SCADA System Fundamentals

Course No: E01-007

Credit: 1 PDH

Tracy Adams, P.E.

Continuing Education and Development, Inc.
9 Greyridge Farm Court
Stony Point, NY 10980

P: (877) 322-5800
F: (877) 322-4774

info@cedengineering.com

SCADA System Fundamentals

INTRODUCTION

Just as different countries have their own languages so do different technologies. The first step to understanding a new technology is learning the unique language of that technology. This course is intended to provide you with an understanding of the terms and equipment associated with Supervisory Control and Data Acquisition (SCADA) systems.

SCADA systems at their fundamental level are Industrial Control Systems. They are computer based control systems that monitor and control industrial processes that exist in the physical world. SCADA systems can be found in manufacturing facilities, oil production and processing, pharmaceuticals, energy, water treatment and distribution, and the list goes on. They are the best control method for processes that have large amounts of data that need gathering and analyzing, or are spread over large distances, or require critical control in fast paced processes.

SCADA SYSTEM SIGNALS

The very basic components of a SCADA system are these signals:

- **DI –** Discrete Input
- **DO –** Discrete Output

Discrete signals (also called Digital signals) provide an ON or OFF input to a SCADA system. This is the same binary signal format used in computer processors.

The next basic types of signals are:

- **AI –** Analog Input
- **AO –** Analog Output

Analog signals are continuous. A change in signal value reflects change in the parameters being monitored. Examples of analog signals are temperature and pressure.

The signals generated by the instruments being monitored by a SCADA system are voltage or current based. Analog signals can be formatted as: 4-20 mA, 0-20 mA, 1-5VDC, 0-5VDC, -10VDC to 10VDC.

Values (whether discrete or analog), when used in a SCADA system, they need to be seen by Operators to be of any use.

SCADA SYSTEM DATA GATHERING

The Operator's access into a SCADA system is by:

- **OIT –** Operator Interface Terminal or an
- **HMI –** Human Machine Interface

OIT's provide a local interface, typically in a remote location or into an isolated system like skid mounted equipment. Screens to display information have a simple layout since displays are not large; anywhere from 4 inches to 14 inches.

HMI software is used at the Central Control location. Software is installed on computers with faster processors and larger monitors so the screens display more information. They also make use of animation to emphasize critical data or focus operator attention to important areas of a process or annunciate an alarm.

The work horse of the SCADA system that effectively grabs data from instruments, converts the information to a format a computer program can understand, and handles high speed communication is the:

- **PLC –** Programmable Logic Controller

The Programmable Logic Controller (PLC) was invented in 1968 to support the automobile industry by Bedford Associates' engineer Dick Morley. The first PLC was called a MOdular DIgital CONtroller, aka MODICON.

Over time variations of the PLC have developed. The two primary ones are:

- **RTU –** Remote Telemetry Unit
- **PAC -** Programmable Automation Controller

The Remote Telemetry Unit (RTU) was developed to gather data and then transmit that data to a remotely located processor. A RTU has communication capabilities of a PC and the IO capability of a PLC, as well as being industrial hardened. However, it does not control processes using an internal program. It functions as a Data logger that can transmit data at a certain time to Central or when polled. A hybrid version of the RTU contains a PLC that does control local processes and performs the communication functions of a RTU.

A PAC is the next generation of a PLC. It has the same form and function as a PLC but its processor is more related to a computer in its speed and computing methods. Its greatest advantage is the communication function which allows it to work more effectively with modern communication networks that are Ethernet based.

SCADA SYSTEM TYPES

Data gathering and system control at the highest level is broken into two basic systems:

- **SCADA –** Supervisory Control and Data Acquisition
- **DCS –** Distributed Control System

Definition of SCADA is a Monitoring and/or Control System that utilizes a central computer for storing information, and onsite/remote hardware to monitor facilities and processes. Control may be automatic or manual and may occur at the remote units or the central computer.

Definition of DCS is a Monitoring and/or Control System that utilizes a central computer for storing information and onsite/remote hardware to monitor facilities and processes. Control may be automatic or manual and may occur at the remote units or the central computer.

While a SCADA system and a DCS system are essentially the same at all levels, there is a very basic difference. A SCADA system is event driven and operator concentric. It is data gathering orientated. Data is stored in database and control is usually remotely originated. Whereas, a DCS is process state driven. It is directly connected with field devices and control is done locally and automatically. The operator is just informed of what has happened.

A SCADA master station generally considers changes of state (both status points and analogue changes leading to alarms) as the main criteria driving the data gathering and presentation system. Any undetected changes of state simply cannot be missed. A change of state will cause the system to generate all alarms, events, database updates and any special processing required relating to that. Event lists and alarm lists are of major importance to the operator, sometimes more so than data screens. S is for Supervisory - an Operator takes action.

Conversely, DCS systems are process control systems that are state based and consider the process variable's present and past states to be the main criteria driving the DCS. PLC protocols are generally register scanning based, with no specific change of state processing provided. Should a point toggle between scans, it will not be seen by the DCS. If any change of states are critical (as some would be for a DCS used for SCADA applications), a point must be latched on until it is confirmed it has been scanned, which can be difficult and non-deterministic. DCS software tasks are generally run sequentially, rather than event driven. If a process starts to move from a set parameter, the DCS responds to maintain that parameter value. Notifying the Operator is a secondary consideration. Events and alarm lists are secondary in importance to the process displays, and filtering may not be as complex and flexible. On the up side, the generation and display of data, especially analogue trends and standard process blocks, is far more user friendly and easier for both operators and engineers.

SCADA systems historically have been broken down into two basic flavors:

Proprietary SCADA System:

- All or most components manufactured by one supplier
- Installation and service from same single source
- Lack of compatibility with other products
- Uses proprietary communications and programming

Mix & Match SCADA System

- Usually supplied by System Integrator
- Usually uses open communication protocols
- Uses off-the-shelf products
- PLC's program using standard procedures
- Utilizes open HMI Software

Original SCADA systems were proprietary. The Manufacturer built all the hardware, software, installed the equipment and did all the programming.

As computer technology improved, SCADA systems evolved to take advantage of the advancement. Hardware components started coming off the shelf. SCADA software started to be developed to use open protocol communication standards. This led to the rise of System Integrators, companies that developed custom systems to meet the needs of the end users.

SCADA SYSTEM COMPONENTS

These are the four basic parts of a SCADA system.

- Field Instruments
- PLC/Remote Terminal Unit
- Communications Link – open standard (like MODBUS) and proprietary
- Central Computer Station including HMI Software – Proprietary for specific RTUs or open including interfacing many products

We are going to look at each of these parts and identify the basic components for each:

A. FIELD INSTRUMENTS

Discrete signals are generated by:

a. Limit switches

b. Pushbuttons

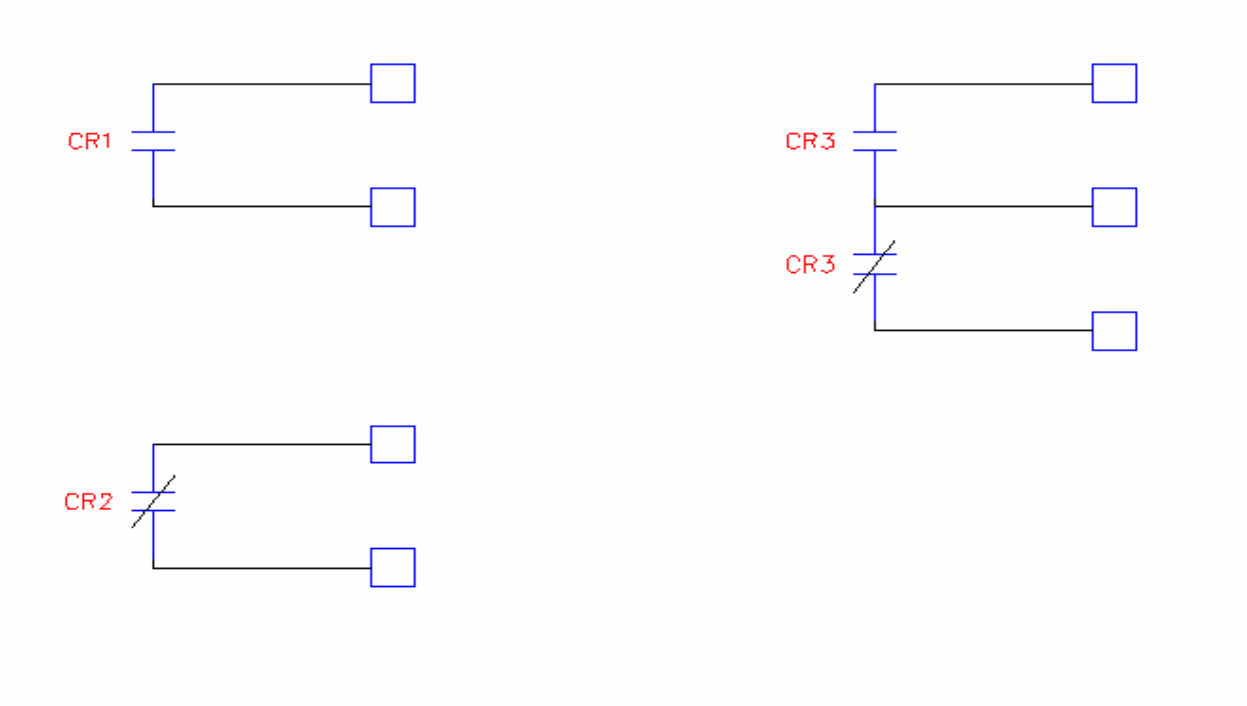
c. Float switches

d. Flow switches

e. Relay contacts

f. Selector switches

Discrete signals have three basic configurations that are used:



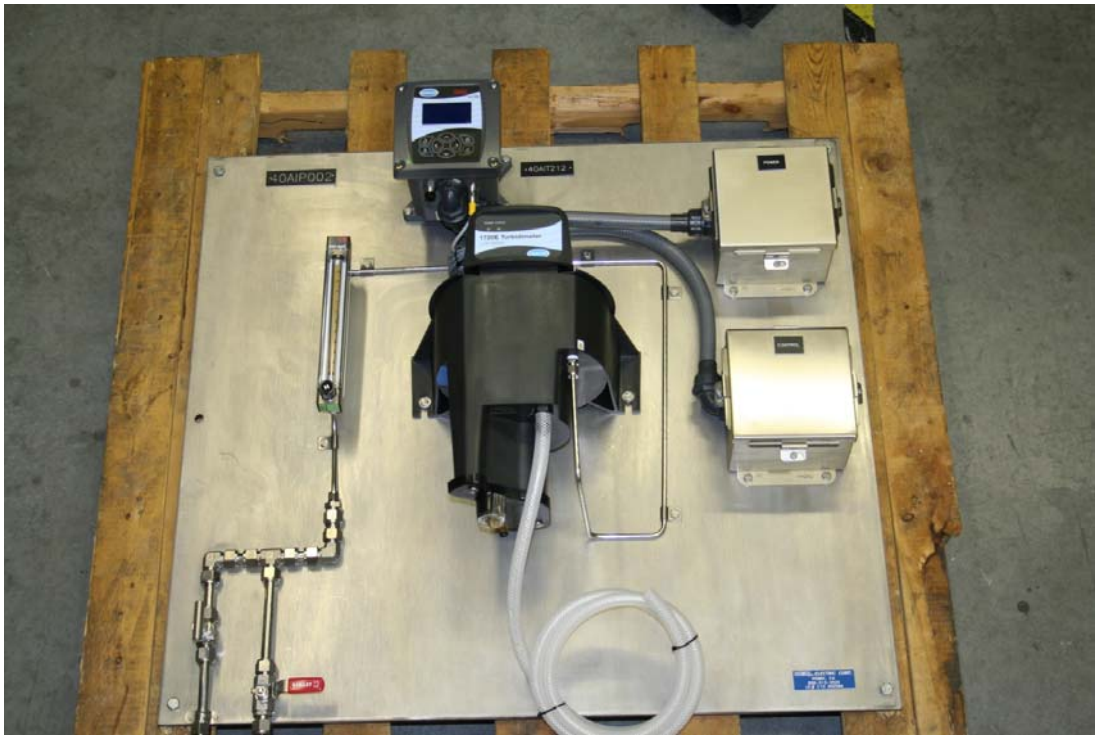
Form A - Normally Open

Form B - Normally Closed

Form C - Normally Open-Normally Closed combined

Analog signals generally come from instruments and motion controlling equipment. The most common instrument is the analyzer. Analyzers are test equipment located in the field for monitoring the quality of a process. Analyzer primary signal output is analog but there are typically some discrete contacts for alarms. Below are some examples of analyzers:

This is a turbidity meter used to measure solids in water.



Below is a Chlorine Analyzer used to measure the level of chlorine in water leaving a treatment plant to ensure it is safe for humans.

While not an instrument, a Variable Frequency Drive (VFD) is a field device that frequently interfaces with SCADA systems to control process outputs. VFD's are used to power motors driving pumps and fans. VFD's generate analog and discrete signals.

Typical signals from a VFD are:

- Speed Indication (Analog)
- Speed Control (Analog)
- Running (Discrete)
- Fault (Discrete)
- Start Command (Discrete)

B. PLC/RTU

PLC's come in a wide variety of sizes and shapes. They are used from controlling nuclear power plants to controlling a sump pump in a parking garage.

High end PLC's can handle multiple racks of IO modules, various communication modules, and may be installed in a redundant configuration so the loss of a power supply or processor will not stop control of a facility.

The latest step in the evolution of PLC's is the Programmable Automation Controller (PAC).

A PAC has a computer processor so it works better with Ethernet networks (routers/switches) which are becoming prevalent in SCADA systems. Programming can also be done in more main stream programs (C++, etc)

Smaller PLC's are configured for just a few points. Sometimes they may only have discrete signals, and function as intelligent relays. They are not typically expandable to add more IO points.

Programming is usually simple. Sometimes the programming can even be done with the keys on the front of the PLC. Relay Ladder Logic was the first programming language for PLC's. It mimicked the wiring diagrams electricians were used to seeing in control panels in software. In fact, electricians were the first PLC programmers.

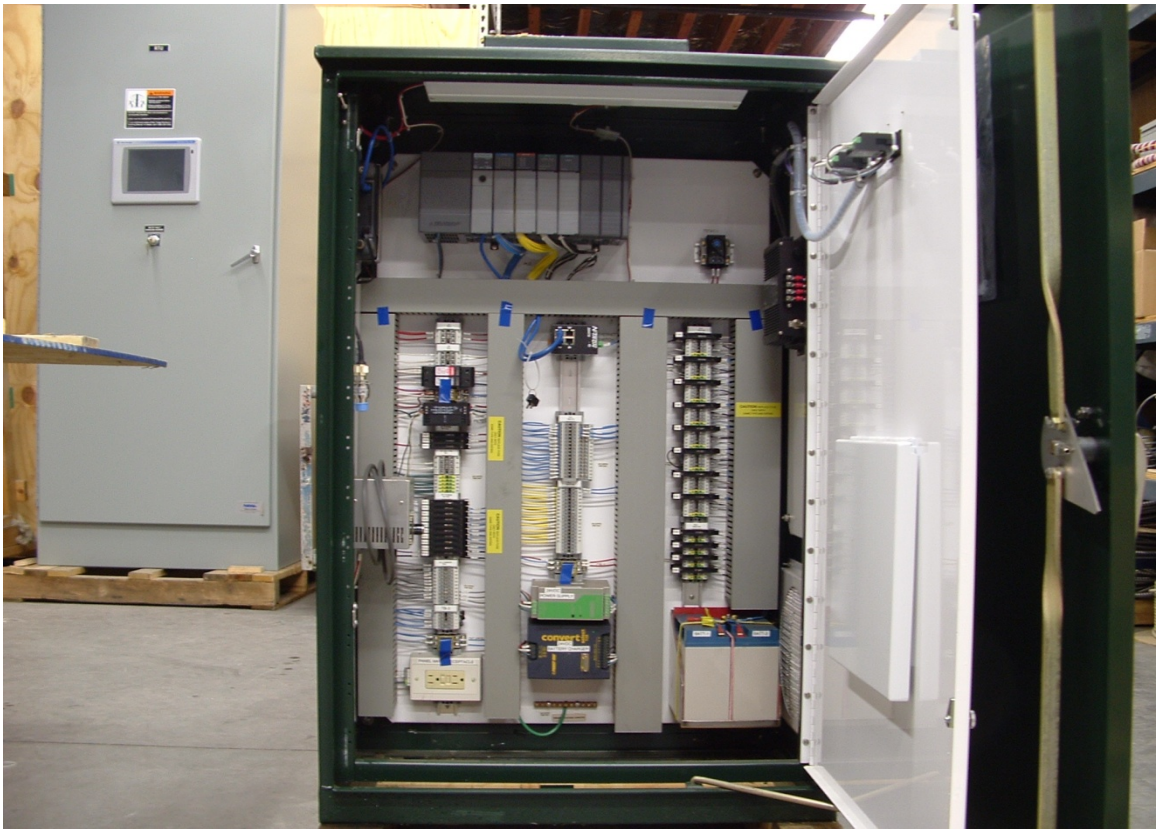
As hardware and software changed, the companies making the products started diverging. It became apparent that standards had to be developed so the software and hardware could work together. There also started to be programmers who were familiar with multiple high level programming languages and never saw the inside of a control panel. In Europe IEC developed standard 61131 which specified five styles of programming to be used in PLC's:

- Relay Ladder Logic
- Function Block Diagram
- Structure Text
- Instruction List
- Sequential Function Chart

In addition to these standards, PLC's can have specialty modules installed that use C++ or Basic for special program requirements.

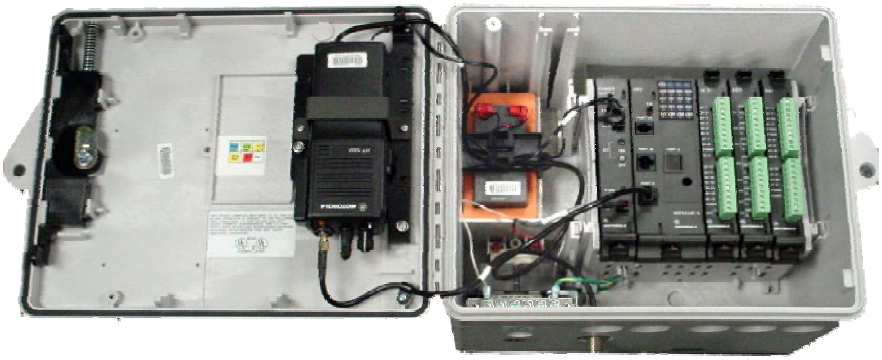
PLC's cannot be mounted to a wall and left unprotected. They are mounted in enclosures that protect them from hostile environments. A typical PLC panel is shown below with high end PLC's configured with redundant processors and power supplies.

Shown below is an RTU configured with a PAC that can provide local control in case communications are lost. This panel communicates via leased line using the modem in the lower left corner of the panel.



This is an example of a control panel that shows the customized approach taken to building control panels. This is designed for a site with a large number of physical IO. A radio will be

installed in the upper right hand corner for communication. Note the batteries in the lower right corner for backup power. A Remote IO panel (an RTU) interfaces with field devices but has no processors for local control. It is equipped with a communication module instead.



This style reflects the original design on RTU's. It has a processor to handle communications via the radio mounted on the door. It receives signals from field devices which it passes through to Central for display by the SCADA HMI. It then passes any commands from Central to the field devices.

Autodialers (shown below) are a very basic form of RTU. This device receives site alarms as Digital Input signals. It then calls a Duty Operator over a standard telephone line (POTS) or a cell phone. The Operator can acknowledge the alarm using the telephone keyboard. Higher end Autodialers also allow the Operator to do basic controls via the keyboard such as starting a backup pump or operate valves.

C. Communication

Radios are the most common communication method in large SCADA systems. Licensed radios were originally used. Then in 1987 the FCC marked a radio frequency band segment for Industrial Scientific Medical (ISM) use. This was an unlicensed segment that was opened for use and did not require a license. The ISM is in the low 900MHz range.

The ISM band is limited to a maximum of 1 Watt transmitting power. This was the method selected to reduce interference by limiting the range of the transmissions. Licensed radios are still used in SCADA systems for operators who have a long distance that needs to be covered between sites.

Characteristics of most frequently used frequencies are:

1) Licensed VHF – 132-174 Mhz, 400Mhz

- Up to 5 Watts Power
- Very Good Signal Transmission

2) Licensed UHF – 380-512 Mhz

- Good Signal Transmission

3) Unlicensed Spread Spectrum – 900 Mhz

- 1 Watt max. Power
- Line-of-Sight, weather dependent
- Ethernet protocol versions are available in all frequencies.

A recent trend in SCADA system has been the incorporation of video cameras and still cameras to provide Operators real time images of what is happening at remote sites. The need for increased security was the driving force behind this trend.

Images contain a lot of data. In order to transmit images over a radio link and make them practical, frequencies in the 2.4 GHz and 5.8 GHz are used.

Above is the basic radio form that was originally selected for industrial use and is still a very popular and functional form used today.

As electronics improved, radios became smaller while still keeping the same performance capabilities. This style of radio is designed to be mounted on DIN rail.

One of the areas that a radio link loses transmission power is the cable connecting the radio with the antenna. The above radio is a weatherized unit that can be mounted on the mast just below the antenna. This eliminates signal power lost during transmission through the antenna cable. Typically an Ethernet connection is provided to interface with PLC's or computers.

The two basic workhorse antennas of SCADA systems are YAGI and Omni.

YAGI

OMNI

The yagi is for directional transmission and the omni provides 360 degrees of transmission.

An omni antenna will be used at a SCADA Central site to broadcast to RTU's at many different locations. The yagi antenna transmits radio signals in the direction the antenna is pointing.

As higher radio frequencies (2.4 GHz and 5.8 GHz) have come into use for transmitting more data (e.g. video signals), panel and parabolic antennas are now common in SCADA Systems.

Another application using radios is wireless IO. This is a paired set of radios that have terminals for connecting physical IO signals (discrete or analog). One radio is for connecting field devices: a pressure transmitter or a high level float. The second radio receives the signals with the field devices values and retransmits the signals over wires connected to a PLC.

The two radios are paired to work together. They cannot communicate to any other radios. This system eliminates all the conduits and wires that would have been installed to connect the field devices to the PLC. No special communication configuration had to be designed to allow the radio to talk to the PLC. This is a way to save money when needing to pick up a single point and tie it into a SCADA system.

Within SCADA systems multiple protocols are available for communication. Protocols are the methodology used to encapsulate data for transmission between SCADA components. Designers just need to select the method best suited for the system.

Originally serial communications were conducted over special cables with various protocols (Fieldbus, ControlNET, Modbus RTU, etc). These were the standards for many years and they are still used frequently.

The late comer Ethernet has recently made big move into the field. As the electronics became industrialized, the ability to use the same communication in a SCADA system (that the IT Department was familiar with) became a money saver.

It also streamlined the interface between PLC and SCADA computers. It has simplified SCADA communications by allowing the gathering of data from "smart" devices such as VFD's, power monitors, analyzers, etc. with just a single cable.

In addition to the traditional radio and serial cable communications, SCADA systems also use:

- Cellular – PCS, CDPD
- Telephone Lines – Dedicated leased and Dial-up
- Wireless Internet
- DSL Broadband
- Fiber Optic – supports Ethernet protocol
- Satellite – Geosynchronous LEO

Designers just need to find the right method to solve the communication problem. For example, satellites are used for accessing remote sites in mountainous terrain where it is impossible to get a radio signal out or run a cable.

D. Central Computers

One of the first steps in designing a SCADA system is to determine which Communication Protocol will be used. The most common protocols used are:

- MODBUS RTU or MODBUS ASCII (original protocol used)
- DEVICENET
- CONTROLNET
- Profibus
- Foundation Fieldbus
- DH+, DF1
- DNP3
- Ethernet (MODBUS TCP, ETHERNET IP)

Protocols are the languages that the equipment uses to communicate. Just as people speak English, French, German, etc., so have different protocols been developed by different manufacturers. These different protocols are intended to maximize the hardware benefits of their equipment. Some of these protocols are open for anyone to use and some are proprietary.

The second step is determining the hardware:

- Computer Hardware inc. UPS – Off-the-shelf
- Central RTU – Sometimes for polling
- Communication Interface – Radio/Antenna, Telephone Modem, DSL Modem
- HMI – Human Machine Interface
- Common HMIs – Intellution, Wonderware, Citec, Trihedral Engineering VT-Scada
- Internet Based – Mission
- Web based - Inductive Automation

At the high level end of a SCADA system, you see the equipment and software that the Operators use to interface with the system. At this level communication is the key process. There is the hardware and software to interface with all the field components.

Also, there is hardware and software to interface with the operators. This side of the process is very graphic oriented.

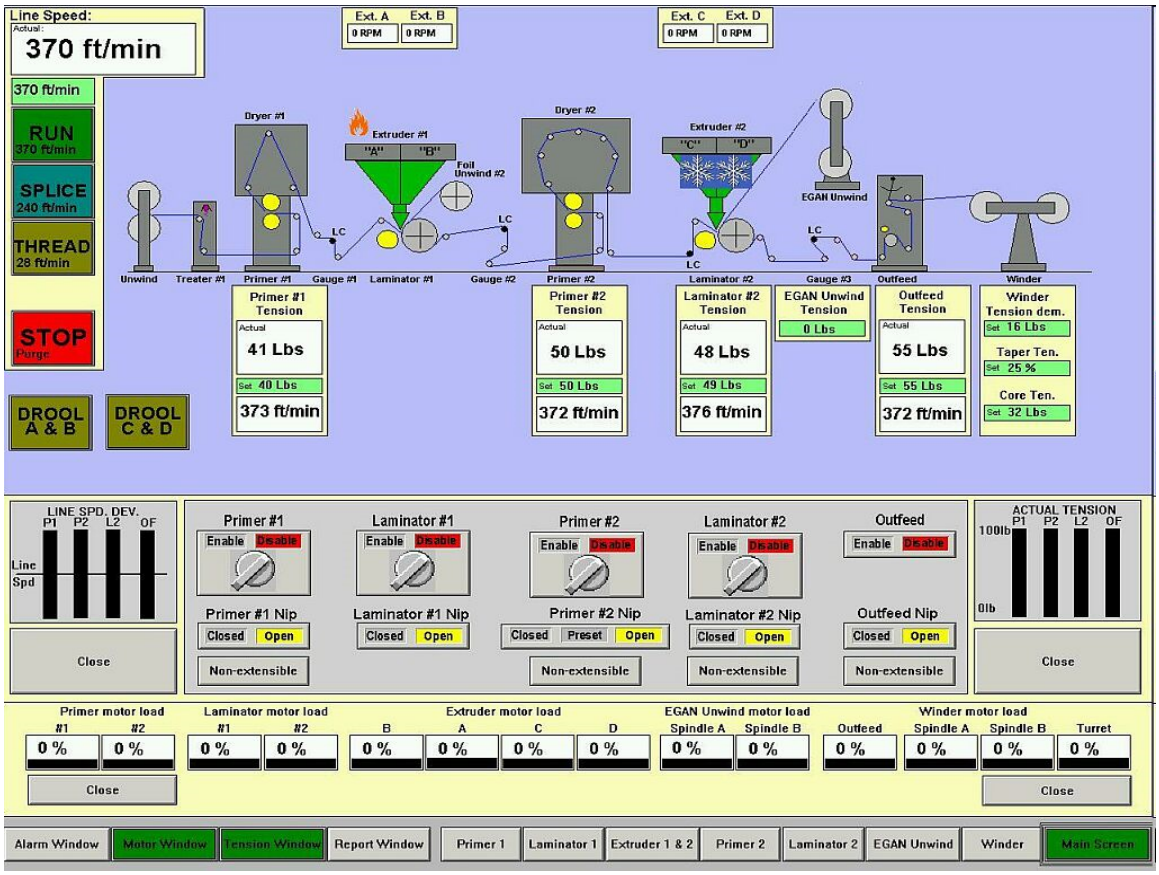
- SCADA Fundamentals
- Alarm Annunciation
- Remote Control
- Trending – Real Time/Historical
- Data Logging / History
- Alarming
- Reporting
- Security
- High Level Optimization Strategies
- Auto-Dialer / Pager
- Remote Monitoring

The SCADA HMI software is written to provide these services to the Operators for their day to day operations:

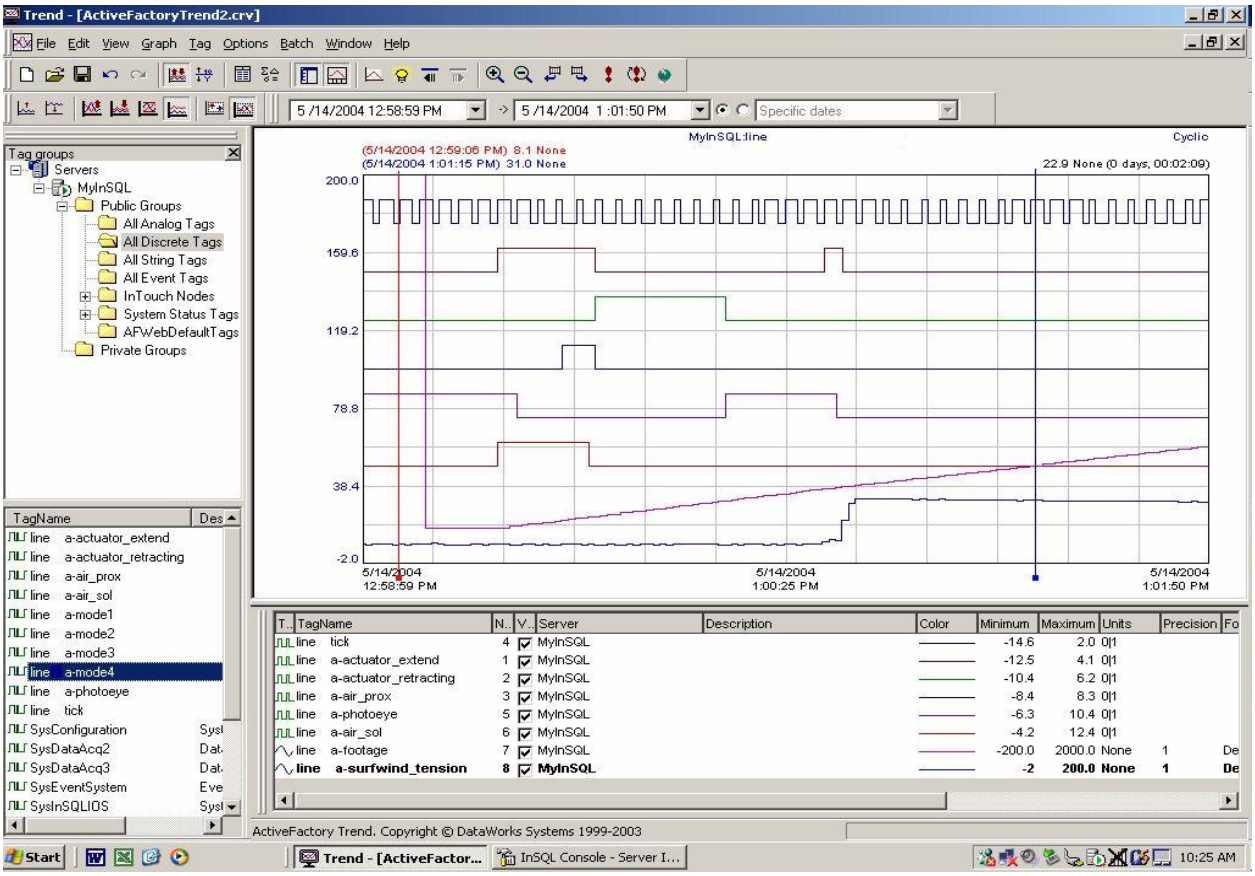
- SCADA Fundamentals
- Analog Summary
- Radio Error Analysis
- Log Report – All Data
- Detail Report
- Pump Activity – Total & Ave Run Times, Starts
- Pump Discrepancy – Excessive changes

- Flow
- Water Quality

Another very important feature of SCADA HMI software is documentation for historical purposes. The data collected is achieved and then distributed in various formats. This information helps with maintenance as well as reporting to supervisory organizations.



A typical graphics screen allows the operator in a quick glance to see the status of all the critical equipment and processes in an area.



Trending is data spread over a period of time and presented in a graph. This is a useful tool for improving processes.

CONCLUSION

SCADA systems are a vital tool for keeping our society going. As electronics and communications have improved, so have the capabilities of SCADA systems. SCADA systems make controlling large and small processes easier for Operators whether they are in telecommunications, water treatment, manufacturing, energy production, oil production, transportation, etc.