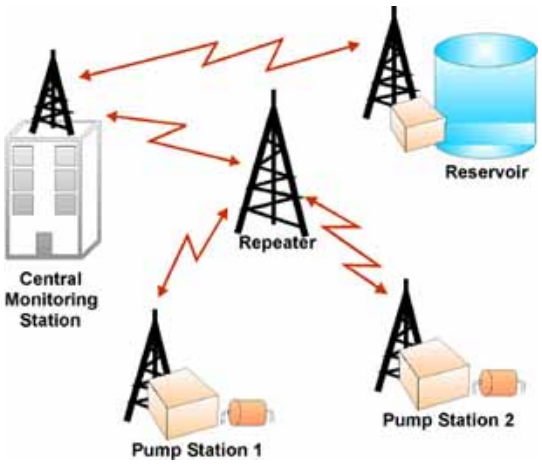

Fig. 2 - SCADA System for Water Distribution

5.1 - SCADA Component: Field Instrumentation

Field Instrumentation refers to the devices that are connected to the equipment or machines being controlled and monitored by the SCADA system. These are sensors for monitoring certain parameters; and actuators for controlling certain modules of the system.

These instruments convert physical parameters (i.e., fluid flow, velocity, fluid level, etc.) to electrical signals (i.e., voltage or current) readable by the Remote Station equipment. Outputs can either be in analog (continuous range) or in digital (discrete values). Some of the industry standard analog outputs of these sensors are 0 to 5 volts, 0 to 10 volts, 4 to 20 mA and 0 to 20 mA. The voltage outputs are used when the sensors are installed near the controllers (RTU or PLC). The current outputs are used when the sensors are located far from the controllers.

Digital outputs are used to differentiate the discrete status of the equipment. Usually, <1> is used to mean EQUIPMENT ON and <0> for EQUIPMENT OFF status. This may also mean <1> for FULL or <0> for EMPTY.

Actuators are used to turn on or turn off certain equipment. Likewise, digital and analog inputs are used for control. For example, digital inputs can be used to turn on and off modules on an equipment. While analog inputs are used to control the speed of a motor or the position of a motorized valve.

5.2 - SCADA Component: Remote Station

Field instrumentation connected to the plant or equipment being monitored and controlled are interfaced to the Remote Station to allow process manipulation at a remote site. It is also used to gather data from the equipment and transfer them to the central SCADA system. The Remote Station may either be an RTU (Remote Terminal Unit) or a PLC (Programmable Logic Controller). It may also be a single board or modular unit.

RTU versus PLC
The RTU (Remote Terminal Unit) is a ruggedized computer with very good radio interfacing. It is used in situations where communications are more difficult. One disadvantage of the RTU is its poor programmability. However, modern RTUs are now offering good programmability comparable to PLCs.

The PLC (Programmable Logic Controller) is a small industrial computer usually found in factories. Its main use is to replace the relay logic of a plant or process. Today, the PLC is being used in SCADA systems to due its very good programmability. Earlier PCL's have no serial communication ports for interfacing to radio for transferring of data. Nowadays, PLC's have extensive communication features and a wide support for popular radio units being used for SCADA system. In the near future we are seeing the merging of the RTU's and the PCL's.
Micrologic is offering an inexpensive RTU for SCADA system wherein the PLC may be an overkill solution. It is a microcontroller-based RTU and can be interfaced to radio modems for transmitting of data to the CMS.

Single Board versus Modular Unit
The Remote Station is usually available in two types, namely, the single board and the modular unit. The single board provides a fixed number of input/output (I/O) interfaces. It is cheaper, but does not offer easy expandability to a more sophisticated system. The modular type is an expandable remote station and more expensive than the single board unit. Usually a backplane is used to connect the modules. Any I/O or communication modules needed for future expansion may be easily plugged in on the backplane.

5.3 - SCADA Component: Communication Network

The Communication Network refers to the communication equipment needed to transfer data to and from different sites. The medium used can either be cable, telephone or radio.

The use of cable is usually implemented in a factory. This is not practical for systems covering large geographical areas because of the high cost of the cables, conduits and the extensive labor in installing them.

The use of telephone lines (i.e., leased or dial-up) is a cheaper solution for systems with large coverage. The leased line is used for systems requiring on-line connection with the remote stations. This is expensive since one telephone line will be needed per site. Besides leased lines are more expensive than ordinary telephone line. Dial-up lines can be used on systems requiring updates at regular intervals (e.g., hourly updates). Here ordinary telephone lines can be used. The host can dial a particular number of a remote site to get the readings and send commands.

Remote sites are usually not accessible by telephone lines. The use of radio offers an economical solution. Radio modems are used to connect the remote sites to the host. An on-line operation can also be implemented on the radio system. For locations wherein a direct radio link cannot be established, a radio repeater is used to link these sites.

5.4 - SCADA Component: Central Monitoring Station (CMS)

The Central Monitoring Station (CMS) is the master unit of the SCADA system. It is in charge of collecting information gathered by the remote stations and of generating necessary action for any event detected. The CMS can have a single computer configuration or it can be networked to workstations to allow sharing of information from the SCADA system.

A Man-Machine Interface (MMI) program will be running on the CMS computer. A mimic diagram of the whole plant or process can be displayed onscreen for easier identification with the real system. Each I/O point of the remote units can be displayed with corresponding graphical representation and the present I/O reading. The flow reading can be displayed on a graphical representation of a flowmeter. A reservoir can be displayed with the corresponding fluid contents depending on the actual tank level.

Set-up parameters such as trip values, limits, etc. are entered on this program and downloaded to the corresponding remote units for updating of their operating parameters.

The MMI program can also create a separate window for alarms. The alarm window can display the alarm tag name, description, value, trip point value, time, date and other pertinent information. All alarms will be saved on a separate file for later review.

A trending of required points can be programmed on the system. Trending graphs can be viewed or printed at a later time. Generation of management reports can also be scheduled on for a specific time of day, on a periodic basis, upon operator request, or event initiated alarms.

Access to the program is permitted only to qualified operators. Each user is given a password and a privilege level to access only particular areas of the program.. All actions taken by the users are logged on a file for later review.

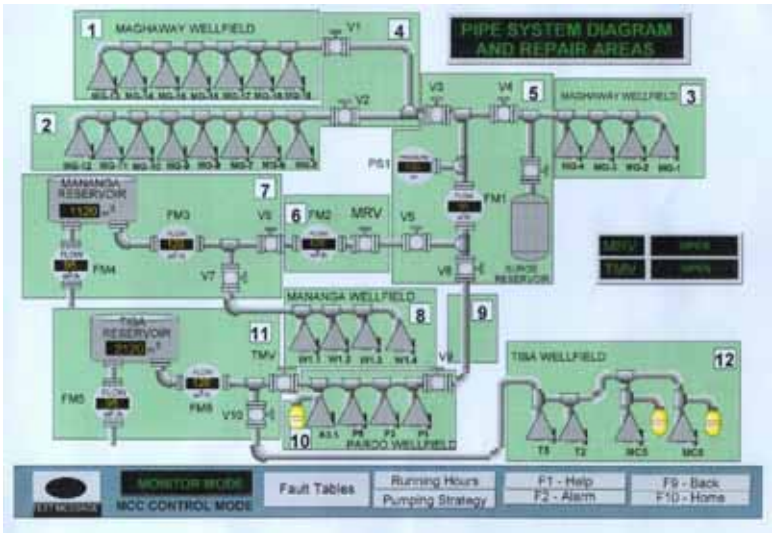

Fig. 3 - MMI Screen Showing Pipe System Diagram and Repair Areas

6 - Typical System Configurations

There are two typical network configurations for the wireless telemetry radio-based SCADA systems. They are the point-to-point and the point-to-multipoint configurations.

6.1 - Point-to-Point Configuration

The Point-to-Point configuration is the simplest set-up for a telemetry system. Here data is exhanged between two stations. One station can be set up as the master and the other as the slave. An example is a set-up of two RTUs: one for a reservoir or tank and the other for a water pump at a different location. Whenever the tank is nearly empty, the RTU at the tank will send an EMPTY command to the other RTU. Upon receiving this command, the RTU at the water pump will start pumping water to the tank. When the tank is full, the tank's RTU will send a FULL command to the pump's RTU to stop the motor.

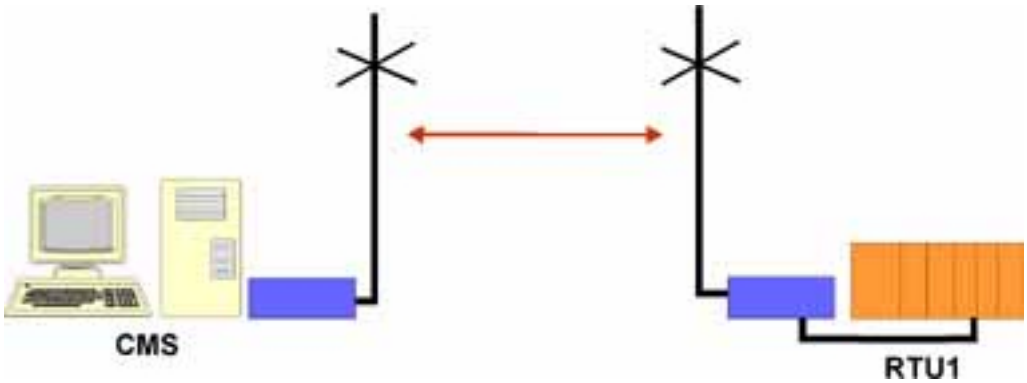

Fig. 4 - Point-to-Point Configuration

6.2 - Point-to-Multipoint Configuration

The Point-to-Multipoint configuration is where one device is designated as the master unit to several slave units. The master is usually the main host and is located at the control room. While the slaves are the remote units at the remote sites. Each slave is assigned a unique address or identification number.

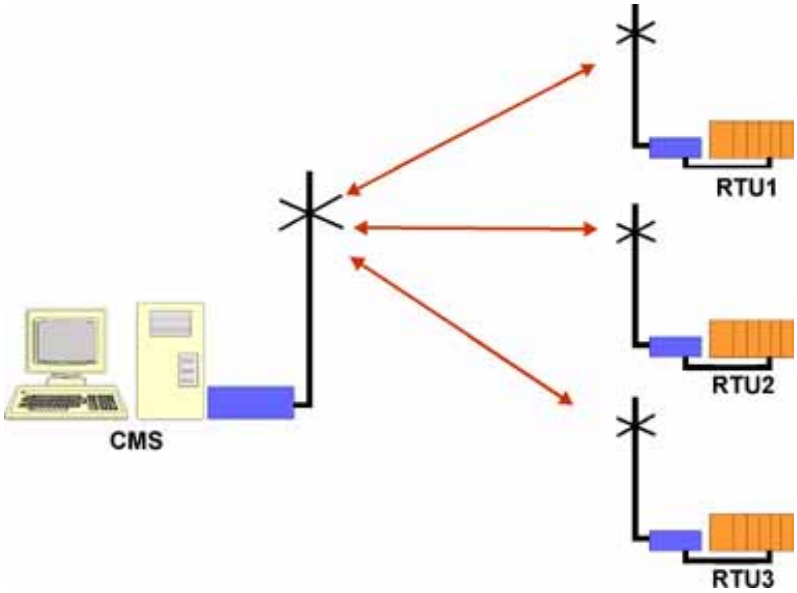

Fig. 5 - Point-to-Multipoint Configuration

7 - Modes of Communication

There are two modes of communication available, namely, the polled system and the interrupt system.

7.1 - Polled System

In the Polled or Master/Slave system, the master is in total control of communications. The master makes a regular polling of data (i.e., sends and receives data) to each slave in sequence. The slave unit responds to the master only when it receivers a request. This is called the half-duplex method. Each slave unit will have its own unique address to

allow correct identification. If a slave does not respond for a predetermined period of time, the master retries to poll it for a number of times before continuing to poll the next slave unit.

Advantages:
Process of data gathering is fairly simple No collision can occur on the network Link failure can easily be detected.

Disadvantages:
Interrupt type request from a slave requesting immediate action cannot be handled immediately Waiting time increases with the number of slaves All communication between slaves have to pass through the master with added complexity.

7.2 - Interrupt System

The interrupt system is also referred to as Report by Exception (RBE) configured system. Here the slave monitors its inputs. When it detects a significant change or when it exceeds a limit, the slave initiates communication to the master and transfers data. The system is designed with error detection and recovery process to cope with collisions. Before any unit transmits, it must first check if any other unit is transmitting. This can be done by first detecting the carrier of the transmission medium. If another unit is transmitting, some form of random delay time is required before it tries again. Excessive collisions result to erratic system operation and possible system failure. To cope with this, if after several attempts, the slave still fails to transmit a message to the master, it waits until polled by the master.

Advantages:
System reduces unnecessary transfer of data as in polled systems. Quick detection of urgent status information. Allows slave-to-slave communication.

Disadvantages:
Master may only detect a link failure after a period of time, that is, when system is polled. Operator action is needed to have the latest values. Collision of data may occur and may cause delay in the communication.