Chapter 9. SCADA

9.1. Introduction and Brief History of SCADA

SCADA (Supervisory Control and Data Acquisition) has been around as long as there have been control systems. The first "SCADA" systems utilized data acquisition by means of panels of meters, lights and strip chart recorders. Supervisory control was exercised by the operator manually operating various control knobs. These devices were and still are used to do supervisory control and data acquisition on plants, factories and power generating facilities.

9.1.1. Fundamental Principles of Modern SCADA Systems

SCADA refers to the combination of telemetry and data acquisition. SCADA encompasses the collecting of the information, transferring it back to the central site, carrying out any necessary analysis and control and then displaying that information on a number of operator screens or displays. The required control actions are then conveyed back to the process.

The PLC or Programmable Logic Controller is still one of the most widely used control systems in industry. As needs grew to monitor and control more devices in the plant, the PLCs were distributed and the systems became more intelligent and smaller in size. PLCs and DCS or (Distributed Control Systems) are used as shown below.

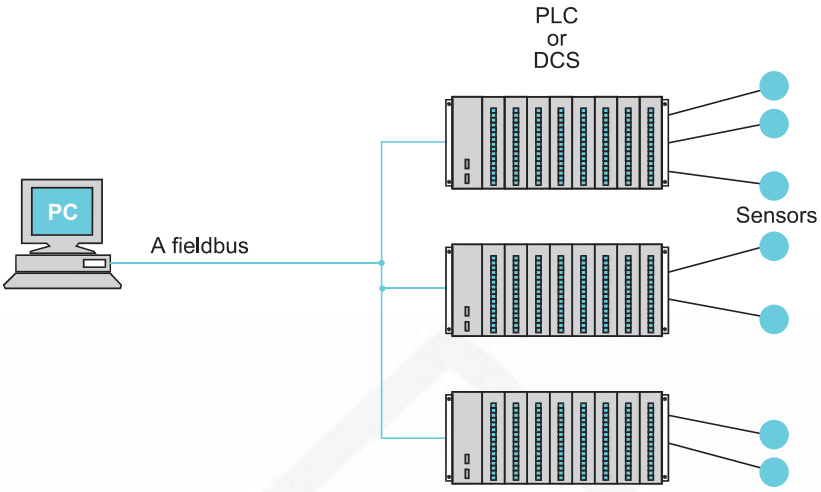

Figure 9.1
PC to PLC or DCS with a fieldbus and sensors

The advantages of the PLC / DCS SCADA system are:

- The computer can record and store a very large amount of data.
- The data can be displayed in any way the user requires.
- Thousands of sensors over a wide area can be connected to the system.
- The operator can incorporate real data simulations into the system.
- Many types of data can be collected from the RTUs.
- The data can be viewed from anywhere, not just on site.

The disadvantages are:

- The system is more complicated than the sensor to panel type.
- Different operating skills are required, such as system analysts and programmer.
- With thousands of sensors there is still a lot of wire to deal with.
- The operator can see only as far as the PLC.

9.1.2. SCADA Hardware

A SCADA System consists of a number of Remote Terminal Units (or RTUs) collecting field data and sending that data back to a master station via a communications system. The master station displays the acquired data and also allows the operator to perform remote control tasks.

On a more complex SCADA system there are essentially five levels or hierarchies:

- Field level instrumentation and control devices
- Marshalling terminals and RTUs
- Communications system
- The master station(s)
- The commercial data processing department computer system

9.1.3. SCADA Software

SCADA Software can be divided into two types, Proprietary or Open. Companies develop proprietary software to communicate to their hardware. These systems are sold as “turn key” solutions. Open software systems have gained popularity because of the Interoperability they bring to the system.

Citect and WonderWare are just two of the open software packages available on the market for SCADA systems

9.1.4. SCADA and Local Area Networks

To enable all the nodes on the SCADA network to share information, they must be connected by some transmission medium. The method of connection is known as the network topology.

Nodes need to share this transmission medium in such a way as to allow all nodes access to the medium without disrupting an established sender.

Ethernet is the most widely used LAN today because it is cheap and easy to use. Connection of the SCADA network to the LAN allows anyone within the company, with the right software and permission, to access the system. Since the data is held in a database the user can be limited to reading the information.

9.1.5. Modem Use in SCADA Systems

Figure 9.2
PC to RTU Using a Modem

Often in SCADA systems the RTU (Remote Terminal Unit (PLC, DCS or IED)) is located at a remote location. This distance can vary from tens of meters to thousands of Kilometers. One of the most cost-effective ways of communicating with the RTU over long distances can be by dialup telephone connection. With this system the devices needed are a PC, two dialup modems and the RTU (assuming that the RTU has a built in COM port). The modems are put in the auto-answer mode and the RTU can dial into the PC or the PC can dial the RTU.

9.1.6. System Implementation

When first planning and designing a SCADA system, consideration should be given to integrating new SCADA systems into existing communication networks in order to avoid the substantial cost of setting up new infrastructure and communications facilities. This may be carried out through existing LANs, private telephone systems or existing radio systems used for mobile vehicle communications.

9.2. SCADA Systems Software

The typical components of a SCADA system, with emphasis on the SCADA software are indicated in the Figure 9.3.

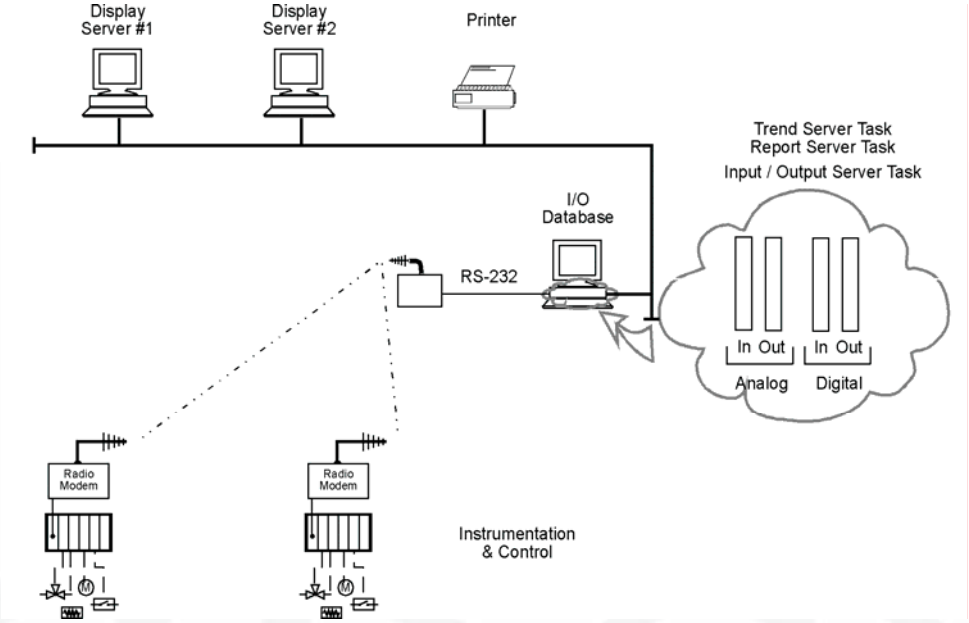

Figure 9.3
Components of a SCADA System

Typical key features expected of the SCADA software are listed below. These features depend on the hardware to be implemented.

9.2.1. SCADA Key Features

User Interface

- Keyboard
- Mouse
- Trackball
- Touch screen

Graphics Displays

- Customer-configurable, object orientated and bit mapped
- Unlimited number of pages
- Resolution: up to 1280 x 1024 with millions of colors

Alarms

- Client server architecture
- Time stamped alarms to 1 millisecond precision (or better)
- Single network Acknowledgment and control of alarms
- Alarms shared to all clients
- Alarms displayed in chronological order
- Dynamic allocation of alarm pages
- User-defined formats and colors

- Up to four adjustable trip points for each analog alarm
- Deviation and rate of change monitoring for analog alarms
- Selective display of alarms by category (256 categories)
- Historical alarm and event logging
- Context-sensitive help
- On-line alarm disable and threshold modification
- Event-triggered alarms
- Alarm-triggered reports
- Operator comments that can be attached to alarms

Trends

- Client server architecture
- True trend printouts (not screen dumps)
- Rubber band trend zooming
- Export data to DBF, CSV files
- X/Y plot capability
- Event based trends
- Pop-up trend display
- Trend gridlines or profiles
- Background trend graphics
- Real-time multi-pen trending
- Short and long term trend display
- Length of data storage and frequency of monitoring that can be specified on a per-point basis
- Archiving of historical trend data
- On-line change of time-base without loss of data
- On-line retrieval of archived historical trend data
- Exact value and time that can be displayed
- Trend data that can be graphically represented in real time

RTU (and PLC) Interface

- All compatible protocols included as standard
- DDE drivers supported
- Interface also possible for RTUs, loop controllers, bar code readers and other equipment
- Driver toolkit available
- Operates on a demand basis instead of the conventional predefined scan method
- Optimization of block data requests to PLCs
- Rationalization of network user data requests
- Maximization of PLC highway bandwidth

Scalability

Additional hardware can be added without replacing or modifying existing equipment. This is limited only by the PLC architecture (typically 300 to 40,000 points)

Access to Data

- Direct, real-time access to data by any network user
- Third-party access to real-time data, e.g. Lotus 123 and EXCEL
- Network DDE
- DDE compatibility: read, write and exec
- DDE to all IO device points
- Clipboard

Database

- ODBC driver support
- Direct SQL commands or high level reporting

Networking

- Supports all NetBIOS compatible networks such as NetWare, LAN Manager, Windows for Workgroups, Windows NT (changed from existing NT)
- Support protocols NetBEUI, IPX/SPX, TCP/IP and more
- Centralized alarm, trend and report processing - data available from anywhere in the network
- Dual networks for full LAN redundancy
- No network configuration required (transparent)
- May be enabled via single check box, no configuration
- LAN licensing based on the number of users logged onto the network, not the number of nodes on the network
- No file server required
- Multi-user system, full communication between operators
- RAS and WAN supported with high performance
- PSTN dial up support

Fault Tolerance and Redundancy

- Dual networks for full LAN redundancy
- Redundancy that can be applied to specific hardware
- Supports primary and secondary equipment configurations
- Intelligent redundancy allows secondary equipment to contribute to processing load
- Automatic changeover and recovery
- Redundant writes to PLCs with no configuration
- Mirrored disk I/O devices
- Mirrored alarm servers
- Mirrored trend servers
- File server redundancy
- No configuration required, may be enabled via single check box, no configuration

Client/Server Distributed Processing

- Open architecture design
- Real-time multitasking
- Client/server fully supported with no user configuration
- Distributed project updates (changes reflected across network)

- Concurrent support of multiple display nodes
- Access any tag from any node
- Access any data (trend, alarm, report) from any node

9.2.2. The SCADA Software Package

Whilst performance and efficiency of the SCADA package with the current plant is important, the package should be easily upgradeable to handle future requirement. The system must be easily modifiable to allow for the requirements changing and expanding as the task grows - in other words the system must use a scaleable architecture.

There have been two main approaches to follow in designing the SCADA system:

- Centralized, where a single computer or mainframe performs all plant monitoring and all plant data is stored on one database which resides on this computer.
- Distributed, where the SCADA system is shared across several small computers (usually PCs).

An effective solution is to examine the type of data required for each task and then to structure the system appropriately. A client server approach also makes for a more effective system.

There are typically five tasks in any SCADA system. Each of these tasks performs its own separate processing.

- Input/Output Task. This program is the interface between the control and monitoring system and the plant floor.
- Alarm Task. This manages all alarms by detecting digital alarm points and comparing the values of analog alarm points to alarm thresholds.
- Trends Task. The trends task collects data to be monitored over time.
- Reports Task. Reports are produced from plant data. These reports can be periodic, event triggered or activated by the operator.
- Display Task. This manages all data to be monitored by the operator and all control actions requested by the operator.

9.2.3. System Response Times

These should be carefully specified for the following events. Typical speeds which are considered acceptable are:

- Display of analogue or digital value (acquired from RTU) on the Master Station Operator Display (1 to 2 seconds maximum)
- Control request from operator to RTU (1 second critical; 3 seconds non- critical)
- Acknowledge of alarm on operator screen (1 second)
- Display of entire new display on operator screen (1 second)
- Retrieval of historical trend and display on operator screen (2 seconds)
- Sequence of events logging (at RTU) of critical events (1 millisecond)

It is important that the response is consistent over all activities of the SCADA system.

9.2.4. Specialized SCADA Protocols

A Protocol controls the message format common to all devices on a network. Common protocols used in radio communications and telemetry systems include the HDLC, MPT1317 and Modbus protocols. The CSMA/CD protocol format is also used.

9.2.4.1. Introduction to Protocols

The transmission of information (both directions) between the master station and RTUs using time division multiplexing techniques requires the use of serial digital messages. These messages must be efficient, secure, flexible, and easily implemented in hardware and software. Efficiency is defined as:

Information Bits Transmitted ÷ Total Bits Transmitted

Security is the ability to detect errors in the original information transmitted, caused by noise on the communication channel. Flexibility allows different amounts and types of information to be transmitted upon command by the master station. Implementation in hardware and software requires the minimum in complicated logic, memory storage, and speed of operation.

All messages are divided into three basic parts as follows:

- Message Establishment; which provides the signals to synchronize the receiver and transmitter.
- Information; which provides the data in a coded form to allow the receiver to decode the information and properly utilize it.
- Message Termination; which provides the message security checks and a means of denoting the end of the message. Message security checks consist of logical operations on the data which result in a predefined number of check bits transmitted with the message. At the receiver the same operations are performed on the data and compared with the received check bits. If they are identical, the message is accepted; otherwise, a retransmission of the original message is requested.

A typical example of commonly used asynchronous message format is shown in Figure 9.4.

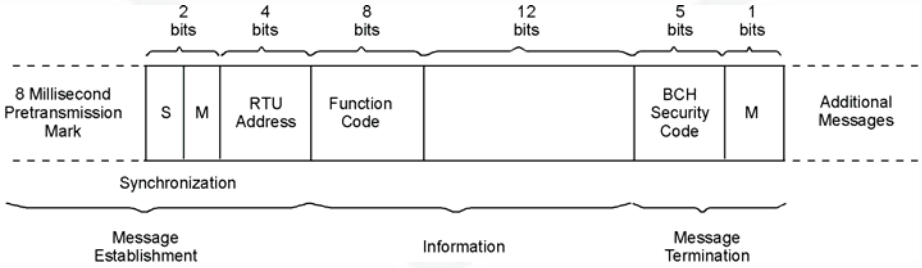

Figure 9.4
Typical Asynchronous Message Format

9.2.4.2. Information Transfer

Master to Remote Data Transfer: Information transmitted from master to remote is for the purpose of device control, set point control, or batch data transfer. Due to the possible severe consequences of operating the wrong device or receiving a bad control message, additional security is required for control. This is provided in the form of a sequence of messages, commonly called a select-before-operate sequence, as shown in Figure 9.5.

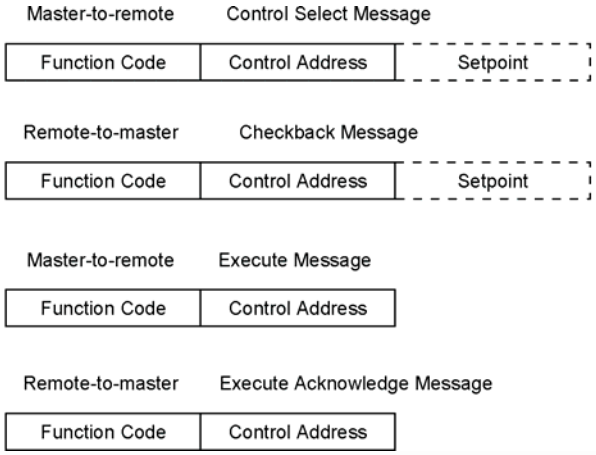

Figure 9.5
Sequence of Messages for Control

The following explanatory notes apply to Figure 9.5:

- Message establishment and message termination fields are not shown
- Function code specifies the operation to be performed by the RTU.
- Control address specifies the device or set point to be controlled
- Set point provides the value to be accepted by the RTU
- A remote to master checkback message is derived from the RTU point selection hardware in order to verify that the RTU has acted correctly in interpreting the control selection.

Remote to Master Data Transfer: All remote to master data transfer is accomplished with one basic message sequence by using variations in the field definitions to accommodate different types of data. The basic sequence is shown in Figure 9. 6.

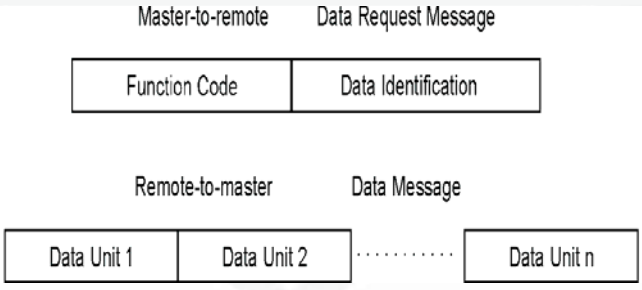

Figure 9. 6
Sequence of Messages for Data Acquisition

The following explanatory notes apply to Figure 9. 6:

- Message establishment and message termination fields are not shown.
- Function code specifies the type of data to be transferred by the RTU.
- Data identification identifies the amount and type of data requested by the master station.

9.2.4.3. High Level Data Link Control (HDLC) Protocol

HDLC has been defined by the International Standards Organization for use on both multipoint and point-to-point links. HDLC is a bit based protocol. The two most common modes of operation of HDLC are:

Unbalanced Normal Response Mode (NRM): This is used with only one primary (or master) station initiating all transactions.

Asynchronous Balanced Mode (ABM): In this mode each node has equal status and can act as either a secondary or primary node.

The standard format is indicated in Figure 9.7 below. .

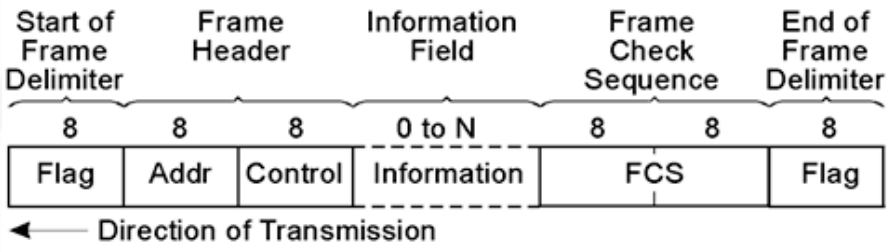

Figure 9.7
HDLC Frame Format

Contents of Frame: The contents of the frame are briefly as follows:

The flag character is a byte with the form 01111110. In order to ensure that the receiver always knows that the character it receives is a unique flag character (rather than merely some other character in the sequence); a procedure called zero insertion is followed. This requires the transmitter to insert a '0' after a sequence of five 1's in the text (i.e. non flag characters).

The Frame Check Sequence (FCS) uses the CRC-CCITT methodology except that 16 ones are added to the tail of the message before the CRC calculation proceeds and the remainder is inverted.

The address field can contain one of three types for the request or response message to or from the secondary node:

- Standard secondary address
- Group addresses for groups of nodes on the network
- Broadcast addresses for all nodes on the network (here the address contains all 1s)

Where there are a large number of secondarys on the network, the address field can be extended beyond 8 bits by encoding the least significant bit as a 1. This then indicates that there is another byte to follow in the address field.

The control field is indicated in Figure 9.7. Note that the send and receive sequence numbers are important to detect and correct errors in the messages. The P/F bit is the poll/final bit and when set indicates to the receiver that it must respond or acknowledge this frame (again with the P/F bit set to 1).

Protocol Operation: A typical sequence of operations is given below.

- In a multidrop link, a normal response mode frame is sent by the primary node with the P/F bit set to 1 together with the address of the secondary.
- The secondary responds with an unnumbered acknowledgment with the P/F bit set to 1. Alternatively if the receiving node is unable to accept the set up command a disconnected mode frame is returned.
- Data is then transferred with the information frames.
- The primary node then sends an unnumbered frame containing disconnect in the control field.
- The secondary then responds with an unnumbered acknowledgment.
- A similar approach is followed for a point to point link using asynchronous balanced mode except that both nodes can initiate the setting up of the link and the transfer of information frames, and the clearing of the point to point link.
- When the secondary transfers the data, it transmits the data as a sequence of information frames with the F bit set to 1 in the final frame of the sequence.
- In NRM mode if the secondary has no further data to transfer, it responds with a receiver not ready frame with the P/F bit set to 1.

9.2.4.4. The CSMA/CD Protocol Format

The CSMA/CD protocol is not as comprehensive as HDLC and is concerned with the method used to get data on and off the physical medium. HDLC and CSMA/CD can be incorporated together for a more complete protocol.

The format of a CSMA/CD frame which is transmitted is shown in Table 9. 1 The MAC frame consists of seven bytes of preamble, one byte of the start frame Delimiter and a data frame. The data frame consists of a 48 bit source and destination address, 16 bits of length or type fields, data and a 32 bit CRC field.

The minimum and maximum sizes of the data frames are 64 bytes and 1518 bytes respectively.

Table 9. 1
Format of a Typical CSMA/CD Frame

Preamble	SFD	Destination Address	Source Address	Length Indicator	Data	Frame Check Sequence
7 Bytes	1 Byte	2 or 6 Bytes	2 or 6 Bytes	2 Bytes		4 Bytes

The format of the frame can be briefly described as follows (with reference to each of the fields): The following sequence is followed for the transmission and reception of a frame.

9.2.5. Distributed Network Protocol

The Distributed Network Protocol is a data acquisition protocol used mostly in the electrical and utility industries. It is designed as an open, interoperable and simple protocol specifically for SCADA controls systems. It uses the master/slave polling method to send and receive information, but also employs sub-masters within the same system. The physical layer is generally designed around RS232 (V.24), but it also supports other physical standards such as RS422, RS 485 and even Fiber Optic.

The DNP is well developed as a device protocol within a complete SCADA system. It is designed as a data acquisition protocol with smart devices in mind. These devices can be coupled as a multi-drop fieldbus system. The fieldbus DNP devices are integrated into a software package to become a SCADA system. DNP does not specify a single physical layer for the Serial bus (multi-mode) topology. Devices can be connected by 422 (four wire), 485 (two wire), modem (Bell 202) or with fiber optic cable. The application program can integrate DNP with other protocols if the SCADA software permits. Using tunneling or encapsulation the DNP could be connected to an Intranet or the Internet.

9.2.6. New Technologies in SCADA Systems

A few of the new developments that are occurring in SCADA technology will be briefly listed below. The rapid advances in communications technology are an important driving force in the new SCADA system.

- Rapid Improvement in LAN Technology for Master Stations
- Man Machine Interface
- Remote Terminal Units
- Communications

9.3. Distributed control system (DCS)

SCADA technology has existed since the early sixties and there are now two other competing approaches possible - Distributed control system (DCS) and Programmable logic controller (PLC).

In a DCS, the data acquisition and control functions are performed by a number of distributed microprocessor-based units, situated near to the devices being controlled or, the instrument from which data is being gathered. DCS systems have evolved into providing very sophisticated analogue (e.g. loop) control capability. A closely integrated set of operator interfaces (or man machine interfaces) is provided to allow for easy system configurations and operator control. The data highway is normally capable of high speeds - typically 1 Mbps up to 10 Mbps (see Figure 9.8).

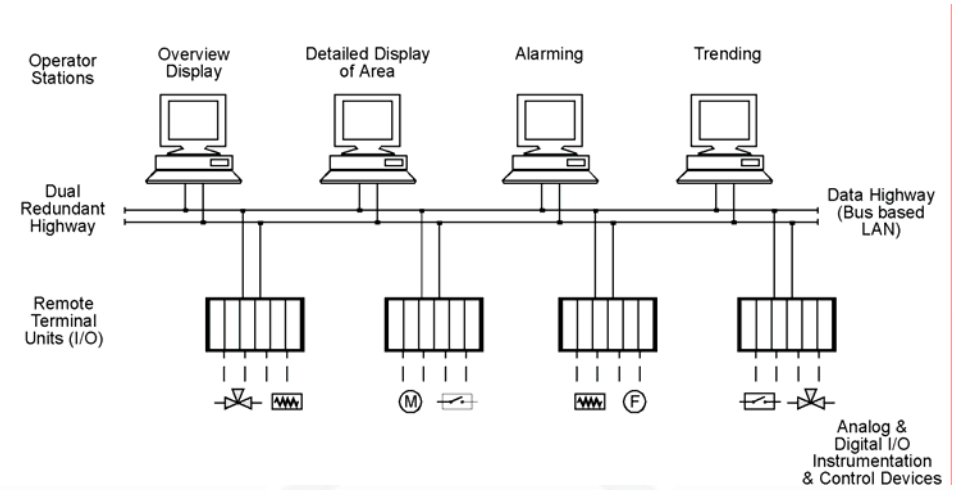

Figure 9.8
Distributed control system (DCS)

9.3.1. DCS versus SCADA terminology

The goals of a DCS (distributed control system) and SCADA (supervisory control and data acquisition system) can be quite different.

A DCS is a process-oriented system and it treats the control of the process, (the chemical plant, refinery or whatever) as its main task, and it presents data to operators as part of its job. On the other hand, a SCADA system is data gathering oriented; and the control center and operators are its focus. Interestingly enough, the remote equipment is merely there to collect the data - though it may also do some very complex process control.

A DCS operator station is intimately connected with its input/output signals (I/O) through local wiring, communication buses (e.g. Field Bus, networks) etc. When the DCS operator wants to see information he/she usually makes a request directly to the field I/O and gets a response. Field events can directly interrupt the system and advise the operator.

A SCADA system must continue to operate when field communications have failed. The 'quality' of data shown to the operator is an important facet of SCADA system operation. SCADA systems often provide special 'event' processing mechanisms to handle conditions that occur between data acquisition periods.

There are many other differences, but they tend to involve a lot of detail. The underlying points are:

- A SCADA system needs to transfer secure data and control signals over a potentially slow, unreliable communications medium, and needs to maintain a database of 'last known good values' for prompt operator display. It frequently needs to do event processing and data quality validation. Redundancy is usually handled in a distributed manner.
- A DCS is always connected to its data source, so it does not need to maintain a database of 'current values'. Redundancy is usually

handled by parallel equipment, not by diffusion of information around a distributed database.

9.3.2. DCS Controller

A DCS controller is a high-performance device capable of handling hundreds of discrete or regulatory control loops per second. The control performance capability of a DCS controller varies from manufacturer to manufacturer. But a user can customize his control configuration to meet the application requirements.

For configuring a DCS controller, it is important to understand the types of controller slots and control functions and algorithms the DCS controller offers.

Control modes: A basic DCS controller has thefollowing operating modes:

- Manual mode
- Automatic mode.
- Cascade mode.
- Backup cascade mode.

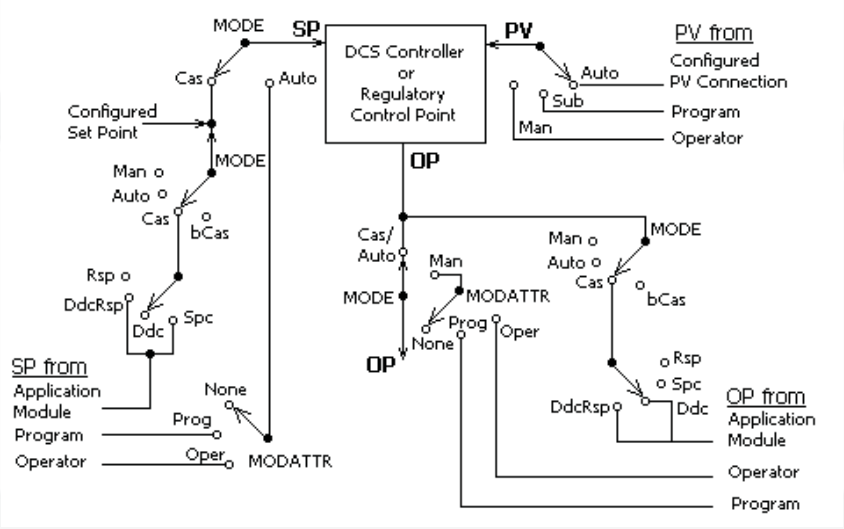

Figure 9.9
Typical mode structure of a basic DCS controller

9.3.3. Control functions

The DCS controller provides a variety of control tools that can be customized to address a wide range of process automation needs.

Functions from I/O scanning through regulatory and logic control to more advanced control strategies can be easily implemented through the DCS advanced controller. Control strategies include; a sophisticated regulatory control package, fully integrated interlock logic functions, and an advanced high level, process engineer-oriented control programming language.

Conceptually, a DCS controller can be thought of as partitioned into ‘slots’ of various types. These slots provide an allocated resource of processing power and money that can be user-configured, including the assignment of a tag name.

A tagged slot is referred to as a 'data point' or 'point' in some DCS systems. Predefined groups, detail displays as well as custom graphics support this data point structure.
Following are some of the different types of data points that can be configured into a DCS controller slot:

- Regulatory PV
- Regulatory control
- Digital composite
- Logic
- Device control
- Array
- Flag
- Numeric
- Timer
- String, etc.

9.3.4. Control algorithms

For different DCS system controllers, different control algorithms are available. Some common control algorithms follow.

- Proportional, integral, derivative (PID): The PID algorithm operates as a 3-mode (proportional, integral and derivative) controller. One can choose from one of the two forms of this algorithm; the interactive (real) form, and the non-interactive (ideal) form.
- PID control algorithm equations for the interactive form
- PID control algorithm equations for the non-interactive form
- PID with feed-forward (PIDFF) control algorithm
- PID with external reset-feedback (PIDERFB)
- Position proportional control algorithm

9.4. Introduction to the PLC

"PLC" means "Programmable Logic Controller". The word "Programmable" differentiates it from the conventional hard-wired relay logic. It can be easily programmed or changed as per the application's requirement. The PLC also surpassed the hazard of changing the wiring.

The PLC as a unit consists of a processor to execute the control action on the field data provided by input and output modules.

In a programming device, the PLC control logic is first developed and then transferred to the PLC.

9.4.1. What can a PLC do?

- It can perform relay-switching tasks.
- It can conduct counting, calculation and comparison of analog process values.
- It offers flexibility to modify the control logic, whenever required, in the shortest time.

- It responds to the changes in process parameters within fractions of seconds.
- It improves the overall control system reliability.
- It is cost effective for controlling complex systems.
- It trouble-shoots more simply and more quickly
- It can be worked with the help of the HMI (Human-Machine Interface) computer

9.4.2. Basic block diagram of the PLC

Figure 9.10 shows the basic block diagram of a common PLC system.

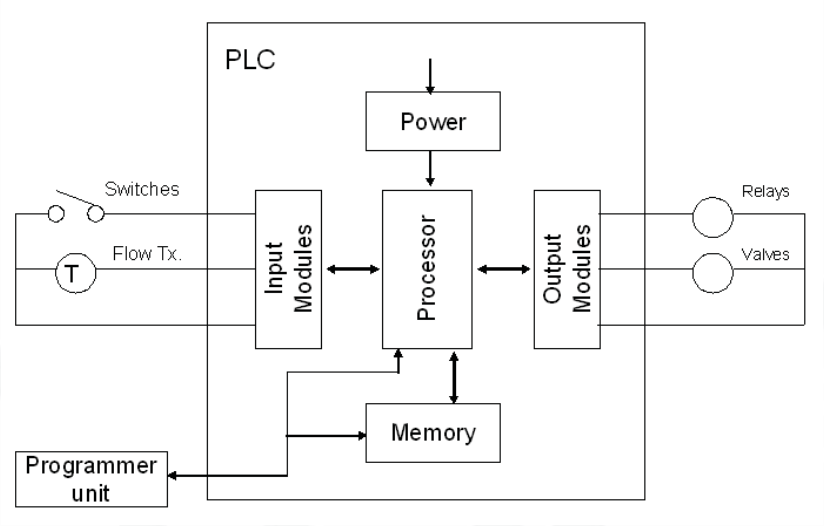

Figure 9.10
Block diagram of a PLC

As shown in the above figure, the heart of the "PLC" in the center, i.e., the Processor or CPU (Central Processing Unit).

- The CPU regulates the PLC program, data storage, and data exchange with I//O modules.
- Input and output modules are the media for data exchange between field devices and CPU. It tells CPU the exact status of field devices and also acts as a tool to control them.
- A programming device is a computer loaded with programming software, which allows a user to create, transfer and make changes in the PLC software.
- Memory provides the storage media for the PLC program as well as for different data.

9.4.3. Size of the PLC system

PLCs are classified on the basis of their size:

- A small system is one with less than 500 analog and digital I/Os.
- A medium system has I/Os ranging from 500 to 5,000.
- A system with over 5,000 I/Os are considered large.

9.4.4. Components of the PLC system

CPU or processor: The main processor (Central Processing Unit or CPU) is a microprocessor-based system that executes the control program after reading the status of field inputs and then sends commands to field outputs.

I/O section: I/O modules act as "Real Data Interface" between field and PLC CPU. The PLC knows the real status of field devices, and controls the field devices by means of the relevant I/O cards.

Programming device: A CPU card can be connected with a programming device through a communication link via a programming port on the CPU.

Operating station: An operating station is commonly used to provide an "Operating Window" to the process. It is usually a separate device (generally a PC), loaded with HMI (Human Machine Software).

9.5. Considerations and benefits of SCADA system

Typical considerations when putting a SCADA system together are:

Overall control requirements

- Sequence logic
- Analog loop control
- Ratio and number of analog to digital points
- Speed of control and data acquisition

Master/Operator control stations

- Type of displays required
- Historical archiving requirements

System consideration

- Reliability/availability
- Speed of communications/update time/system scan rates
- System redundancy
- Expansion capability
- Application software and modeling

Obviously a SCADA system's initial cost has to be justified. A few typical reasons for implementing a SCADA system are:

- Improved operation of the plant or process resulting in savings due to optimization of the system
- Increased productivity of the personnel
- Improved safety of the system due to better information and improved control
- Protection of the plant equipment
- Safeguarding the environment from a failure of the system
- Improved energy savings due to optimization of the plant
- Improved and quicker receipt of data so that clients can be invoiced more quickly and accurately

- Government regulations for safety and metering of gas (for royalties and tax etc).

9.6. An alarm system

In industrial plants and installations, control systems are used to monitor and control processes. Control Systems, whether a conventional Control Desk or a Computer/PLCs System with SCADA or a Distributed Control System (DCS), provides a man-machine-interface to monitor and control the plant equipment and processes.

Alarm Systems are an integral part of man-machine interface. An alarm system consists of both hardware and software including; field signal sensors, transmitters, alarm generators & handlers, alarm processors, alarm displays, annunciator window panels, alarm recorders and printers. Alarm systems indicate the abnormal conditions and problems of the plant and equipment to the operators, enabling them to take corrective action and bring the plant/equipment back to normal conditions. Alarm systems give signals to the operators in the form of audible sound, visual indications in different colors and/or continuous blinking, text messages, etc.

An alarm system brings the following to the notice of the operator:

- problems that need operator attention
- process changes that require corrective action
- unsafe operating conditions before Emergency Shut-down of the plant
- hazardous conditions
- deviations from desired/normal conditions

9.6.1. Functions of the plant or process operator

An alarm system helps/assists the operators in monitoring and controlling the plant, equipment and processes within safe and normal operating conditions. In order to design a suitable alarm system, it is important to understand the functions of the operator who monitors and controls the equipment and processes in the plant.

Generally, the functions of a plant operator are inclusive of the following activities but are not limited to:

- safe and normal operation of plant/equipment
- production at optimum levels
- identification of abnormal, hazardous and unsafe plant/equipment conditions and taking corrective action
- fault identification and communication of faults to maintenance

The above mentioned function and task priorities of a plant operator change with the changing conditions of the plant. For instance:

- during start-up
- when the plant is being stabilized
- when the plant is running under normal conditions
- when the plant is running in abnormal conditions

- when the plant is in emergency shut-down
- when the plant is in planned shut-down,
- when the plant, or sub-section of plant, is in manual mode of operation
- during automatic mode of operation

9.6.2. Functions of an alarm system

The main function of an alarm system is to direct the attention of an operator towards the plant abnormal conditions that need timely assessment and/or timely corrective action(s). An Alarm system alerts, informs and guides an operator regarding an abnormal situation and helps him to take timely corrective action to bring back the plant to normal conditions.

When an abnormal condition arises, the alarm system gives an alarm in the form of an audible warning, flashing or blinking alarm indication and an alarm message. The Alarm gives information about the problem or abnormal condition and its details. In a good alarm system, guidance or help messages on how to respond and take corrections are also provided. An ideal Alarm system also provides feedback on the corrective actions taken by the operator in response to the alarm. Such feedback is generally provided on supplementary display screens that can be accessed by selecting an alarm in the Alarm list.

9.6.3. An effective alarm system

For designing an effective Alarm system, it is important to consider the following key points:

- Present only relevant and useful alarms to the operator
- Each alarm should have a defined response from the operator
- Configure and present only a good alarm
- Allow adequate time for an operator to respond to an alarm

9.6.4. Alarm system design

Designing an alarm system is a process. While designing each alarm it is important to consider how important the alarm is and what its reliability should be. To determine the importance and reliability of an alarm, it is necessary to carry out a qualitative and quantitative risk assessment to consider whether the alarm is safety related and whether it is to be implemented on an independent stand-alone system as opposed to the process control system. Safety related alarms should be given special considerations while designing the man-machine interface.

9.6.5. Assessment of risk

Risk is a measure of the probable rate of occurrence of a hazard and its severity. Risk can be applied to safety hazards, environmental hazards and economic losses.

Alarms are configured and presented to the operator to take corrective action(s) and minimize the sub-optimal operations of the plant/equipment or to protect plant/equipment from damages that can lead to injury to people, damage to environment and/or economic losses. So the design of an alarm system should consider these risks and it must be clearly identified which risk is intended to be reduced by the alarm.

9.6.6. Protection provided by the alarm system

Protection provided by an alarm system can take place in two ways. The operator is warned by the alarm and he/she takes corrective action before the protection operates, or the operator is warned that the protection has failed to operate and he/she takes corrective action.

9.6.7. Safety related alarms

As per the international standard IEC 61508, an alarm system, whether electrical or electronic or programmable, should be considered as safety related only if:

- It is a claimed part of the facilities for reducing the risk(s) from hazards to people to an acceptable or tolerable level, and
- The claimed reduction by the alarm system in the risk(s) is significant. Here the significant reduction means a claimed Average Probability of Failure on Demand (PFDAvg) < 0.1,
- It is designed, operated and maintained as per the requirements defined in the standard,
- It is independent and separate from the process control system, unless the process control system itself has been identified as a safety related system and implemented accordingly.

9.6.8. What is the purpose of an alarm?

(i) It is important to know what the purpose is of the proposed alarm and for what hazards or risks it will provide a warning or an alert to the operator. The consequences of alarm failure or the alarm being missed need to be identified. If the proposed alarm provides only information of an event/incident, then it should not be configured as an alarm.

(ii) Assessment of the severity of the risk in terms of potential loss of life or an injury, economic losses, environmental impact and plant damages must be done. Any hazard to people should be in the form of formal risk assessment for the plant. Economic risks, potential plant damages or losses should be expressed in terms of financial losses.

(iii) Expected frequency of the risk occurrence should be estimated. Though it is difficult to know the accurate chances/frequency of occurrence, it may be appropriate to have some approximate estimate that is more realistic. Appropriate frequency of occurrence may be specified as once a week or once in month, etc.

(iv) Are there any other protection systems in the plant to provide protection against the risk? If not, then it needs to be decided whether or not an automatic protective system can be used with or without configuring the alarm.

(v) Are any reliability claims made in the plant, in terms of safety and protection, provided by the alarm? Do these reliability claims require the alarm to be classified as a safety related alarm? If an alarm is not safety related, then what are the economic and/or environmental risks involved in implementing the alarm within the process control system?

(vi) It is important to know the implications of alarm failure due to alarm sensor/instrument failure. How then can these failures be detected and can the alarm signal be validated. Should the alarm sensor/instrument be made redundant?

(vii) How effective will the operator response to the alarm be? If the operator cannot take any corrective or preventive action to prevent the risk, then the alarm hardly provides any benefit and should not be configured as an alarm.

9.6.9. Operator response

(i) What should the response of the operator be to the alarm? The response may be an action, a conditional action or only a cognitive switch. The response must be clearly defined for each alarm.

(ii) The alarm message should be easy to read and understand.

(iii) If required, additional displays should be developed that provide the operator with information to help him decide how to respond in different conditions of the plant.

(iv) How long will the operator take to respond to the alarm and how long will the plant take to respond to the corrective action(s) taken by the operator?

(v) Procedure for Alarm response should be prepared and provided to the operators.

9.6.10. Alarm prioritization

(i) The likely safety, economic and environmental consequences of the operator not responding to the alarm should be assessed.

(ii) Identify whether the alarm is time critical and what time is available for the operator to respond to the alarm.

(iii) Depending on the severity of safety, economic and environmental consequences of missing the alarm and/or not responding to a time critical alarm and how fast the operator is required to respond to the alarm, priority should be allocated to the alarm.

(iv) It should be determined whether it will be required to change the priority of the alarm depending on changes in the operating conditions.

9.6.11. Alarm settings

(i) What is the normal range for the alarmed process variable? What should be the alarm settings for alarming the safety hazard, and/or economic losses and/or environmental damages?

(ii) How many alarms should be set for the process variable – Low, Low-Low, High, High-High and what should the settings be for these alarms?

(iii) Is there a need for changing the alarm setting depending on plant operating conditions?

(iv) During normal plant operation, what are the fluctuations in the process variable to be alarmed?

9.6.12. Alarm suppression

(i) If the alarm is likely to be generated during large disturbance/upset in the plant or during plant trips, then the alarm should be suppressed using a suitable logic.

(ii) If other alarms, having more significance, occur, the alarm should be suppressed?

(iii) Are there any conditions during which the process variable will cross the alarm setting but where no risk is involved?

(iv) What signals should be used for logical suppression of the alarm?

(v) What are the chances of the process variable going out of range or being invalid? How will it affect the alarm? Will it create a nuisance (repeating) alarm? How should such situations be made known to the operator, or how can plant/equipment trip be avoided if the process variable alarm limit/Flag is used for plant/equipment interlock?