TELEMETRY & SCADA SYSTEM IN GAS PIPELINES- PROBLEMS AND SOLUTIONS

A Project Report submitted in partial fulfillment of the requirements for the Degree of

MASTER OF TECHNOLOGY
in
GAS ENGINEERING
(Academic Session 2003-05)

By
Gaurav Tayal

Under the Supervision of
Dr. B. P. Pandey

COLLEGE OF ENGINEERING STUDIES
UNIVERSITY OF PETROLEUM & ENERGY STUDIES
DEHRADUN (U.A) 248007
May 2005

CERTIFICATE

This is to certify that the Project Report on *"Telemetry & SCADA System in Gas Pipe Lines- Problems and Solutions"* submitted to University of Petroleum & Energy Studies, Dehradun, by **Mr. Gaurav Tayal,** in partial fulfillment of the requirement for the award of Degree of Master of Technology in Gas Engineering (Academic Session 2003-05) is a bonafide work carried out by him under my supervision and guidance. This work has not been submitted anywhere else for any other degree or diploma.

Date: May 23, 05

Dr.B.P.Pandey

ACKNOWLEDGEMENT

The project report, which the reader has in his hands, is the essence of blessings of elders, cooperation and support of many people and friends. In the sequel that follows, some names may be mentioned and some may be not, but their contribution has all been of great importance.

I am thankful to **Dr. B.P. Pandey**, Dean, College of Engineering, UPES, Dehradun (UA) for all the help, encouragement, valuable suggestions and parental attitude and guidance.

I wish to express my sincere gratitude to **Dr. Himmat Singh**, Distinguished Professor, UPES, Dehradun for his able guidance and for his encouragement, inspiration and understanding without which this work would not have been in its present form.

I owe special thanks to **Mr. Kamal Bansal**, Senior Lecturer, UPES, Dehradun for his valuable suggestion and encouraging comments during the entire tenure of the project work. It was for his co-operation and critical comments without which I would have missed many things in my project.

Sincere thanks are due to the management **of Indraprastha Gas Limited, New Delhi** for providing me the necessary inputs. I appreciate their helping attitude and cooperation extended to me.

Sincere thanks are due to the management of **Oil and Natural Gas Corporation, Dehradun** for allowing me to excess their library and providing me the valuable subject material.

I am also very thankful to **my parents** for supporting me at every step and showing confidence in me.

Gaurav Tayal

Gaurav Tayal

CONTENTS

EXECUTIVE SUMMARY

Gas companies have been using computers to handle data acquisition, pipeline control, billings and other tasks since the 1960s. Over the years, computers and associated equipment used for such purposes have become categorized as Supervisory Control and Data Acquisition systems (SCADA).

SCADA systems in the mid-1970s were limited in the amount of data acquisition and control possible, because the facilities for transmitting to and from various points in the gas supply system, from gate stations to meters at customers sites were somewhat primitive. Then, escalating gas prices, gas supply security, spot-market purchases, and increasing attention from regulatory agencies made it essential that gas companies use computers to handle the increased need for information and for more advanced control.

Today's modern remote terminal units are able to provide local signal conditioning, perform calibration and diagnostics, compute running totals, control local valves, detect alarm conditions and communicate with a host computer.

If implemented, rules providing "right of access" will allow large consumers to buy gas from any suppliers and have the gas delivered by the local distributor, as the trend to spot-market purchases have generated new tracking, accounting and billing requirements.

Any gas utility that has to participate in this process must be able to handle increased bookkeeping requirements, in particular when a pipeline open-access transmission program is implemented. Keeping track of gas consumption by large consumers and calculating the correct charges is a serious issue. For example, if a customer takes more or less than the contracted amount of gas, the discrepancy can affect the transmission system, the customer or the gas distributor can incur take-or-pay penalties from the gas suppliers, the gas distributor can overcharge or undercharge the customer.

A modern SCADA system constantly monitors incoming gas at gate stations and deliveries to customers, so it contains all the data needed to track gas being transported and to perform the accounting functions and correct billing.

The system permits the gas dispatcher to enter nominations for transportation orders as soon as they are received from a customer, asking for the information – such as injection point, flow rate/day, delivery point, contract dates – needed to track the incoming gas on the dates specified, and bill accordingly for transportation and reservation costs. Before accepting the nomination, the system checks to make sure the pipeline can accommodate the order, and that the order will not affect the existing orders. For this purpose, and in order to avoid discrimination charges, the system has to be able to document the over-capacity situation. On the dates indicated, the system makes sure the customer takes the ordered amount.

Due to its multiple functions, a SCADA system has thus important qualitative impacts on safety security, gas supply security, metering and billing, operating and managing effectiveness, and consequently a real impact on related costs.

Gas pipelines are operated with a three-fold objective of ensuring safety of persons and property, reliability of service and cost-effectiveness. Operations are monitored and controlled by use of SCADA systems that provide thousands of data to pipeline controllers and operators. Some data are provided at intervals of a few seconds, other data are provided at intervals of a few minutes and still others on an hourly or daily basis.
Operational data include pipeline pressure, flow rate, gas composition, and equipment status. Maintaining appropriate pressures in the pipeline is essential to ensure safety, maximize throughput and provide reliability of service. Flow rates are determined on the basis of energy as well as volume and are used to balance system demands and supplies. Gas composition is required to maintain appropriate combustion characteristics, screen for undesirable contaminants, and balance gas transmission on a thermal basis. Equipment status, such as valve position and compressor information, is used to confirm that the system is configured to meet operational objectives.
Understanding the basics of telemetry and how it applies to pipeline supervisory control and data acquisition (SCADA) systems can help personnel increase their productivity.

This report contains the concepts of Telemetry & SCADA and its application in the oil and gas industry. It also highlights on the general problems which occurs in SCADA operations. At last, inputs from Indraprastha Gas Limited, New Delhi are taken and a proposed scheme is suggested which include- ladder logic, line diagram, main menu screen, alarm screen, history screen, report generation screen and trend screen. With more number of inputs (analog & digital), more parameters can be monitored and shown.

CHAPTER 1

"Background of Telemetry & SCADA in the pipeline remote-control process"

What is telemetry? What is SCADA? Answers to these questions, in some detail, should help everyone in operations and maintenance paint a more vivid "big picture" of what they are striving to accomplish every day.

Telemetry can be defined as the process in which data from a measured device is being transmitted to a distant location by any of a variety of media, such as radio and telephone.

SCADA is an acronym that stands for supervisory control and data acquisition. A supervisory control system has the ability and intelligence to perform controls with minimal supervision. A data acquisition system has the ability to gather data.

SCADA systems are specialized systems used to monitor and control remote facilities. They commonly are used in the gas, oil, electric and water transmission and distribution industries where facilities are stretched out over a large area. A SCADA system can be divided into the following essential areas:

- Sensors and actuators
- Remote terminal units (RTUs)
- Communications
- Host central computer systems
- User interface.

Sensors and Actuators: A SCADA system's ultimate purpose is to monitor and control facilities. There are various devices that provide the interface between the system and the outside world. These devices can be divided into two categories:

- Sensors convert external data into input signals that can be used by the SCADA system (Figure1.1)

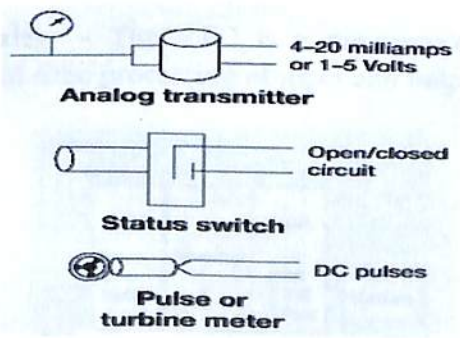


Figure 1.1: Sensors, which convert a deterministic value into a signal that can be understood by a remote terminal unit (RTU) come in three types.

- Actuators take signals from the SCADA system and convert them into control actions.

The sensor provides the means of converting a deterministic value into a signal that can be understood by the RTU. The signals can be any of three types:

- Analog input provides a representation of a measured variable, such as temperature, flowrate and pressure
- Status (or digital) input provides a logical, true or false, representation of data
- Pulse input, usually a frequency signal proportional to some measured variable.

Transmitters, which are an example of sensors that provide an analog input signal to the RTU, usually do so by means of a 4-20 milliamperes (Ma) current loop signal. The transmitter will act as a regulator of a current source provided by the RTU, varying the current in proportion to the variable the transmitter is measuring, such as pressure.

Sensors that provide a digital signal to the RTU usually are switches that will convert a physical status into a contact closure, or relays that will convert an electrical signal into a contact closure. The contact closure serves as the means of providing the RTU with a logical, true / false representation of the signal.Other sensors are capable of providing signals that are processed as pulse inputs in the RTU. Pulse inputs are either electronic pulses or contact closure signals with a frequency proportional to the measured variable. Pulses are used to represent an incremental measurement, for example, one pulse = 100 Mcf flowrate.

Actuators or output devices can be driven by any of three signal types from the RTU:

- Analog actuators use an RTU analog output signal to control variables such as flowrate and pressure
- Digital outputs are useful for absolute actions, such as opening a valve or launching a pig
- Pulse outputs often are used as a hand-off signal to other RTUs or controllers. There is no hardware calibration required between the devices.

Remote Terminal Units: - The RTU is a microprocessor-based unit which is specifically designed for real-time processing of input and output data (**Figure1.2**).

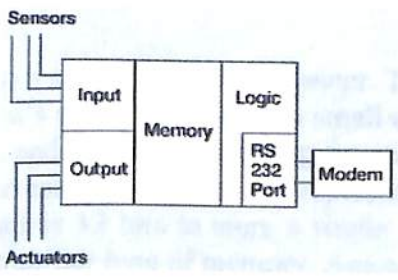


Figure1.2: Block diagram of a typical remote terminal unit (RTU)

On the RTUs input side, the sensor is connected to circuitry which, depending on the signal, converts it into a digital representation for further processing by the RTU logic.

Similarly, the output circuitry will convert a digital representation of data into a signal that can be understood by an associated actuator. The digital representation referred to here is a value in a specific memory location within the RTU. Each I/O point will have a memory location associated with it.

In the case of analog input signal processing, the sensor is connected to an analog input circuit that runs the current loop through a 250-ohm, high-precision resistor (Figure1.3).

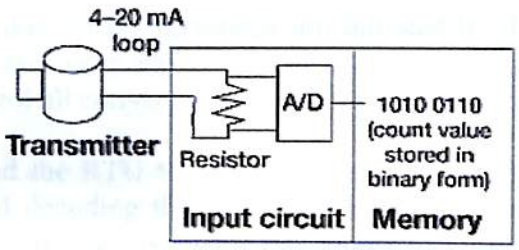


Figure1.3: In analog input signal conversion, the electrical current loop runs through a high-precision resistor where the change in voltage across the resistor indicates the current flow (4-to-20 Ma)

The resistor, according to Ohm's Law, creates a voltage drop proportional to the amount of current. An analog-to-digital (A/D) converter reads the voltage across the resistor, and produces a digital "count". The value of the count depends on:

- Voltage read by the converter
- Resolution.

An A/D converter's resolution is described by the number of bits it uses to produce a value. For a 12-bit A/D converter, the range would be zero to 4096 counts. RTU software typically uses a non-zero count to represent zero percent (4 Ma) current input, so that under-ranging or loop failures can be detected. The RTU software logic will then process the digital value and scale it, such as converting it into engineering units, for use in equations and / or storage.

Digital inputs are processed in a slightly different manner. The status of a digital input is determined by the input device's ability to conduct a small current. Normally the contact is open, no current is flowing, and the bit representing the status input is set to zero. If the contact is closed, there is current flow and the bit representing the input is set to one. Whereas an analog input requires 12 bits to store a single value, a digital input can be stored in a single bit, eight inputs per byte of memory. Again, the RTU software logic can process the input states by accessing them from a memory location.

The pulse input processing circuitry has a memory variable associated with it that is incremented by a value of one each time a pulse is sensed, usually a toggle of a status input. This memory variable is called an accumulator, since it accumulates a pulse count. The input circuitry alone does not determine the frequency of the pulses, it simply will increment the accumulator. Again, the RTU software logic can use the accumulated value by accessing it from memory.

Communications: - This area of a SCADA system can be looked at as the data transport mechanism between the host computer system and the RTU.

The host can communicate with the RTU via a variety of media, including microwave, dedicated telephone leased lines, dial telephone, radio and satellite. Regardless of the communications method, SCADA systems usually use a communications format referred to as master-slave, meaning all conversations are initiated by the master host computer system. The RTU, or slave, only replies when it sees a message with its address. The master is the one to control all conversations on a communications channel.

In order for the host and the RTU to understand each other, there must be a common method of encoding and decoding the messages transmitted between the devices. The technique a SCADA system uses is called the communications protocol. The protocol typically includes information such as the RTUs address, the data type requested, and the location and amount of data to be transmitted or received (**Figure1.4**).

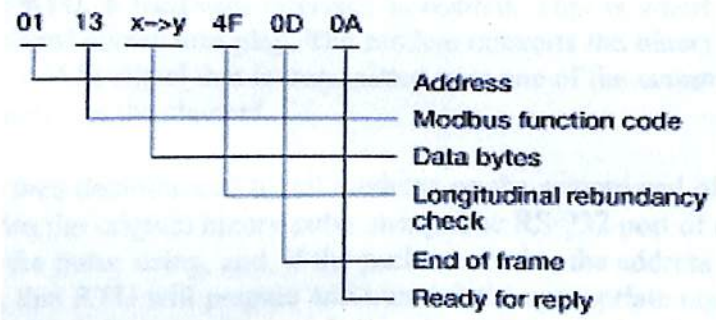


Figure1.4: Modbus ASCII protocol data packet

In addition, virtually all protocols use security of some kind to ensure message integrity. Some host systems and RTUs may support more than one protocol, and can support multiple protocols on a single communications channel.

When the host system determines that a particular data point is needed, it constructs a packet of data (according to the protocol's rules) and sends it out the appropriate serial port. Conforming to the Electronic Industries Alliance (EIA) RS-232 specification, the data stream leaves the host computer as a sequence of pulses greater than +3 (binary zero) or less than –3 volts (binary 1) (Figure1.5).

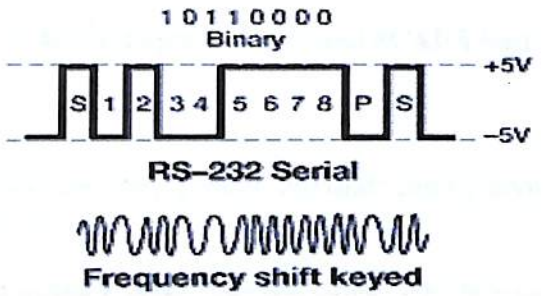


Figure1.5: Data signal encoding showing the binary pulse stream and the corresponding frequency-modulated audio frequency signal

The RS-232 interface is only good for a distance of 50 ft, direct connect. Therefore, to get the signal to the RTU, a hardware interface is needed. This is where the modulator / demodulator (modem) comes into play. The modem converts the binary pulse string into an audio frequency (AF) signal that is transmitted over one of the communications media circuits to the remotes on the channel.

The AF signal is then demodulated by all modems on the remote end of the channel and converted back into the original binary pulse string. The RS-232 port of each RTU on the channel receives the pulse string, and, if the packet contains the address of any RTU that received the poll, that RTU will prepare and transmit the appropriate response. When the response is transmitted, both the host and the other RTUs on the channel can hear the transmission. However, because of the protocol definition, the other RTUs will ignore the transmission.

Host system: - The host is the heart of the SCADA system. This is not only because it is the master in the master / slave relationship already mentioned, but because it controls all data flow throughout the network (Figure1.6).

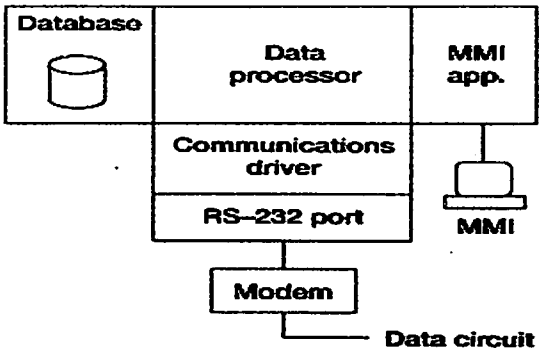


Figure1.6: Block diagram of a typical SCADA host system.

While host system internals can vary greatly, internals can be divided into four functional parts for discussion purposes:

- First, and most important, is the data processor, which is central to the system
- Communications interface
- Database
- Man-machine interface (MMI), also called human-machine interface (HMI), graphic-user interface (GUI), or user interface.

Data processor: - is the system "traffic cop." It is responsible for the routine acquisition of data from RTUs on a scheduled basis, servicing user requests for database access, and activities such as control commands and downloading of parameters.

Communications interface: - is where the protocol drivers reside. This interface formats data requests from the data processor, routes them to the appropriate communications channel for transmission to the RTU, processes the expected replies, and hands the data back to the data processor. Since the communications drivers reside in this area, the system can be designed to utilize multiple drivers for multiple protocols while leaving the data processor essentially "generic." This architecture makes it easy to add new protocols.

Database: - is the repository for all collected data, and contains spot data (or real-time), as well as historical data and calculated data. It is common today to have the RTUs store historical data on site. The RTU-generated historical data, when collected by the host, can be stored directly into the historical database.

For performance reasons, most SCADA database designs keep current scan values in a memory-resident database. This provides optimum access speeds for operators monitoring the data. On the other hand, historical data are stored on disk. The sheer volume makes this necessary, and the less-critical need for instantaneous access makes it acceptable.

MMI, or user interface: - provides the operator with access to the system. The most common access is via a video display, along with a keyboard and a pointing device. Most systems provide some form of graphical display capabilities with high resolution and bit-mapped graphics.

Traditionally, MMI software ran on the same host hardware as the data processor and the database. The application was accessed via a "smart" cathode-ray tube (CRT) terminal connected to a serial RS-232 communications channel. The graphic displays also resided on the host hardware. However, this arrangement limited the number of terminals connected to the SCADA system.

Today, the trend is to separate this functionality and to use relatively low-cost workstations to handle the ever-increasing resources demanded by more sophisticated graphics applications. This philosophy, known as client-server technology, separates areas of a host system into stand-alone systems connected via a network.

In the client-server philosophy, when an operator calls up a particular display, the "background," or the display's static portion, is generated locally by the MMI workstation, not by the SCADA host. At the same time, the workstation generates a dynamic data request that is sent over the network to the host. The appropriate system responds with the required data elements from the database and the MMI workstation displays the dynamic data along with the static portion of the display.

Step-by-step:- Following a signal through the typical SCADA system from one end to the other will illustrate the material discussed above (Figure1.7).

	Zero	Intermediate value	Full scale
Psig	0	750	1000
Milliamps	4	16	20
Volts	1	4	5
Counts	4	3004	4004
Binary	0000 0000 0100	1011 1011 1100	1111 1010 0100

Figure1.7: Signal value at various points in the typical SCADA system.

The walk-through begins at an analog pressure transmitter measuring a gas pipeline's pressure. The pressure in this example will be 750 psi with the transmitter's 4-to-20 Ma calibrated zero to 1,000 psi. The sensor (analog transmitter) will convert the 750 psi pressure into a 16-Ma input signal to the RTU. As this signal passes through the 250-ohms resistor in the RTUs A/D converter, it undergoes a drop in potential to four volts. The RTUs 12-bit A/D converter has been calibrated four to 4004 to take into account

over and under-ranging. The four volts input signal at this point translates into 3004 counts and is stored in the RTUs database as a raw input value.

RTU software logic, using parametric data stored in the database, converts the raw value (3004 counts) into the engineering unit value of 750 and once again, stores the value in the database. At this point, the RTU has in memory a raw value and a calculated value for the 750 psi signal.

The host system's data processor determines that it is time to poll for this particular pressure value and sends a request to the communications interface. The communication driver constructs a data packet containing the address of the RTU, the memory location of the data value, and the number of points requested (one).

For security, the cyclic redundancy check (CRC) algorithm generates a unique two-byte security code that is appended to the packet. The driver transmits the assembled packet to the modem via the appropriate RS-232 serial port. The modem converts the packet from a digital signal into an analog signal with frequency shifts corresponding to the change in the value. The host modem and the RTU modem are now connected via communications media as previously discussed.

At the RTU, the modem translates the frequency shifts (analog signal) back into a digital signal which passes into the RS-232 port of the RTU. Software logic in the RTU uses the same CRC algorithm to calculate security for the message, and compares it to the inbound attached CRC. If security matches, and the address is recognized, the RTU processes the request.

The RTU responds by assembling the data value (750 psi) together with the associated protocol-specific information into the response packet. The RTU transmits the response packet back to the host.

The host communications interface decodes the packet. Having passed all security checks, the packet is handed off to the data processor. The data processor checks the value against alarm limits, notifies the operator if the point is in alarm, and stores it in the database along with an alarm flag, if applicable.

Once the data are in the database, the operator's display (MMI), which is updated at periodic intervals, will reflect the new value. Also, the MMI will display any alarm conditions associated with the data values. What was a pneumatic-pressure telemeter point at a remote sensor a moment ago is now at the operator's console?

CHAPTER 2

"SCADA Systems, Hardware and Firmware"

2.1 Introduction

This chapter introduces the concept of a telemetry system and examines the fundamentals of telemetry systems. The terms SCADA, distributed control system (DCS), programmable logic controller (PLC), smart instrument are defined and placed in the context used in this manual.
The chapter is broken up into the following sections:

Definitions of the terms SCADA, DCS, PLC and smart instrument. Remote terminal unit (RTU) structure

- PLCs used as RTUs
- Control site/master station structure
- System reliability and availability
- Communication architectures and philosophies
- Typical considerations in configuration of a master station

The next chapter, which concentrates on the specific details of SCADA systems such as the master station software, communication protocols and other specialized topics will build on the material, contained in this chapter. As discussed in the earlier chapter, the word telemetry refers to the transfer of remote measurement data to a central control station over a communications link. This measurement data is normally collected in real-time (but not necessarily transferred in real, time). The terms SCADA, DCS, PLC and smart instrument are all applications of Telemetry concept.

2.2 Comparison of the terms SCADA, DCS, PLC and smart instrument

2.2.1 SCADA system

A SCADA (or supervisory control and data acquisition) system means a system consisting of a number of remote terminal units (or RTUs) collecting field data connected 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.

The accurate and timely data (normally real-time) allows for optimization of the operation of the plant and process. A further benefit is more efficient, reliable and most importantly, safer operations. This all results in a lower cost of operation compared to earlier non-automated systems.

There is a fair degree of confusion between the definition of SCADA systems and process control system. SCADA has the connotation of remote or distant operation. The inevitable question is how far 'remote' is - typically this means over a distance such that the distance between the controlling location and the controlled location is such that direct-wire control is impractical (i.e. a communication link is a critical component of the system).

A successful SCADA installation depends on utilizing proven and reliable technology, with adequate and comprehensive training of all personnel in the operation of the system.

There is a history of unsuccessful SCADA systems - contributing factors to these systems includes inadequate integration of the various components of the system, unnecessary complexity in the system, unreliable hardware and unproven software. Today hardware reliability is less of a problem, but the increasing software complexity is producing new challenges. It should be noted in passing that many operators judge a SCADA system not only by the smooth performance of the RTUs, communication links and the master station (all falling under the umbrella of SCADA system) but also the field devices (both transducers and control devices), The field devices however fall outside the scope of SCADA in this manual and will not be discussed further. A diagram of a typical SCADA system is given opposite.

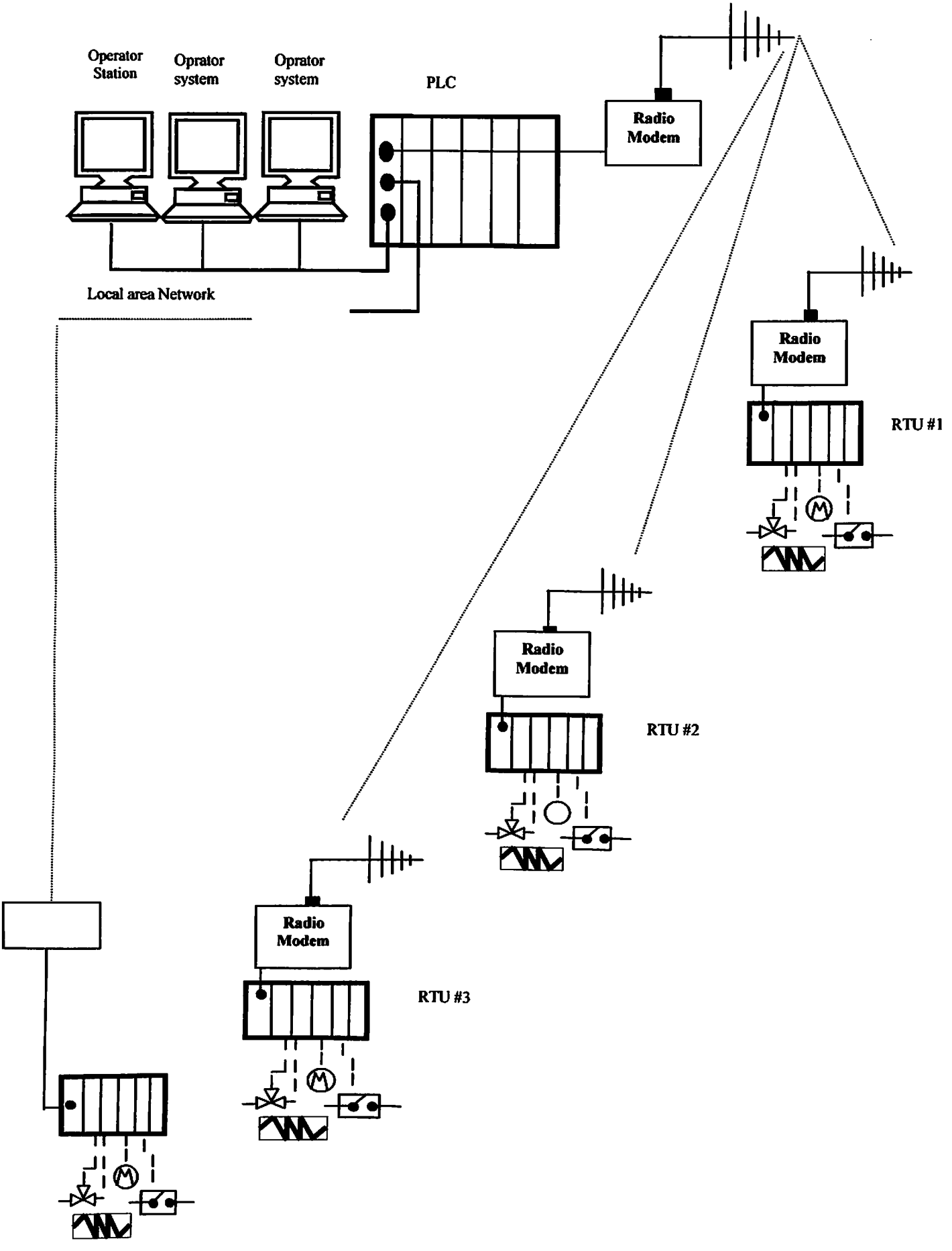


Figure 2.1: Typical SCADA system

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

The RTU provides an interface to the field analog and digital signals situated at each remote site.

The communications system provides the pathway for communications between the master station and the remote sites. This communication system can be radio, telephone line, microwave and possibly even satellite. Specific protocols and error detection philosophies are used for efficient and optimum transfer of data.

The master station (and submasters) gather data from the various RTUs and generally provide an operator interface for display of information and control of the remote sites. In large telemetry systems, submaster sites gather information from remote sites and act as a relay back to the control master station.

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 addition there has been a growing trend to use smart instruments as a key component in all these systems. Of course, in the real world, the designer will mix and match the four approaches to produce an effective system matching his/her application.

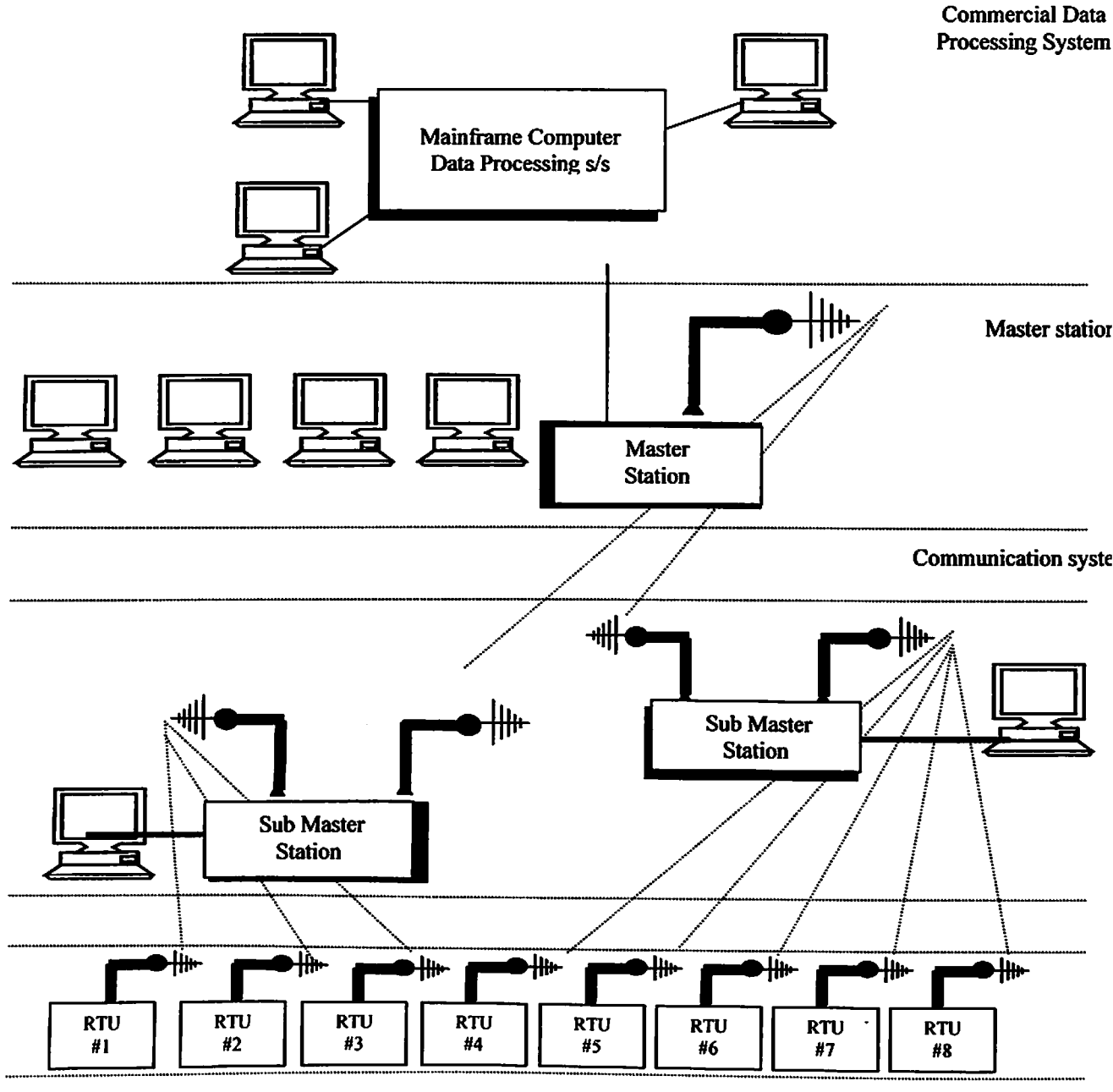


Figure 2.2 SCADA System

2.2.2 Distributed control system (DCS)

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 systems providing very sophisticated analog (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 fairly high speeds (typically I Mbps up to l0 Mbps).

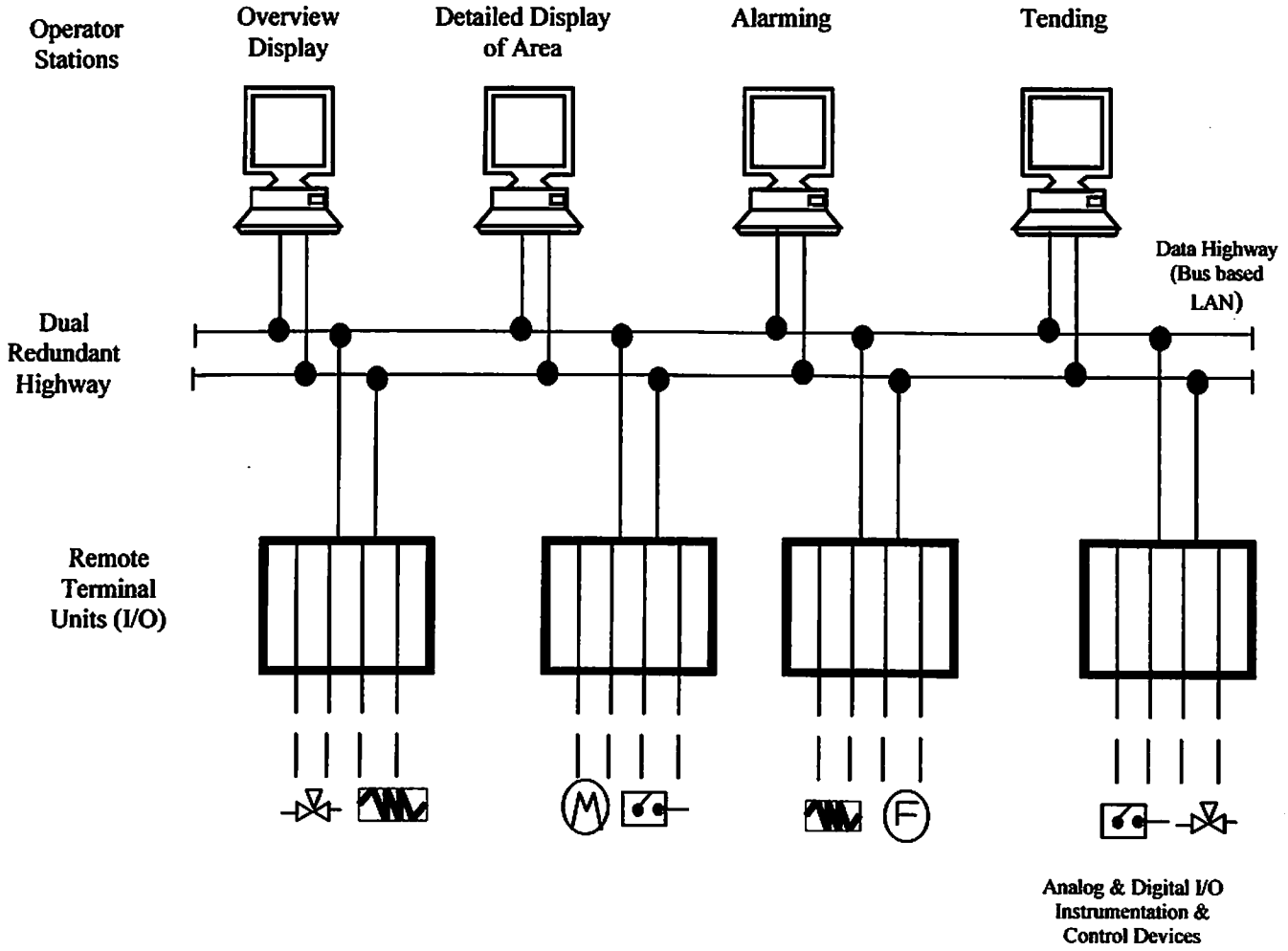


Figure 2.3: Distributed Control System

2.2.3 Programmable logic controller (PLC)

Since the late 1970s, PLCs have replaced hardwired relays with a combination of ladder logic software and solid state electronic input and output modules. They are often used in the implementation of a SCADA RTU as they offer a standard hardware solution, which is very economically priced.

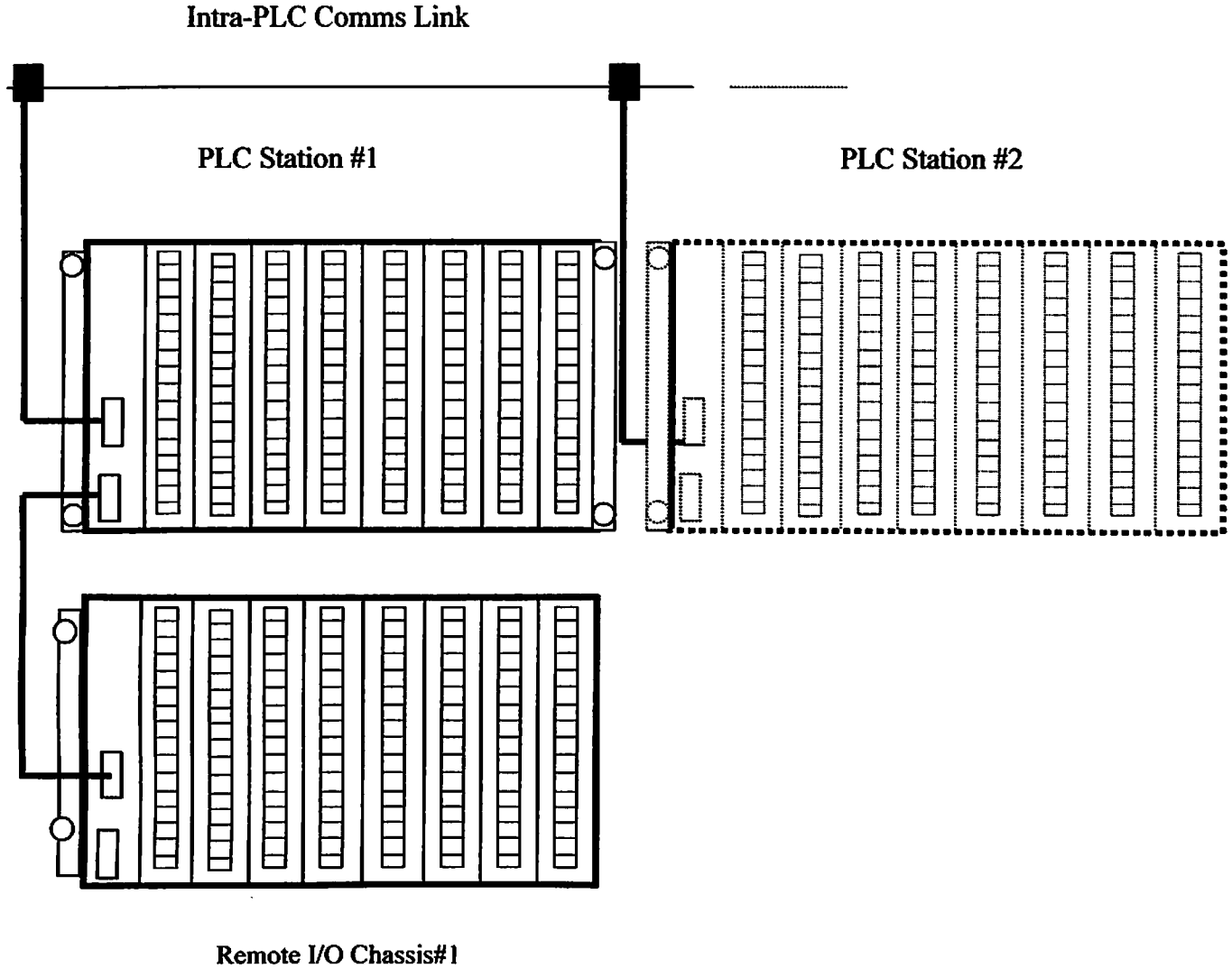


Figure 2.4: Programmable Logic Controller(PLC)System

Another device that should be mentioned *for* completeness is the smart instrument which both PLCs and DCS systems can interface to.

2.2.4 Smart Instrument

Although this term is sometimes misused, it typically means an intelligent (microprocessor based) digital measuring sensor (such as a flow meter) with digital data] communications provided to some diagnostic panel or computer based system.

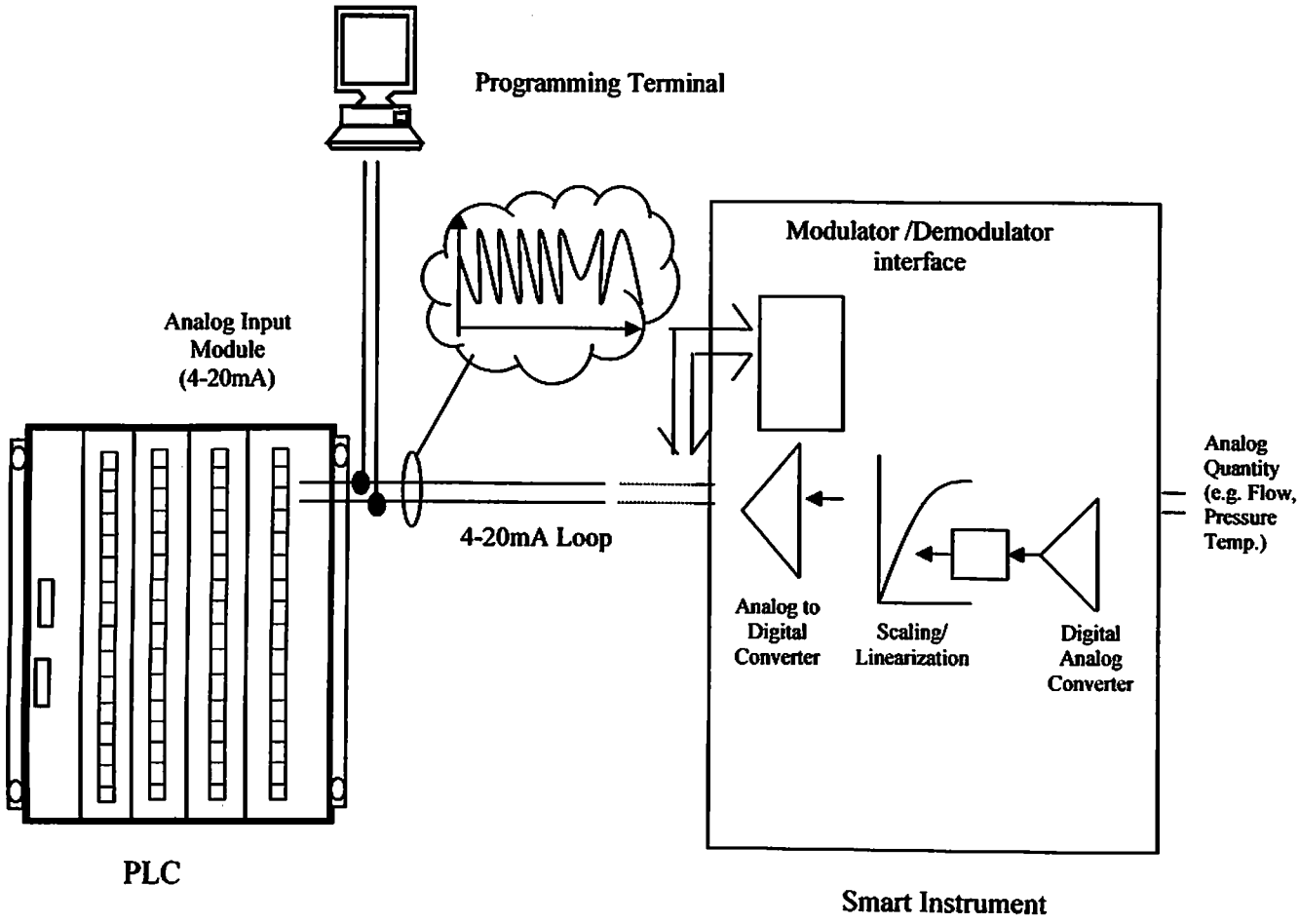


Figure 2.5: Typical example of Smart Instrument

2.2.5 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 requirements
- 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 & tax etc)

2.3 Remote terminal units

An RTU (sometimes referred to as a remote telemetry unit) as the title implies, is a standalone data acquisition and control unit, generally microprocessor based, which monitors and controls equipment at some remote location from the central station. Its primary task is to control and acquire data from process equipment at the remote location and to transfer this data back to a central station. It generally also has the facility for having its configuration and control programs dynamically downloaded from some central station. There is also a facility to be configured locally by some R TU programming unit. Although traditionally the RTU communicates back to some central station, it is also possible to communicate on a peer-to-peer basis with other RTUs. The RTU can also act as a relay station (sometimes referred to as a store and forward station) to another RTU, which may not be accessible from the central station.

Small sized RTUs generally has less than 10 to 20 analog and digital signals, medium sized RTUs have 100 digital and 30to 40 analog inputs. RTUs, having a capacity greater than this can be classified as large.

A typical RTU configuration is shown in Figure 2.6

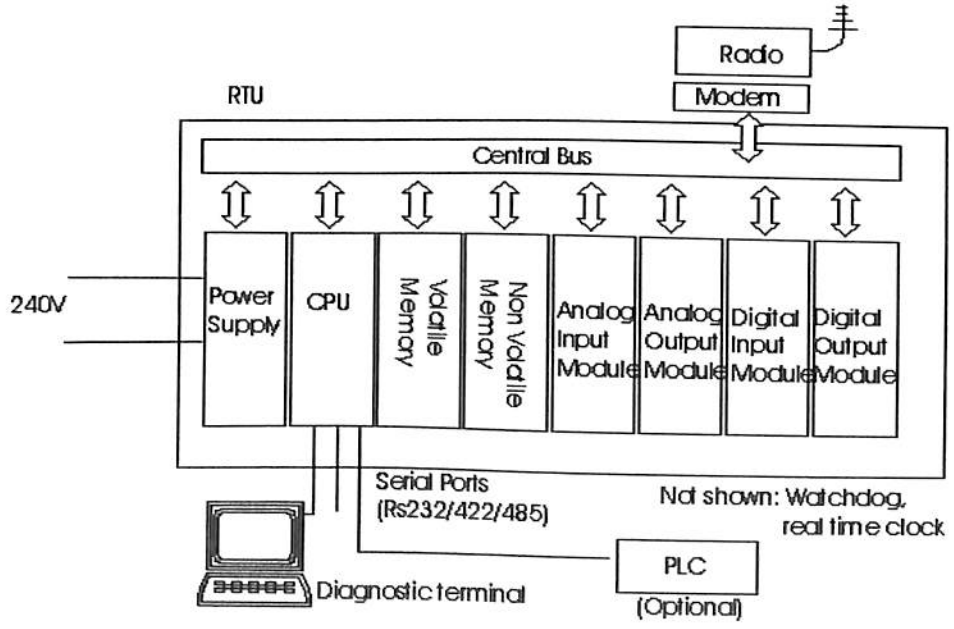


Figure 2.6: Typical RTU Hardware Structure

Typical RTU hardware modules include:

- Control processor and associated memory.
- Analog inputs.
- Analog outputs
- Counter inputs
- Digital inputs
- Digital outputs
- Communication interface(s)
- Power supply

2.3.1 Typical Analog Input Module:

This is shown in the figure below:

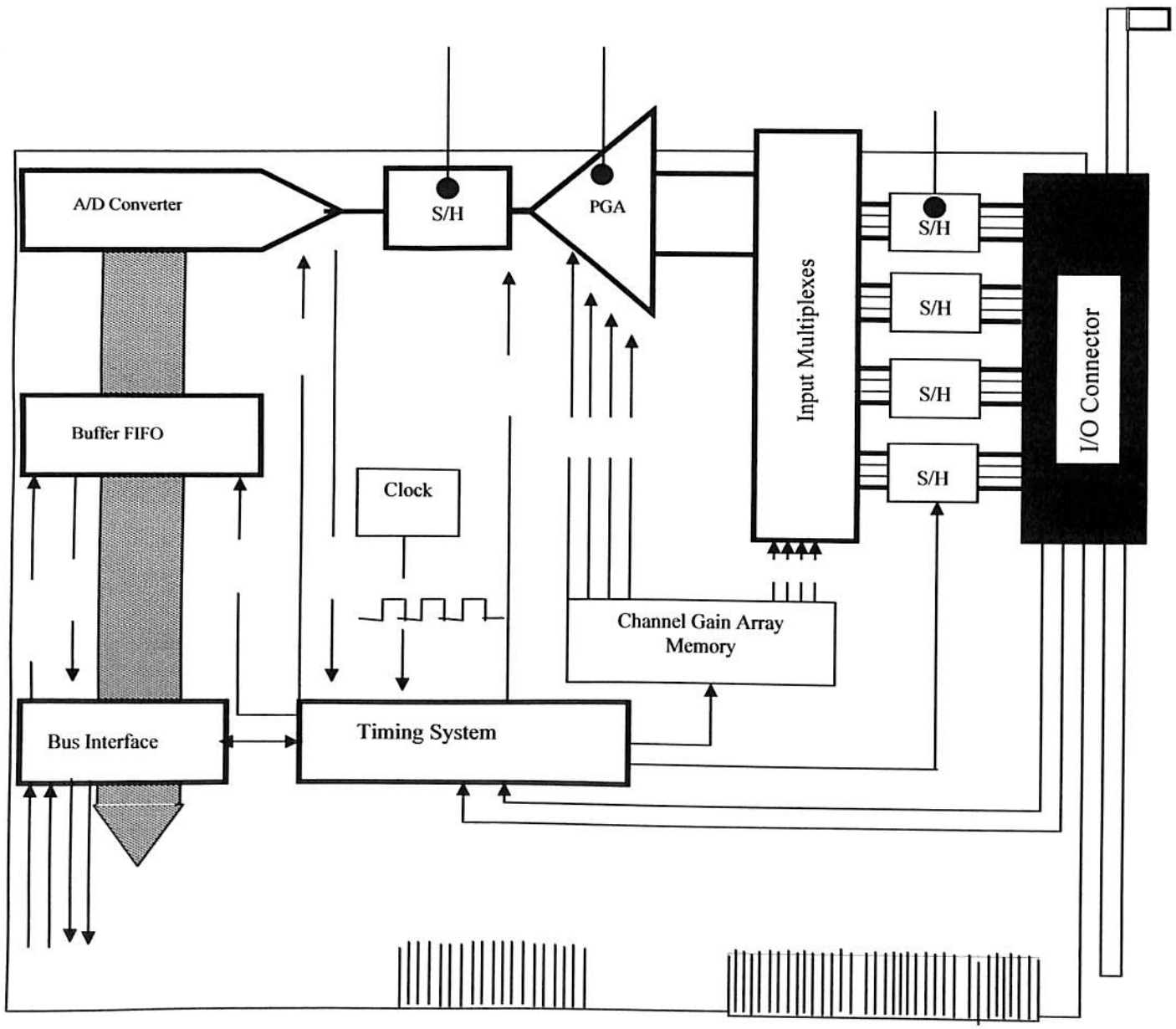


Figure2.7 : Block Diagram of a typical analog input module

These have various numbers of inputs. Typically they are:

- 8 or 16 analog inputs
- Resolution of 8 or 12 bits.
- Range of 4-20 mA (other possibilities are 0-20mA/+10volts/0-10volts)
- Conversion rates typically 10 microseconds to 30 milliseconds
- Inputs are generally single ended (but also differential modes provided)
- Input resistance typically 240 k-ohm to 1 M-ohm.

For reasons of cost and minimization of data transferred over a radio link, a common configuration is eight single ended 8-bit points reading 0-10 volts with a conversion rate of 30 milliseconds per analog point.

An important but often neglected issue with analog input boards is the need for sampling of a signal at the correct frequency. The Nyquist criterion states that a signal must be sampled at a minimum of two times its highest component frequency. Hence the analog to digital system must be capable of sampling at a sufficiently high rate to be well outside the maximum frequency of the input signal. Otherwise filtering must be employed to reduce the input frequency components to an acceptable level. This issue is often neglected due to the increased cost of installing filtering with erroneous results in the measured values. It should be realized the software filtering is not a substitute for an inadequate hardware filtering or sampling rate. This may smooth the signal but it does not reproduce the analog signal faithfully' in a digital format.

2.3.2 Typical analogue output module

Typically the analogue output module has the following features:

- 8 analogue outputs
- Resolution of 8 or 12 bits
- Conversion rate from 10 II seconds to 30 milliseconds
- Outputs ranging from 4-20 mA/± 10 volts/0 to 10 volts

Care has to be taken here on ensuring the load resistance is not lower than specified (typically 50 k ohm) or the voltage drop will be excessive.

Analog output module designs generally prefer to provide voltage outputs rather than current output (unless power is provided externally), as this places lower power requirements on the backplane.

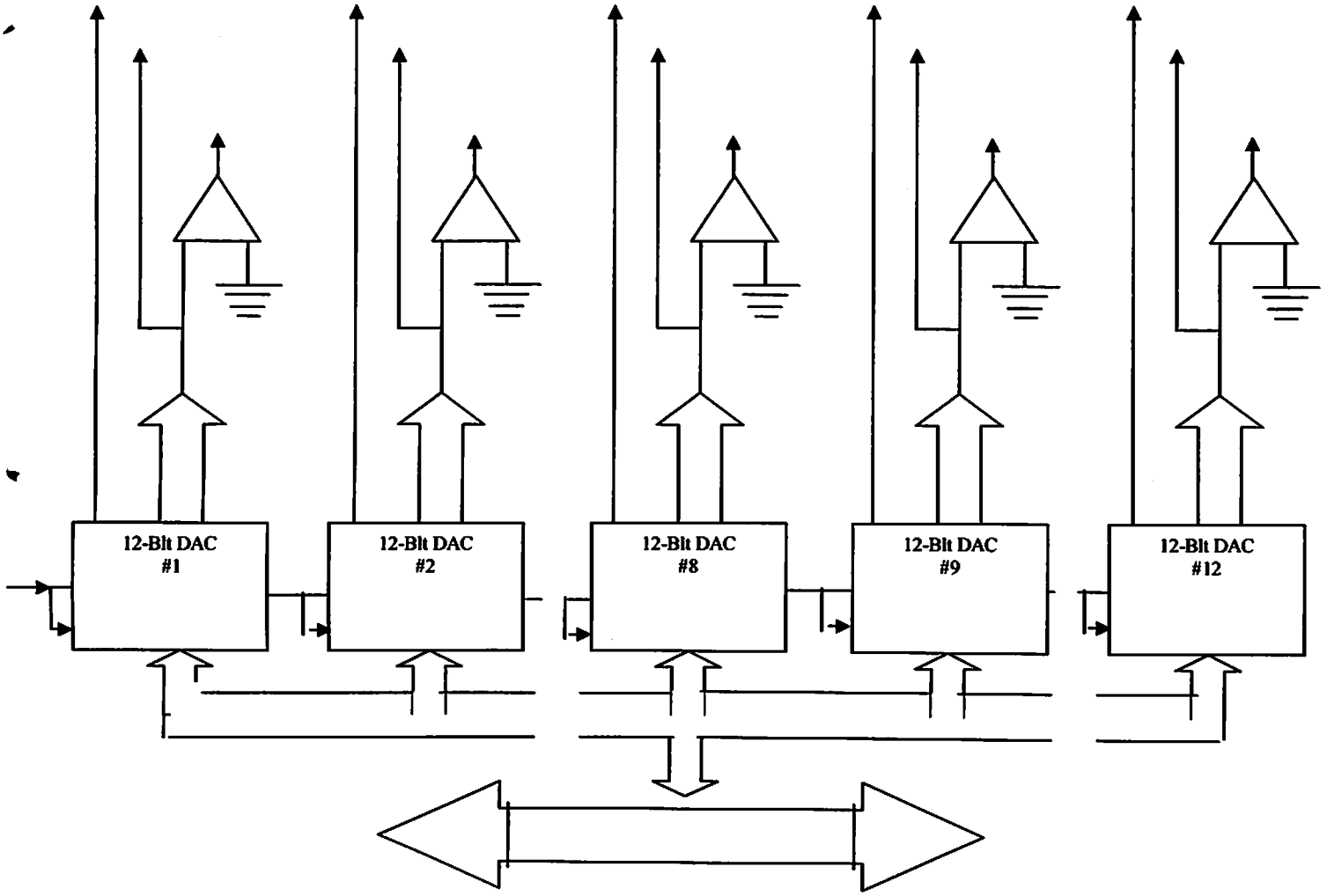


Figure 2.8 Typical analog output module

2.3.3 Digital inputs

These are used to indicate items such as status and alarm signals. Status signals from a valve could comprise two limit switches with contact closed indicating valve - open status and the other contact closed indicating valve - closed status. When both open and closed status contacts are closed, this could indicate the valve is in transit. (There would be a problem if both status switches indicate open conditions.) A high level switch indicates an alarm condition.

It is important with alarm logic that the R TV should be able to distinguish the first alarm from the subsequent spurious alarms that will occur.

Most digital input boards provide groups of 8, 16 or 32 inputs per hoard. Multiple, boards may need to be installed to cope with numerous digital points (where the count of a given board is exceeded).

The standard, normally open or normally closed converter may be used for alarm. In general, normally closed alarm digital inputs are used where the circuit is to indicate an alarm condition.

The input power supply must be appropriately rated for the particular convention used, normally open or normally closed. For the normally open convention, it is possible to de-rate the digital input power supply.

Optical isolation is a good idea to cope with surges induced in the field wiring. A typical circuit and its operation are indicated in Figure 2.12.

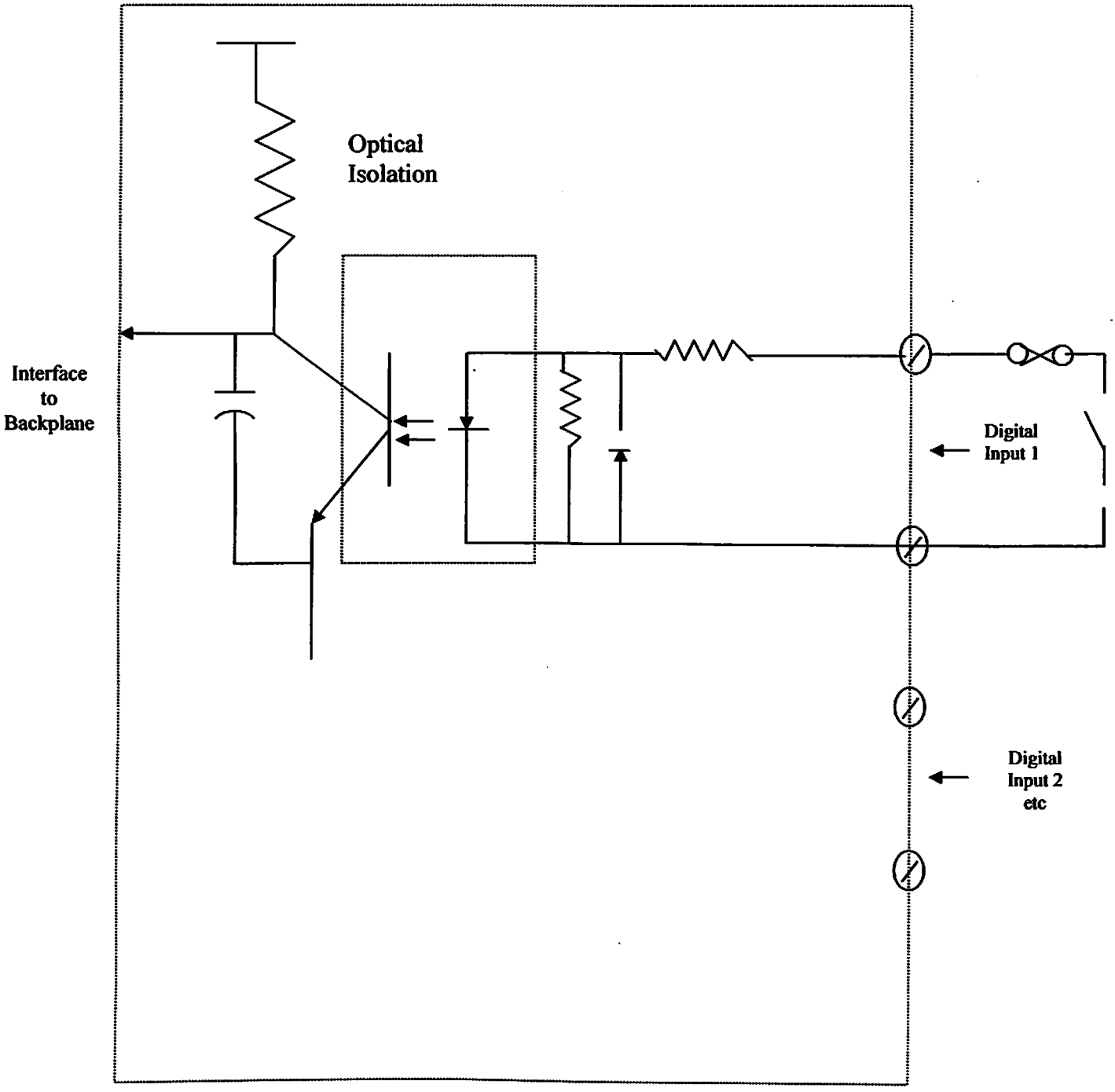


Figure 2.9 Digital Input circuit with flow chart of operation

The two main approaches of setting the input module up as a sink or source module are as indicated in the Figure 2.10.

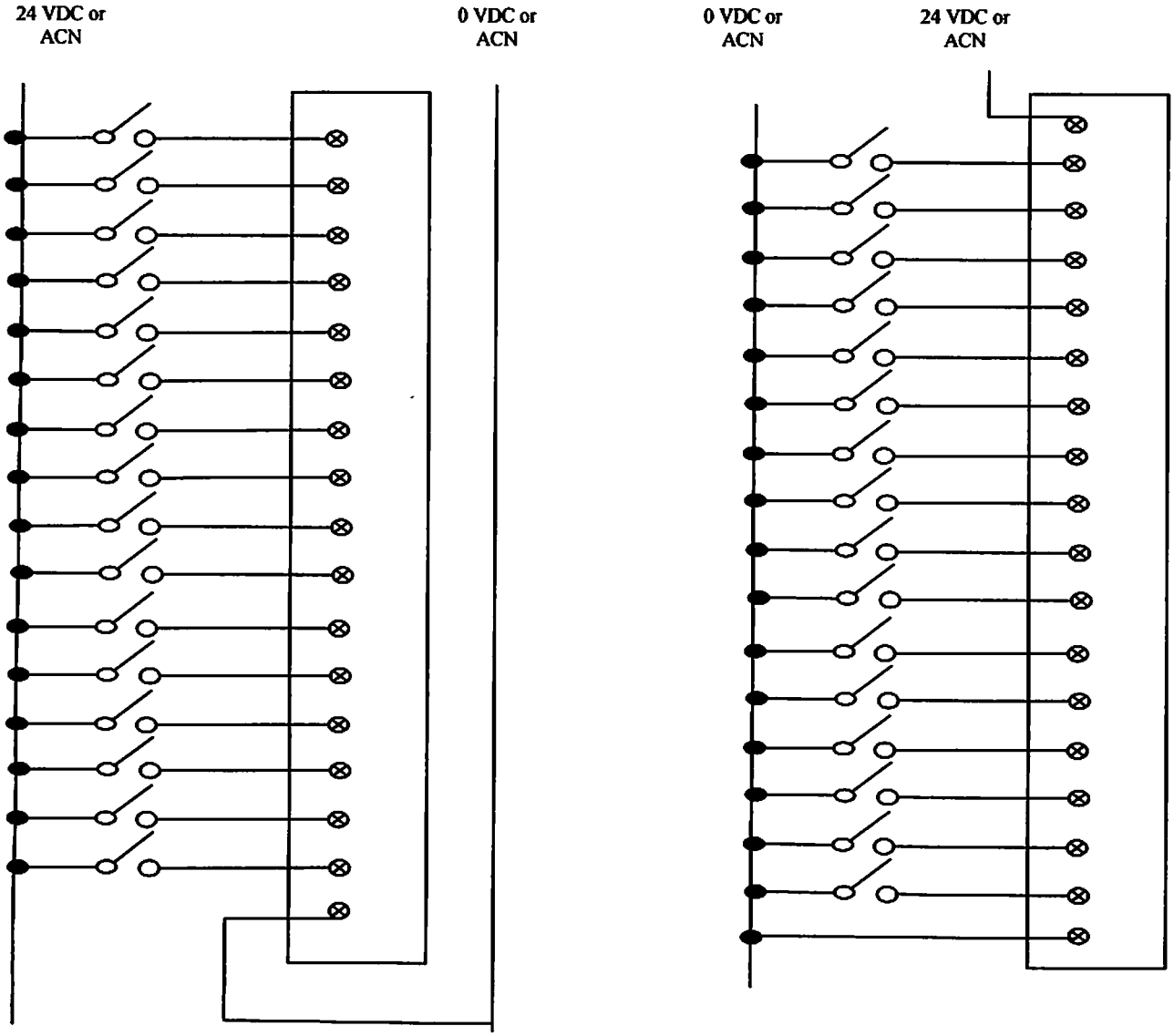


Figure 2.10: Configuring the input module as a sink or source

Typically the following would be expected of a digital input module:

- 16 digital inputs per module
- Associated LED indicator for each input to indicate current states
- Digital input voltages vary from 1.10/240 V AC and 12/24/48 VDC
- Optical isolation provided for each digital input

2.3.3.1 Counter or accumulator digital inputs

There are many applications where a pulse-input module is required - for example from a metering panel. This can be a contact closure signal or if the pulse frequency is high enough, solid state relay signals.

Pulse input signals are normally 'dry contacts' (i.e. the power is provided from the RTU power supply rather than the actual pulse source).

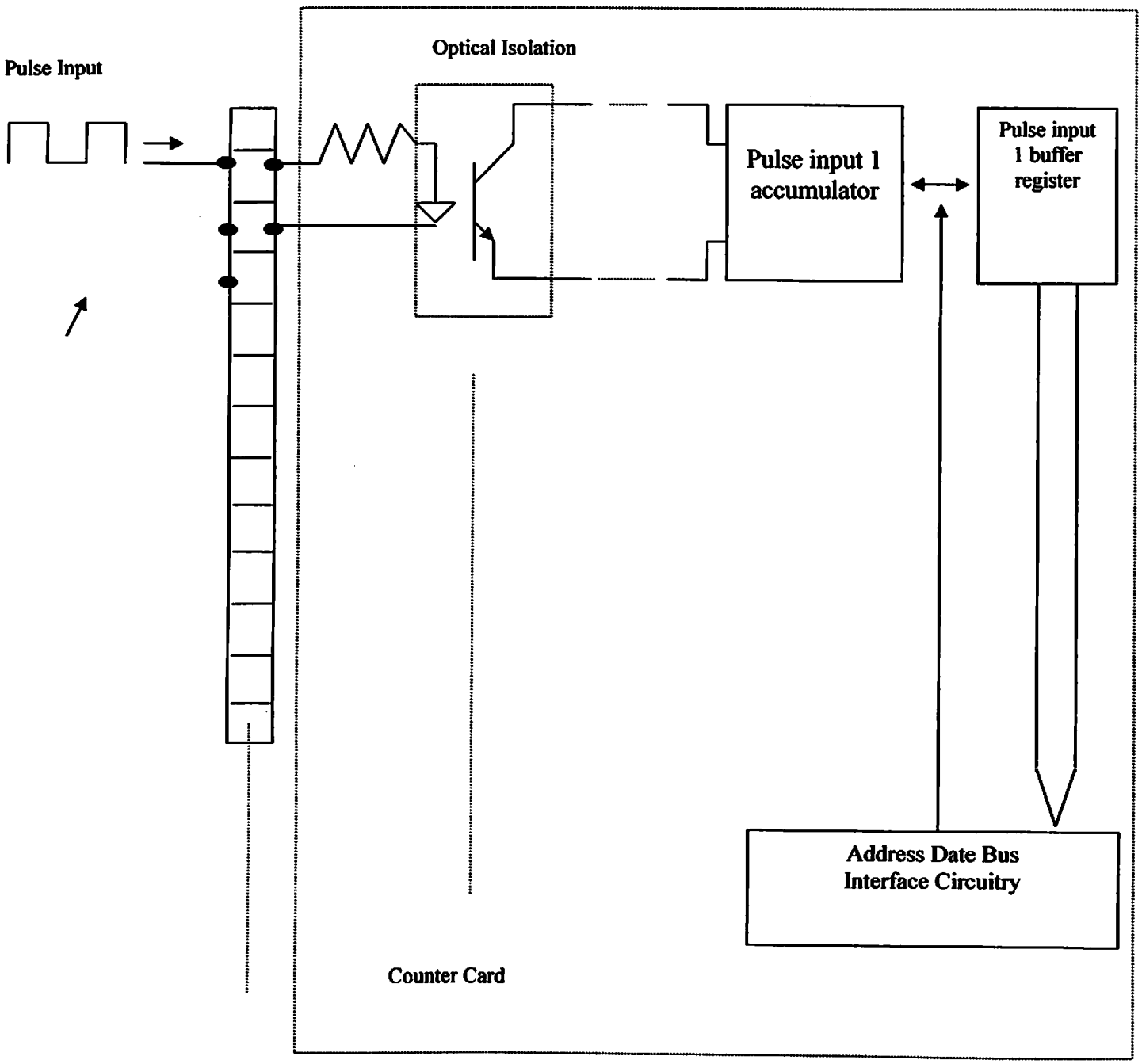


Figure 2.11: Pulse Input Module

The figure 2.11, above, gives the diagram of the counter digital input system. Optical isolation is useful to minimize the effect of externally generated noise. The size of the accumulator is important when considering the number of pulses that will be counted, before transferring the data to another memory location. For example, a 12-bit register has the capacity for 4096 counts. 16-bit gives 65536 pulses, which could represent 48 minutes @ 20 000 barrels/hour, for example. If these limits are ignored, the classical problem of the accumulator cycling through zero when full could occur.

Two approaches are possible:

- The accumulator contents can be transferred to RAM memory at regular intervals where the old and current value difference can be stored in a register.
- The second approach is where a detailed and accurate accounting needs to be made of liquids flowing into and out of a specific area. A freeze accumulator command is broadcast instantaneously to all appropriate RTUs. The pulse, accumulator will then freeze the 'values at this time and transfer to a memory location, and resets the accumulator so that counting can be resumed again.

2.3.3.2 Typical counter specifications

The typical specifications here are:

- counter inputs
- Four 16 bit counters (65 536 counts per counter input)
- Count frequency up to 20 kHz range
- Duty cycle preferably 50% (ratio of mark to space) for the upper count frequency limits.

Note that the duty rating is important, as the counter input needs a finite time to switch on (and then off). If the on pulse is too short, it may be missed although the count frequency is within the specified limits.

A Schmitt trigger gives the preferred input conditioning although a resistor capacitor combination across the counter input can be a cheap way to spread the pulses out. .

2.3.4 Digital output module

A digital output module drives an output voltage at each of the appropriate output channels with three approaches possible:

- Triac switching
- Reed relay switching
- TTL voltage outputs

The TRIAC is commonly used for AC switching. A varistor is often connected across the output *of* the TRIAC to reduce the damaging effect *of* electrical transients.
Three practical issues should also be observed:

- A TRIAC output switching device does not completely switch on and *off* but has low and high resistance values. Hence although the TRIAC is switched *off* it still has some leakage current at the output.
- Surge currents should be *of* short duration (half a cycle). Any longer will damage the module.
- The manufacturer's continuous current rating should be adhered to. This often refers to individual channels and to the number *of* channels. There are situations where all the output channels *of* the module can be used at full rated current capacity. This can exceed the maximum allowable power dissipation for the whole module.

Typically digital output modules have:

- 8 digital outputs
- 240 V AC/24 V DC *(0.5* amp to 2.0 amp) outputs
- Associated LED indicator for each output to indicate current status
- Optical isolation or dry relay contact for each output

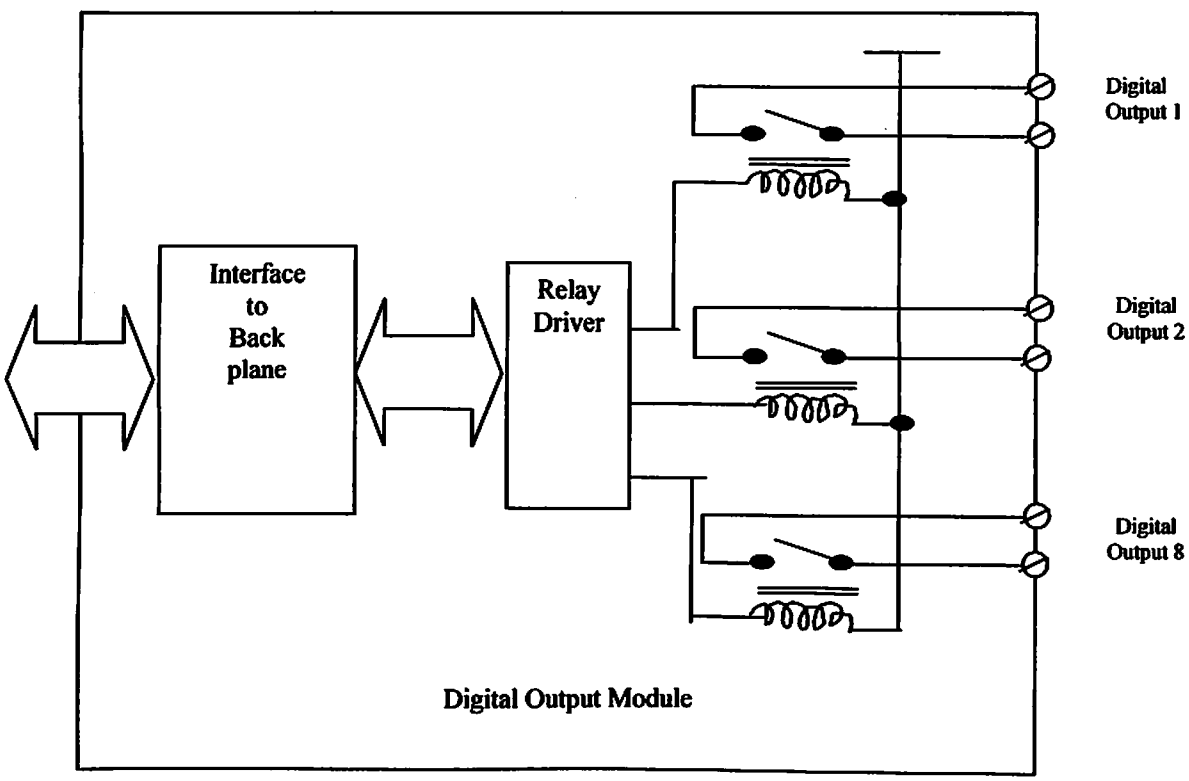


Figure 2.12: Digital Output Module

'Dry' relay contacts (i.e. no voltage applied to the contacts by the output module) are often provided. These could be reed relay outputs for example. Ensure that the current rating is not exceeded for these devices (especially the inductive current). Although each digital output could be rated at 2 Amps, the module as a whole cannot supply 16 Amps (8 by 2 amps each) and there is normally a maximum current rating for the module of typically 60% of the number of outputs multiplied by the maximum current per output. If this total current is exceeded there will be overheating of the module and eventual failure.

2.3.5 Mixed analog and digital modules

As many RTUs have only modest requirements, as far as the analog and digital signals are concerned, a typical solution would be to use a mixed analog and digital module. This would typically have:

- 4 analog inputs (8-bit resolution)
- 2 digital inputs
- 1 digital output
- 2 analog output (8-bit resolution)

2.3.6 Communication interfaces

The modem RTD should be flexible enough to handle multiple communication media such as:

- RS-232/RS-442/RS-485
- Dialup telephone lines/dedicated landlines
- Microwave/MDX
- Satellite
- X.25 packet protocols
- Radio via trunkecllVHF/UHF/900 MHz

Interestingly enough, the morecha.llenging design for RTUs is the radio communication interface. The landline interface is considered to be an easier design problem. These standards will be discussed in a later section.

2.3.7 Power supply module for RTU

The RTD should be able to operate from 110/240 V AC:I: 10% 50 Hz or 12/24/48 V.DC :I: 10% typically. Batteries that should be provided are lead acid or nickel cadmium. Typical requirements here are for 20-hour standby operation and a recharging time of 12 hours for a fully discharged battery at 25°C. The power supply, battery and associated charger are normally contained in the RTD housing.

Other important monitoring parameters, which should be transmitted back to the central site/master station, are:

- Analog battery reading
- Alarm for battery voltage outside normal range

Cabinets for batteries are normally rated to IP 52 for internal mounting and IP 56 for external mounting.

2.3.8 RTU environmental enclosures

Typically, the printed circuit boards are plugged into a backplane in the RTD cabinet. The RTD cabinet usually accommodates inside an environmental enclosure which protects it from extremes of temperature/weather etc.

Typical considerations in the installations are:

- Circulating air fans and filters: This should be installed at the base of the RTU enclosure to avoid heat buildup. Hot spot areas on the electronic circuitry should be avoided by uniform air circulation. It is important to have a heat soak test too.
- Hazardous areas: RTUs must be installed in explosion proof enclosures (e.g. oil and gas environment).

Typical operating temperatures of R TV s are variable when the RM is located outside the building in a weatherproof enclosure. These temperature specifications can be relaxed if the RTU is situated inside a building, where the temperature variations are not as extreme (provided consideration is given to the situation, where there may be failure of the ventilators or air-conditioning systems).

Typical humidity ranges are lO-95%. Ensure at the high humidity level that there is no possibility of condensation on the circuit boards or there may be contact corrosion or short-circuiting. Lacquering of the printed circuit boards may be an option in these cases. Be aware of the other extreme where low humidity air (5%) can generate static electricity on the circuit boards due to stray capacitance. CMOS based electronics is particularly susceptible to problems in these circumstances. Only screening and grounding the affected electronic areas can reduce static voltages. All maintenance personnel should wear a ground strap on the wrist to minimize the risk of creating and transferring static voltages.

If excessive electromagnetic interference (EMI) and radio frequency interference (RFI) is anticipated in the vicinity of the RTU, special screening and earthing should be used. Some manufacturers warn against using handheld transceivers in the neighborhood of their RTUs. Continuous vibration from vibrating plant and equipment can also have an unfavorable impact on an RTU, in some cases. Vibration shock mounts should be specified for such RTUs. Other areas which should be considered with RTUs are lightning (or protection from electrical surges) and earthquakes (which is equivalent to vibrations at frequencies of 0.1 to 10 Hz).

2.3.9 Typical requirements for an RTU system

In the writing of a specification, the following issues should be considered:

Hardware:

Individual RTU expandability (typically up to 200 analog and digital points)

- Off the shelf modules
- Maximum number ofRTU sites in a system shall be expandable to 255
- Modular system - no particular order or position in installation (of modules in a rack)
- Robust operation - failure of one module will not affect the performance of other modules
- Minimization of power consumption (CMOS can be an advantage)
- Heat generation minimized
- Rugged and of robust physical construction
- Maximization of noise immunity (due to harsh environment)
- Temperature of -10 to 65°C (operational conditions)
- Relative humidity up to 90%

- Clear indication of diagnostics
- Visible status LEDs
- Local fault diagnosis possible
- Remote fault diagnostics option
- Status of each I/O module and channel (program running/failed/communications OK/failed)
- Modules all connected to one common bus
- Physical interconnection of modules to the bus shall be robust and suitable for use in harsh environments
- Ease of installation of field wiring. Ease of module replacement.
- Removable screw terminals for disconnection and reconnection of wiring

Environmental considerations

The RTU is normally installed in a remote location with fairly harsh environmental conditions. It typically is specified for the following conditions:

- Ambient temperature range of 0 to +60°C (but specifications of -30°C to 60°C are not uncommon)
- Storage temperature range of -20°C to +70°C
- Relative humidity of 0 to 95% non condensing
- Surge withstand capability to withstand power surges typically 2.5 kV, 1 MHz for 2 seconds with 150 ohm source impedance
- Static discharge test where 1.5 cm sparks are discharged at a distance of 30 cm from the unit
- Other requirements include dust, vibration, rain, salt and fog protection.

Software (and firmware)

- Compatibility checks of software configuration of hardware against actual hardware available
- Log kept of all errors that occur in the system both from external events and internal faults. Remote access of all error logs and status registers.
- Software operates continuously despite powering down or up of the system due to loss of power supply or other faults
- Hardware filtering provided on all analog input channels
- Application program resides in non volatile RAM
- Configuration and diagnostic tools for:
- System setup
- Hardware and software setup
- Application code development/management/operation
- Error logs
- Remote and local operation

Each module should have internal software continuously testing the systems I/O and hardware. Diagnostic LEDs should also be provided to identify any faults or to diagnose failure of components. It is important that all these conditions are communicated back to the central station for indication to the operator.

2.4 Application programs

Many applications, which were previously performed at the master station, can now be performed at the RTU, due to improved processing power and memory/dish storage facilities available. Many RTUs also have a local operator interface provided. Typical application programs that can run in the RTU are:

- Analog loop control (e.g. PID).
- Meter proving
- (Gas) flow measurement
- Compressor surge control

2.5 PLCs used as RTUs

A PLC or programmable logic controller is a computer based solid state device that controls industrial equipment and processes. It was initially designed to perform the logic functions executed by relays, drum switches and mechanical timer/counters. Analog control is now a standard part of the PLC operation as well.

The advantage of a PLC over the RTU offerings from various manufacturers is that it can be used in a general-purpose role and can easily, be set up for a variety of different functions.

The actual construction of a PLC can vary widely and does not necessarily differ much from generalizing on the discussion of the standard RTU.

PLCs are popular for the following reasons:

- **Economic solution**
  PLCs are a more economic solution than a hardwired relay solution manufactured R TU
- **Versatility and flexibility**
  PLCs can easily have their logic or hardware modified to cope with modified requirements for control
- **Ease of design and installation**
  PLCs have made the design and installation of SCADA systems easier because of the emphasis on software.
- **More reliable**
  When correctly installed, PLCs are a far more reliable solution than a traditional hardwired relay solution or short run manufactured RTUs.
- **Sophisticated control**
  PLCs allow for far more sophisticated control (mainly due to the software capability) than RTUs.
- **Physically compact**
  PLCs take up far less space than alternative solutions.
- **Easier troubleshooting and diagnostics**
  Software and clear cut reporting of problems allows easy and swift diagnosis of hardware/firmware/software problems on the system as well as identifying problems with the process and automation system.

A diagram of a PLC and its means of operation using standard ladderlogic are discussed in the following section.

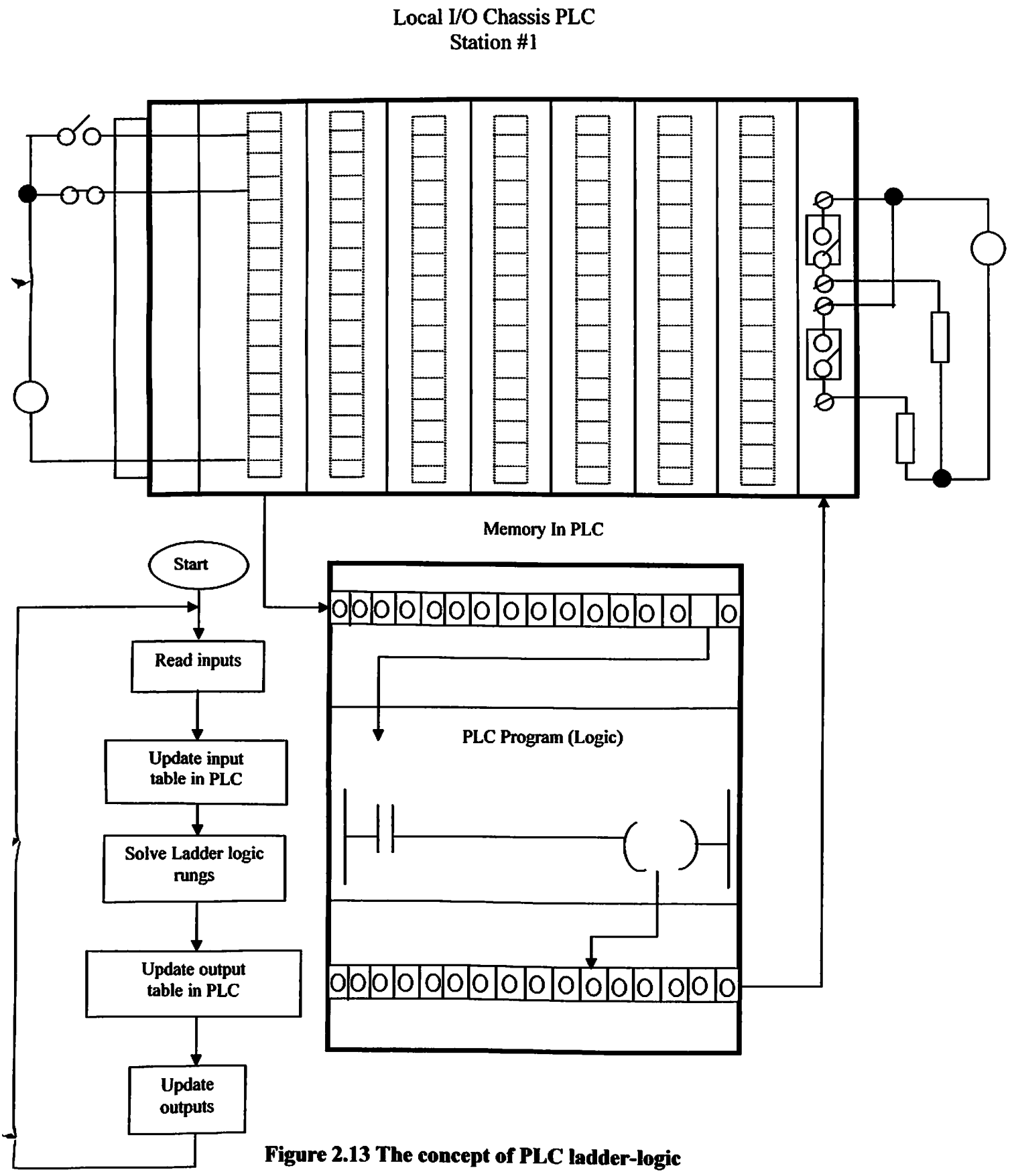


Figure 2.13 The concept of PLC ladder-logic

2.5.1 PLC software

The ladder-logic approach to programming is popular because of its perceived similarity to standard electrical circuits. Two vertical lines supplying the power are drawn at each of the sides of the diagram with the lines of logic drawn in horizontal lines.
The example below shows the 'real world' circuit with PLC acting as the control device and the internal ladder-logic within the PLC.

2.5.2 Basic rules of ladder-logic

The basic rules of ladder-logic can be stated to be:

- The vertical lines indicate the power supply for the control system (12 V DC to 240 V AC). The 'power flow' is visualized to move from left to right.
- Read the ladder diagram from left to right and top to bottom (as in the normal Western convention of reading a book).
- Electrical devices are normally indicated in their normal de-energized condition. This can sometimes be confusing and special care needs to be taken to ensure consistency.
- The contacts associated with coils, timers, counters and other instructions have the same numbering convention as their control device.
- Devices that indicate a start operation for a particular item are normally wired in parallel (so that any of them can start or switch the particular item on). See Figure 2.14 for an example of this.

Figure 2.14 Ladder Logic start operation (& logic diagram)

- Devices that indicate a stop operation for a particular item are normally wired in series (so that any of them can stop or switch the particular items off). See Figure 2.15 for an example of this.

Figure 2.15 Ladder –logic stop operation (& logic diagram)

- Latching operations are used, where a momentary start input signal latches the start signal into the on condition, so that when the start input goes into the OFF condition, the start signal remains energized ON. The latching operation is also referred to as holding or maintaining a sealing contact. See the previous two diagrams for examples of latching.
- Interactive logic: Ladder-logic rungs that appear later in the program often interact with the earlier ladder-logic rungs. This useful feed back mechanism can be used to provide feed back on successful completion of sequence operations (or protect the overall system due to failure *of* some aspect).

2.5.3 The different ladder-logic instructions

Ladder-logic instruction can be typically broken up into the following categories:

- Standard relay logic type
- Timer and counters
- Arithmetic
- Logical
- Move
- Comparison
- File manipulation
- Sequencer instructions
- Specialized analog (PID)
- Communication instructions
- Diagnostic
- Miscellaneous (sub routines etc)

A few of these instructions will be discussed in the following sections.

2.5.3.1 Standard relay type

There are three main instructions in this category. These are:

- **Normally open contact**
  (Sometimes also referred to as 'examine if closed' or 'examine on'). The symbol is indicated in Figure 2.16.

Figure 2.16 Symbol for normally open contact

This instruction examines its memory address location for an ON condition. If this memory location is set to ON or 1, the instruction is set *to* 'ON' or 'TRUE' or 'I'. *If* the location is set to OFF *of '0'*, the instruction is set to 'OFF' or 'FALSE' or *'0'*.

- **Normally closed contact**
  (Sometimes also referred to as 'examine *if* open' or 'examine *if* off). This instruction examines its memory address location for an 'OFF' condition. *If* this memory location is set to OFF *of* 1 " the instruction is set to 'OFF' *of* '0'. *If* the memory location is set to ON or '0', the instruction is set to 'ON' or 'TRUE' or 'I'. The symbol is indicated in Figure 2.17.

Figure 2.17 Symbol for normally closed contact

2.5.3.2 Output energize coil

When the complete ladder-logic rung is set to a 'TRUE' or 'ON' condition, the output energize instruction sets its memory location to an 'ON' condition; otherwise if the ladder-logic rung is set to a 'FALSE' or 'OFF' condition, the output energize coil sets its memory location to an 'OFF' condition.
The symbol is indicated in Figure 2.18.

Figure 2.18:Symbol for output energize coil

2.5.3.3 Timers

There are two types of timers:
- Timer ON delay
- Timer OFF delay

There are three parameters associated with each timer:

- **The preset value**

(Which is the constant number of seconds the timer times to, before being energized or de-energized)

- **The accumulated value**

(Which is the number of seconds which records how long the timer has been actively timing)

- **The time base**

(Which indicated the accuracy in seconds to which the timer operates e.g. 1 second, 0.1 seconds and even 0.01 seconds
The operation of the 'timer ON' timer is indicated in Figure 2.19 below. Essentially the timer output coil is activated when the accumulated time adds up to the preset value due to the rung being energized for this period of time. Should the rung conditions go to the false condition before the accumulator value is equal to the preset value, the accumulator value will be reset to a zero value.

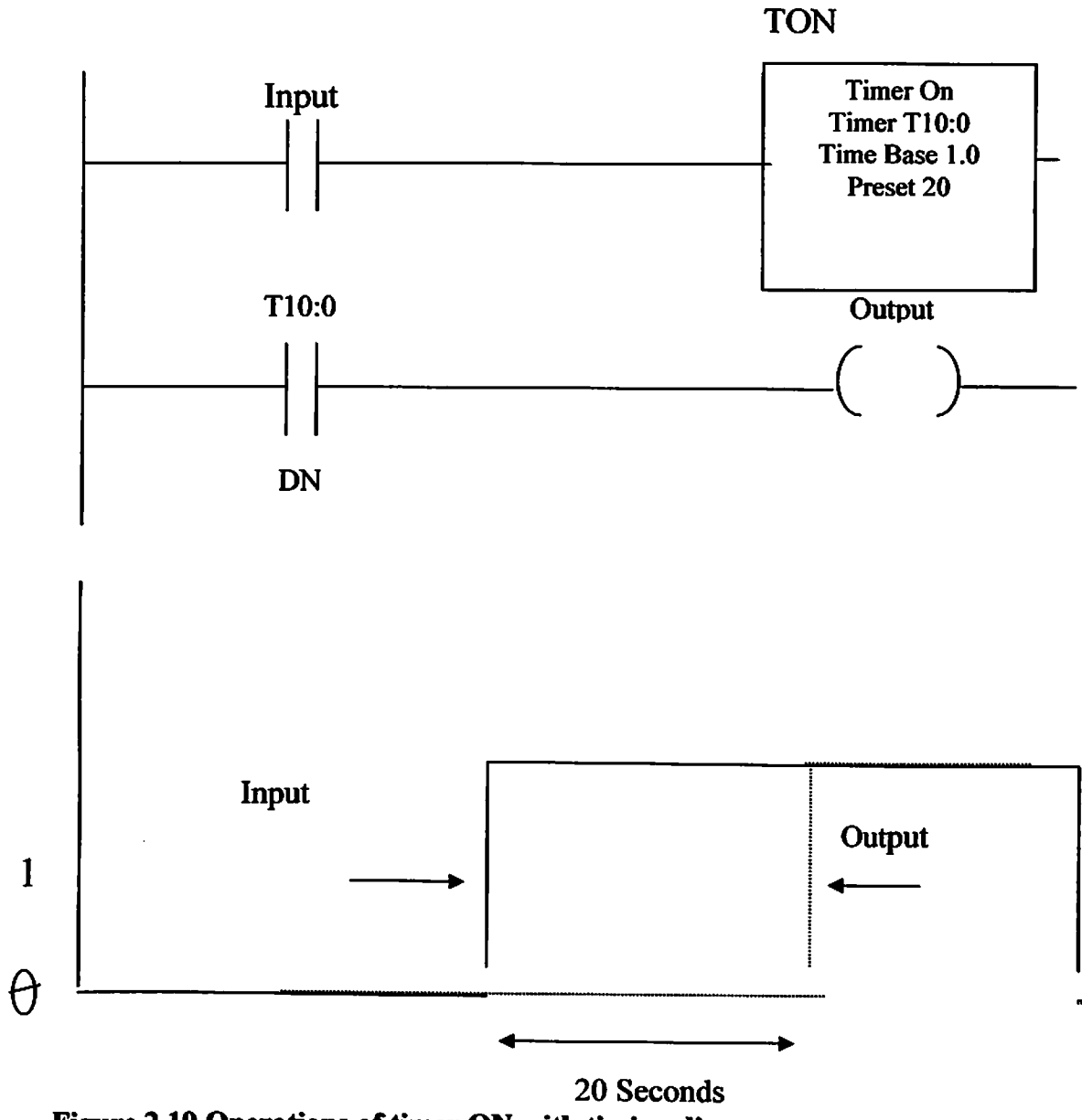


Figure 2.19 Operations of timer ON with timing diagram

The operation of the 'timer OFF' timer is that the timer coil is initially energized when the rung is active. As soon as the rung goes false (or inactive) the timer times out (the accumulated value eventually becoming equal to the preset value). At this point the timer coil becomes de-energized. If the rung conditions go low again before the accumulated value reaches the present value, the accumulator is reset to zero. The full sequence of operation is indicated in the Figure 2.20.

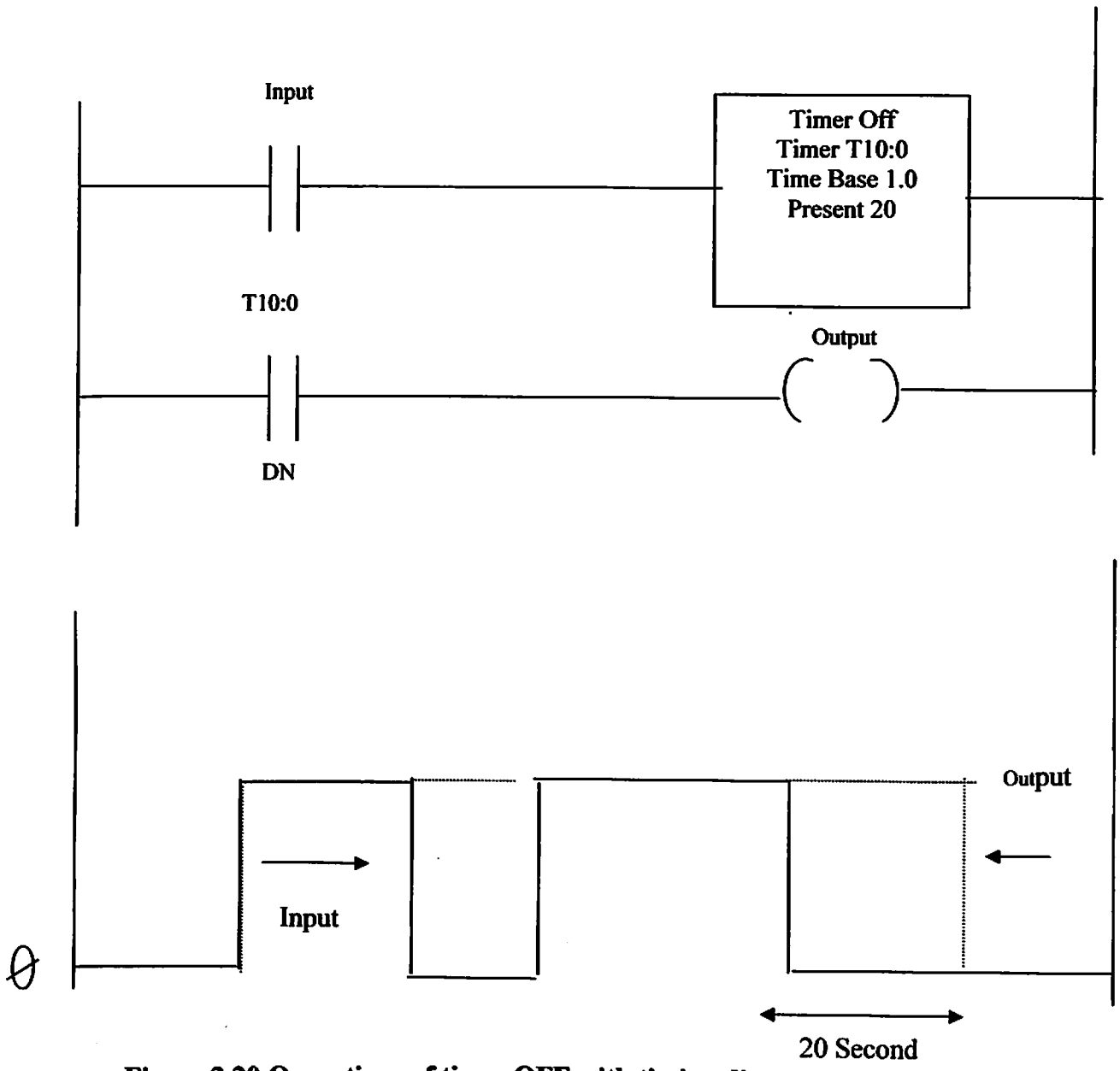


Figure 2.20 Operations of timer OFF with timing diagram

2.5.3.4 Counter

There are two types of counters, Count up and Count down. The operation of these counters is very similar to the timer ON and timer OFF timers.

There are two values associated with counters:

- Accumulated value
- Preset value

Count up counters

This counter increments the accumulator value by 1, for every transition of the input contact from false to true. When the accumulated value equals. the preset value, the counter output will energize. When a reset instruction is given (at the same address as the counter), the counter is reset and the accumulated value is set to zero.

Count down counters

This counter decrements the accumulator value (which started off at the preset value) by 1, for every transition of the input contact from false to true. When the accumulator value equals zero, the counter output is energized. Interestingly, the counters retain their accumulated count during a power failure, or even if programmed after an MCR instruction.

2.5.3.5 Comparison instructions

These are useful to compare the contents of words with each other. Typical instructions here are to compare two words for:

- Equality
- Not equal
- Less than
- Less than or equal to
- Greater than
- Greater than or equal to

When these conditions are true they can be connected in series with a coil which they then drive into the energized state.

2.5.3.6 Sub routines and jump instructions

There are two main ways of transferring control of the ladder-logic program from the standard sequential path in which it is normally executed. These are:

- Jump to part of the program when a rung condition becomes true (sometimes called jump to a label)
- Jump to a separate block of ladder-logic called a sub routine.

Some users unwittingly run into problems with entry of a ladder-logic rung into the PLC due to limitations in the reporting of incorrect syntax by the relevant packages. The typical limitations are:

- **Numbering of coils and contacts per rung (or network)**
  Most ladder-logic implementations typically allow only one coil per rung, a certain maximum number of parallel branches (e.g. seven) and a certain maximum number of series contacts (e.g. ten) per branch. Additional rungs (with 'dummy' coils) would have to be put in if there was a need for more contacts than can be handled by one rung or network.

- **Vertical contacts**
  Vertical contacts are normally not allowed.

- **Nesting of contacts**
  Contacts may only be allowed to be nested to a certain level in a PLC. In others no nesting is allowed.

- **Direction of power flow**
  'Power flow' within a network or rung always has to be from left to right. Any violation of this principle would be disallowed.

2.6 The master station

The central site/master station can be pictured as having one or more operator stations (tied together with a local area network) connected to a communication system consisting of modem and radio receiver/transmitter. It is possible for a landline system to be used in place of the radio system; in this case the modem will interface directly to the landline. Normally there are no input/output modules connected directly to the master stations although there may be an RTU located in close proximity to the master control room. The features that should be available are:

- Operator interface to display status of the RTUs and enable operator control.
- Logging of the data from the RTUs
- Alarming of data from the R TU

As discussed earlier, a master station has two main functions:

- Obtain field data periodically from RTUs and submaster stations
- Control remote devices through the operator station

There are various combinations of systems possible, as indicated in the diagram below.

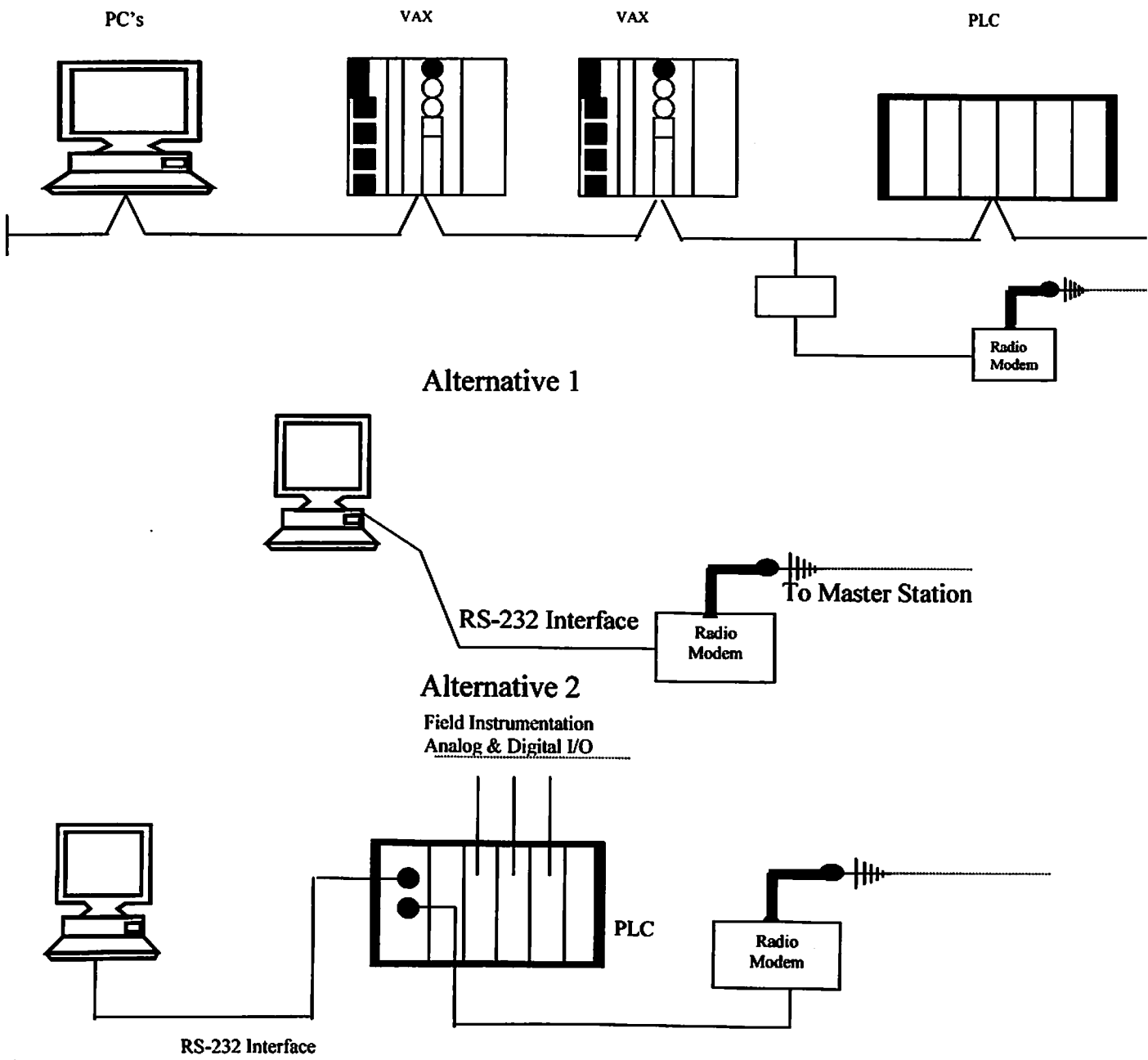


Figure 2.21 Various approaches for the master station

It may also be necessary to set up a submaster station. This is to control sites within a specific region. The submaster station has the following functions:

- Acquire data from RTUs within the region
- Log and display this data on a local operator station
- Pass data back to the master station
- Pass on control requests from the master station to the RTUs in its region

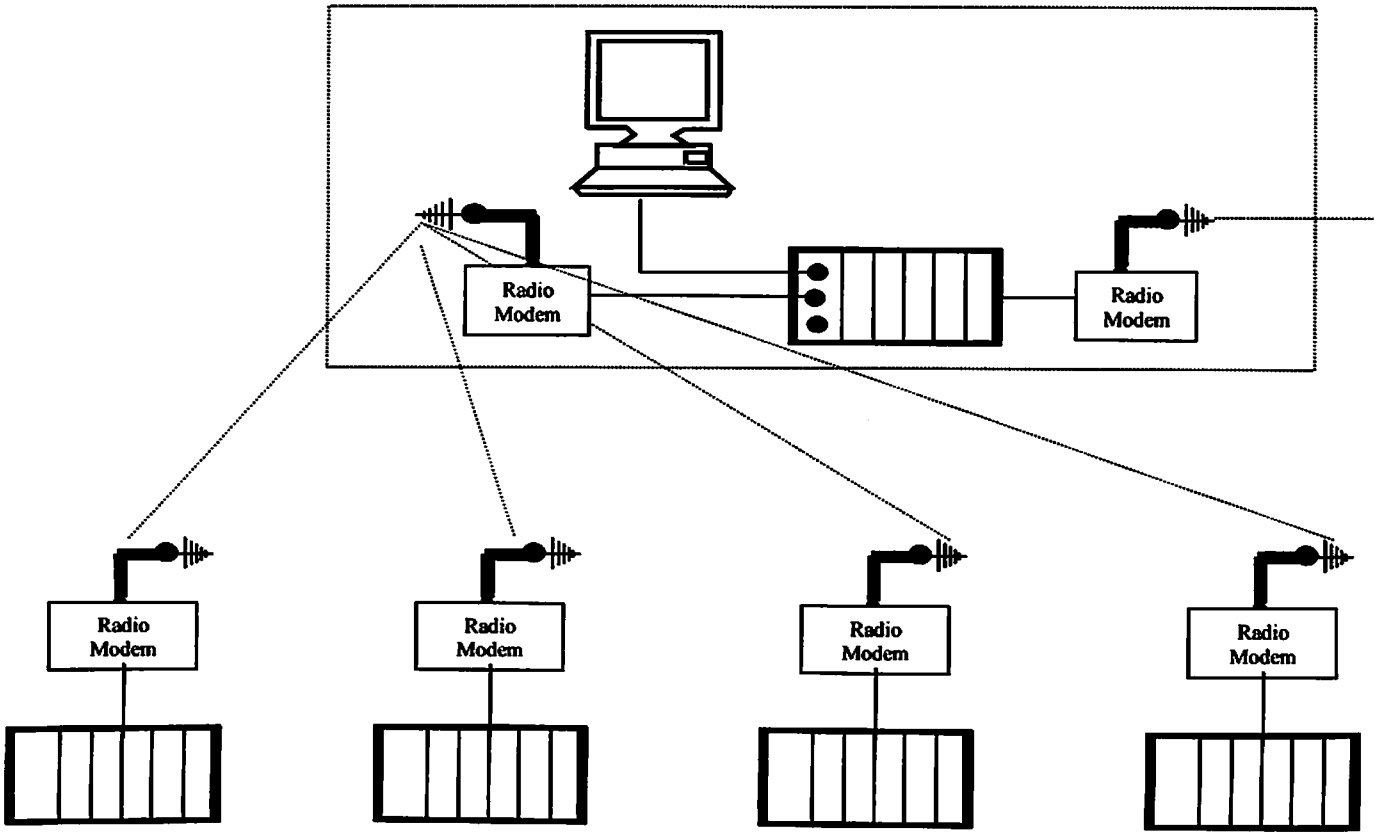


Figure 2.22: Submaster architecture

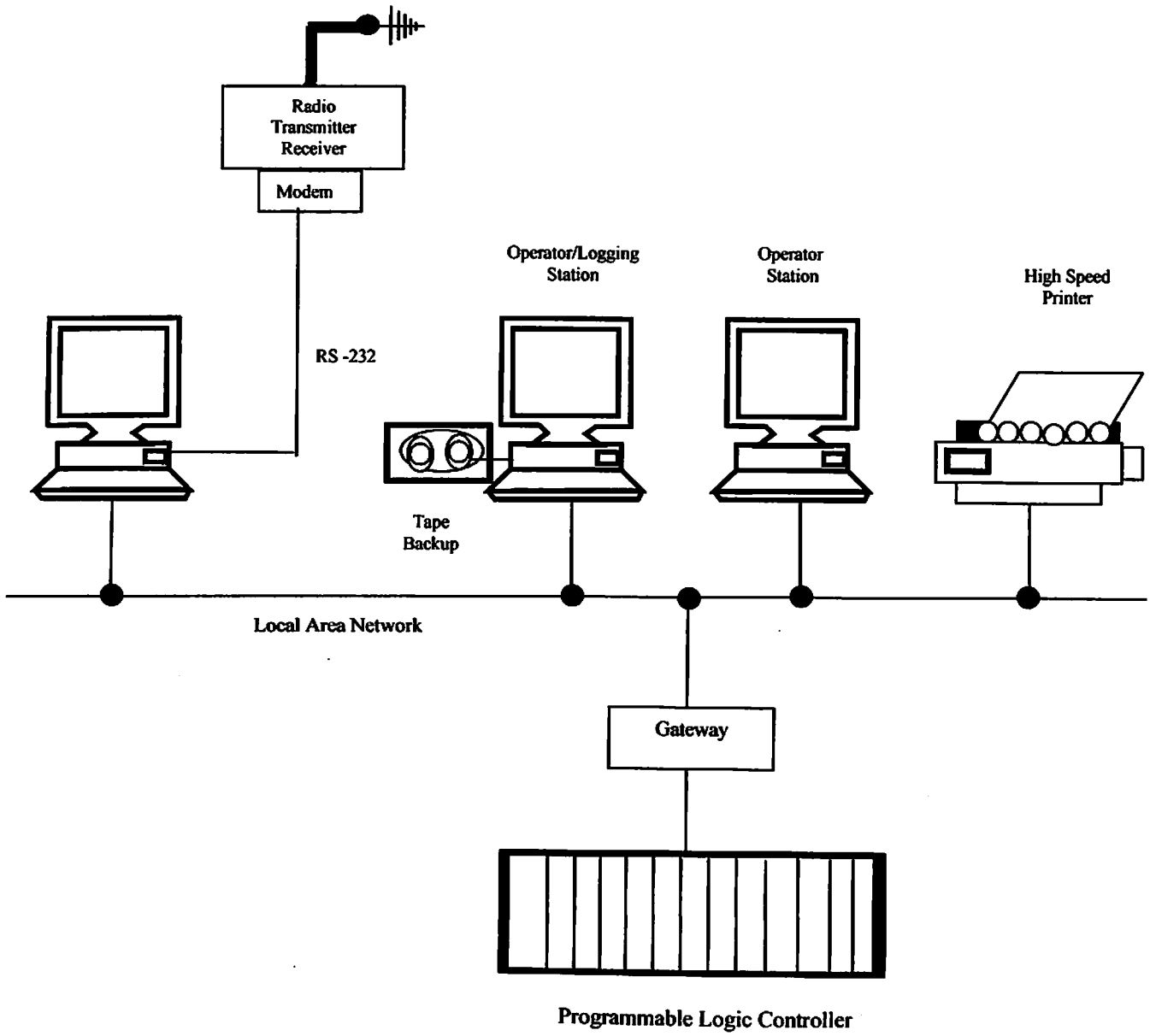


Figure 2.23 Typical structure of Master Station

The master station has the following typical functions:

Establishment of communications

- Configure each RID
- Initialize each RID with input/output parameters
- Download control and data acquisition programs to the RID

Operation of the communications link

- If a master slave arrangement, poll each RID for data and write to RID.
- Log alarms and events to hard disk (and operator display if necessary).

- Link inputs and outputs at different RIDs automatically

Diagnostics

- Provide accurate diagnostic information on failure of RID and possible problems .
- Predict potential problems such as data overloads

2.6.1 Master station software

There are three components to the master station software:

- The operating system software
- The system SCADA software (suitably configured)
- The SCADA application software

There is also the necessary firmware (such as BIOS) which acts as an interface between the operating system and the computer system hardware. The operating system software will not be discussed further here. Good examples of this are DOS, Windows, Windows NT and the various UNIX systems.

2.6.2 System SCADA software

This refers to the software put together by the particular SCADA system vendor and then configured by a particular user. Generally, it consists of four main modules:

- Data acquisition
- Control
- Archiving or database storage
- The man machine interface (MMI)

This software is discussed in more detail in the next chapter. As discussed earlier, a successful SCADA system design implies considerable emphasis on the central site structure. Hence, this will be assessed under the next section. However, one of the features of a central site is the use of LANs. These will be briefly reviewed here.

2.6.3 Local area networks

The central site structure can be based on a distributed architecture and a high-speed data highway using one of the LAN standards such as 802.3 (Ethernet), 802.4 (token bus) or HO2.5 (token ring). The most common approach is to use the Ethernet or token bus arrangement, where there is no one master operator station. The approach that appears to be gaining acceptance in the market place is the token bus approach where a token is used to transfer control from one station to another. This allows for easy expansion of the system.

Each of the network options will be discussed in the following paragraphs. Specific reference will be made to the three types of LANs:

- Ethernet (or CSMA/CD)
- Token ring (e.g. IBM token ring)
- Token bus (e.g. MAPIPLC type industrial systems)

Each of these network types is considered in more detail in the following sections.

2.6.4 Ethernet

This is generally implemented as a 10 Mbps baseband coaxial cable network. Carrier sense multiple access with collision detection (or CSMA/CD) is the media access control (or MAC) method used by Ethernet. This is the more popular approach with LANs and hence will be discussed in more detail than the alternative approaches.

The philosophy of Ethernet originated from radio transmission experiments with multiple stations endeavoring to communicate with each other at random times. Essentially before a station (or node) transmits a message (on the common connecting cable) to another node, it first listens for any bus (cable or radio) activity. If it detects that there are no other nodes transmitting, it sends its message. There is a probability that another station may attempt to transmit at precisely the same time. If there is a resultant collision between the two nodes, both nodes will then back off for a random time before reattempting to transmit (hopefully at different times because of the random delay). A typical view of the construction of the medium access control unit for each Ethernet station is given in Figure 2.24.

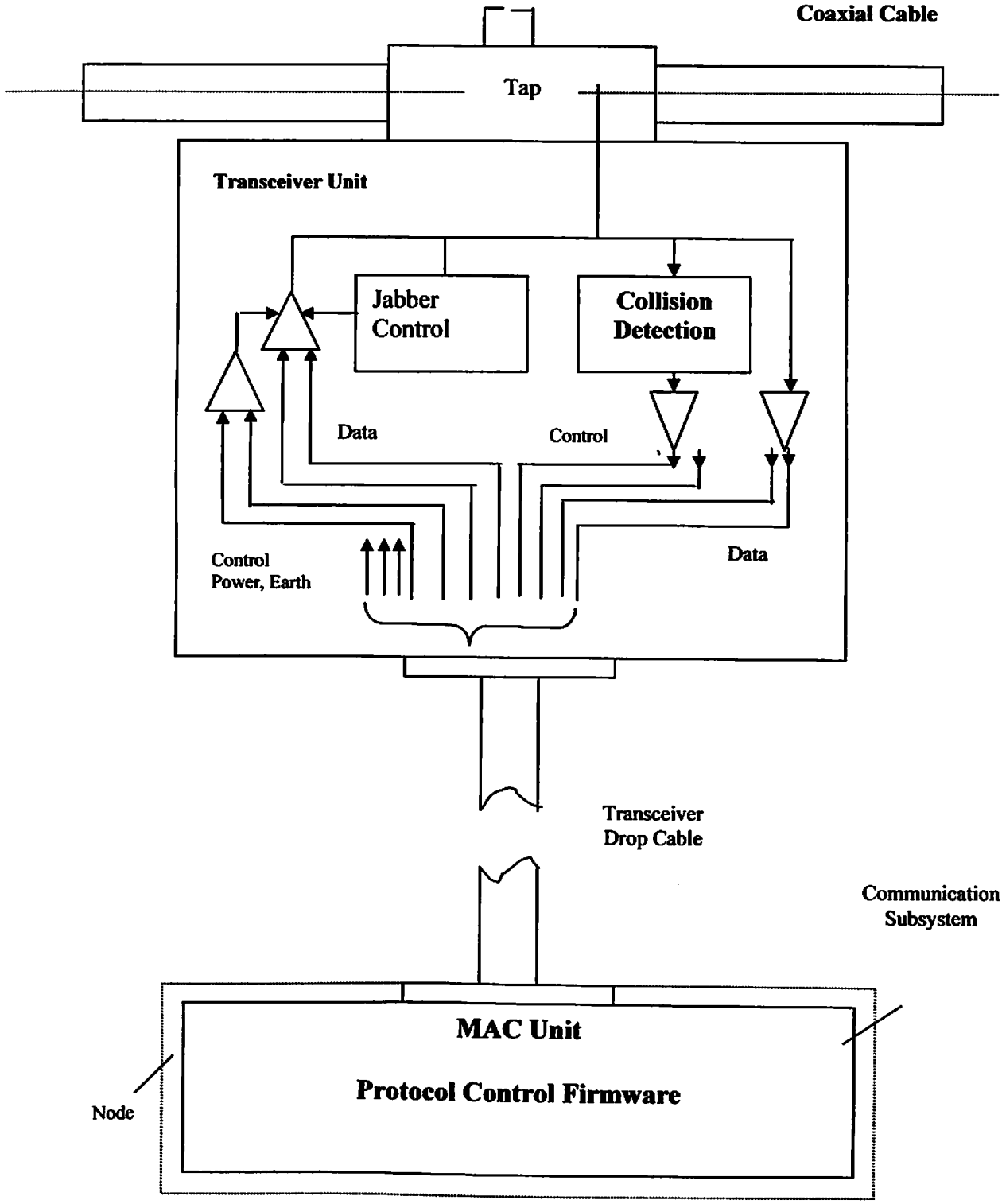


Figure 2.24 A typical hardware layout for a CSMA/CD system

2.7 Communication architectures and philosophies

There are three main physical communication architectures possible. The approaches can be combined in one communication system. However, it is useful to consider each one in' isolation for the purposes of this discussion. The ancillary philosophies of achieving communications will be considered next.

2.7.1 Communication architectures

Point-to-point (two stations)

This is the simplest configuration where data is exchanged between two stations. One station can be setup as the master and one as the slave. It is possible for both stations to communicate in full duplex mode (transmitting and receiving on two separate frequencies) or simplex with only one frequency.

Figure 2.25: Point-to-Point (two staions)

Multipoint (or multiple stations)

In this configuration, there is generally one master and multiple slaves. Generally data points are efficiently passed between the master and each of the slaves. If two slaves need to transfer data between each other they would do so through the master who would act as arbitrator or moderator.

Alternatively, it is possible for all the stations to act in a peer-to-peer communications manner with each other. This is a more complex arrangement requiring sophisticated protocols to handle collisions between two different stations wanting to transmit at the same time.

Figure 2.26: Multiple stations

2.7.2 Communication philosophies

There are two main communication philosophies possible. These are; polled (or master slave) and carrier sense multiple access/collision detection (CSMA/CD). The one notable method for reducing the amount of data that needs to be transferred from one point to another (and to improve the overall system response times) is to use exception reporting which is discussed later. With radio systems, exception reporting is normally associated with the CSMA/CD philosophy but there is no theoretical reason why it cannot be applied to RTUs where there is a significant amount of data to be transferred to the master station.

This discussion concentrates on the radio communication aspects. It is difficult to use token bus or CSMA/CD on cable systems other than in a LAN context (with consequent short distances). For longer distances, cable systems would use a polled philosophy.

2.7.3 Polled (or master slave)

This can be used in a point to point or multipoint configuration and is probably the simplest philosophy to use. The master is in total control of the communication system and makes regular (repetitive) requests for data and to transfer data, to and from each one of a number of slaves. The slaves do not initiate the transaction but rely on the master. It is essentially a half-duplex approach where the slave only responds on a request from the master. If a slave does not respond in a defined time, the master then retries (typically up to three times) and then marks the slave as unserviceable and then tries the next slave node in the sequence. It is possible to retry the unserviceable slave again on the next cycle of polling.

The advantages of this approach are:

- Software is easily written and is reliable due to the simplicity of the philosophy.
- Link failure between the master and a slave node is detected fairly quickly.
- No collisions can occur on the network; hence the data throughput is predictable and constant.
- For heavily loaded s) systems with each node having constant data transfer requirements, as this gives a predictable and efficient system.

The disadvantages are:

- Variations in the data transfer requirements of each slave cannot be handled.
- Interrupt type requests from a slave requesting urgent action cannot be handled (as the master may be processing some other slave).
- Systems, which are lightly loaded with minimum data changes from a slave, are quite inefficient and unnecessarily slow.
- Slaves needing to communicate with each other have to do so through the master with added complexity in the design of the master station.

Two applications of the polled (or master slave) approach are given in the following two implementations. This is possibly the most commonly used technique and is illustrated in the diagram below.

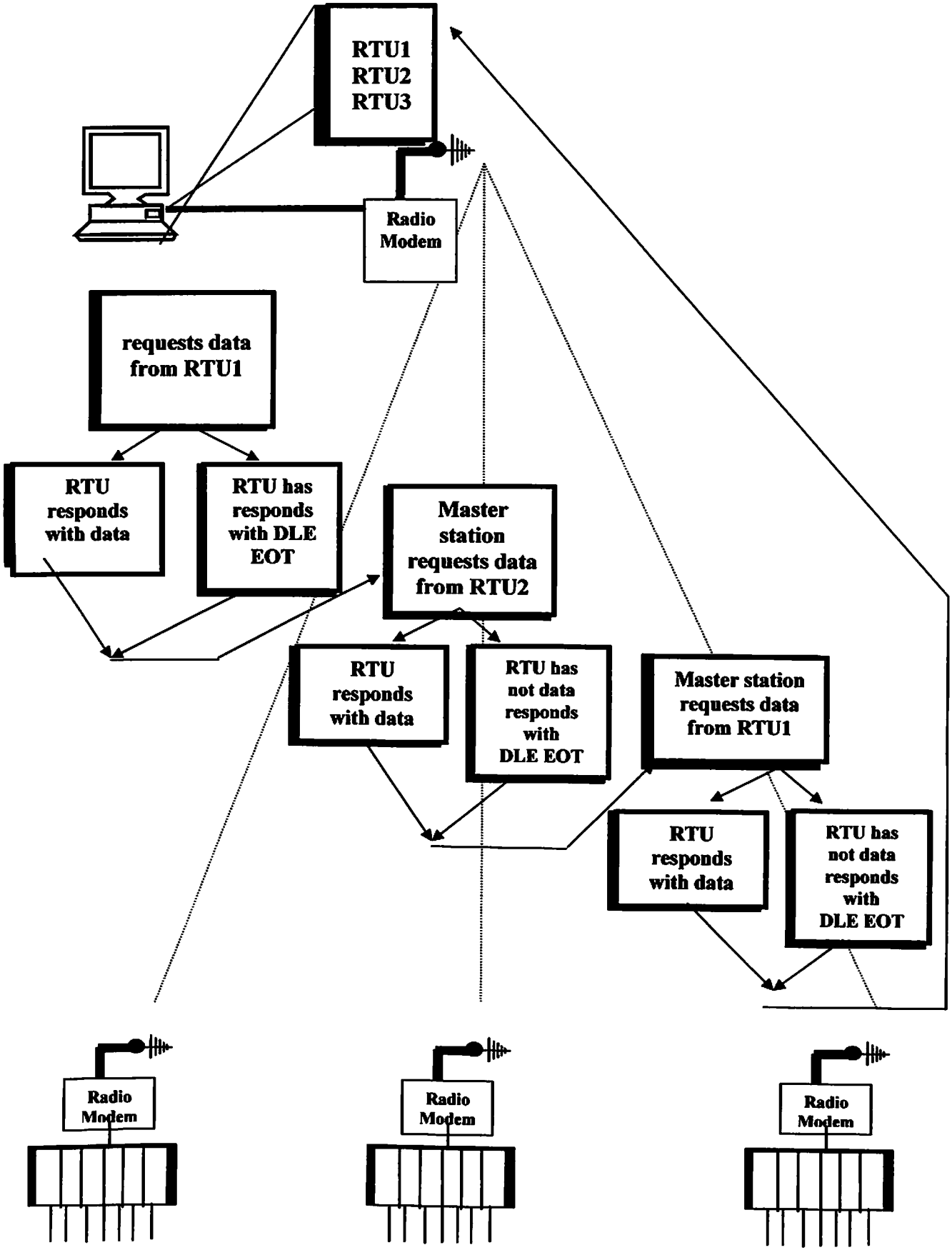


Figure 2.27 Illustration of polling techniques for master station and RTUs

There are certain considerations to refine the, polling scheme beyond what is indicate in the diagram above. These are:

- If there is no response from a given RTU during a poll, a timeout timer has to be set and three retries (in total) initiated *before* flagging this station as inactive.

- If an RTU, is to be treated as a priority station it will be polled at a greater rate than a normal priority station. It is important not to put too many RTUs on the priority list, otherwise the differentiation between high and normal priority becomes meaningless.

An example of a high and normal priority arrangement is given in the diagram below

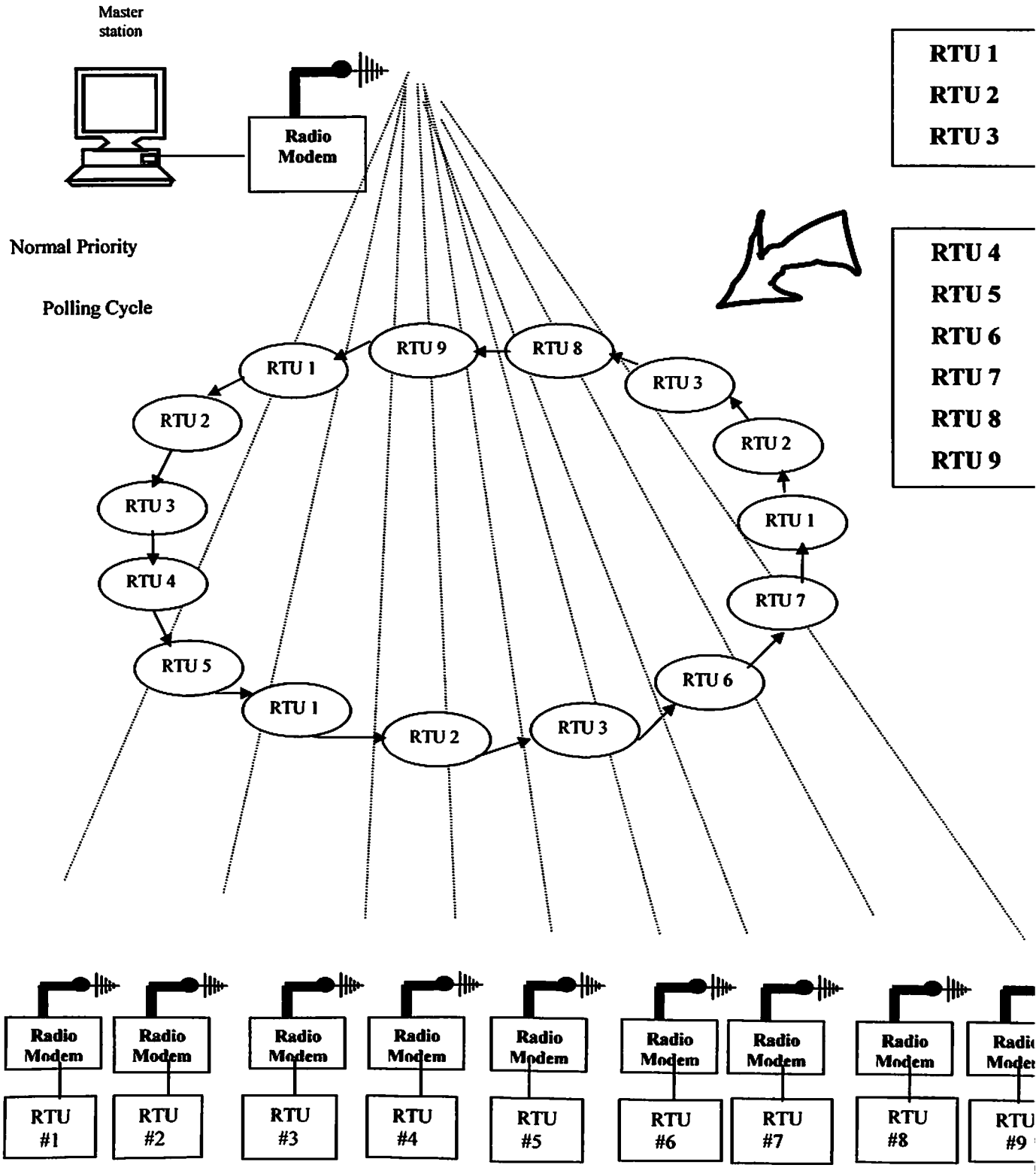


Figure 2.30 High & normal priority arrangement

A priority message sent from the master station can override the standard polling sequence. In this case, the master station completes the poll request for a specific station and. then sends out the priority request to a specific station (which is not necessarily next

in the polling sequence). It can then wait a predefined time *for* a response from this RTU or continue with polling a few more stations in the polling sequencer, before requesting a reply from this specific station.
Care should be taken in defining the optimum values for the timers e.g. a satellite link may have significant development compared to a leased line communications system.

2.7.4 CSMA/CD system (peer-to-peer)

RTU to RTU communication

In a situation where an R TU wants to communicate with another, a solution would be to respond to a poll by the master station having a message with a destination address other than that of the master station's.
The master station will then examine the destination address field of the message received from the R TU and if it does not, mark its own, retransmit onto the appropriate remote station.
The only attempt to avoid collisions is to listen to the medium before transmitting. The systems rely on recovery methods to handle collision problems. Typically these systems are very effective at low capacity rates, as soon as the traffic rises to over 30% *of* the channel capacity there is an avalanche collapse of the system and communications become unreliable and erratic. The initial experiments with radio transmission between multiple stations (on a peer to peer basis) used CSMA/CD.

This technique is used solely on networks where all nodes have access to the same media (within radio range or on a common cable link). All data is transmitted by the transmitting node first encapsulating the data in a frame with the required destination node address at the head of the frame. All nodes will read this frame and the node which identifies its address at the head of the frame will then continue reading the data and respond appropriately.

However with this style of operation it is possible for two nodes to try and transmit at the same time, with a resultant collision. In order to minimize the chance of a collision, the source node first listens for a carrier signal (indicating that a frame is being transmitted) before commencing transmission. Unfortunately this does not always work where certain stations (which cannot hear each other) try and transmit back to the station simultaneously.

There is a collision here, which only the master can detect (and thus correct). However it is possible that two (or more) transmitting nodes may determine that there is no activity on the system and both start to transmit at the same time. Intuitively, this means that two bits of the same polarity will add together, and the resultant signal seen by the transceivers exceeds that which could come from a single station. A collision is said to occur. The two or more transmitting nodes that were involved in the collision then wait for a further short random time interval before trying to retransmit again.

It is possible (especially on the standard cable type systems) for the transmitting nodes to see a collision when it occurs (with TTR radios) and to enforce the collision by sending a random bit pattern *for* a short period (called a jam sequence). This would occur before waiting for the random time interval. It ensures that the master site sees the collision.

Exception reporting (or event reporting)

A technique to reduce the unnecessary transfer of data is to use some form of exception reporting. This approach is popular with the CSMA/CD philosophy but it could also offer a solution for the polled approach where there is a considerable amount of data to transfer" from each slave.

The remote station monitors its own inputs for a change of state or data. When there is a change of state, the remote station writes a block of data to the master station, when the master station polls the remote.

Typical reasons for using polled report by exception include:

- The communications channel is operating at a low data rate (say 4800 bps)
- There is substantial data being monitored at the remote stations (say 80 bits or more)
- There are more than 10 RTUs linked to one master station

Each analog or digital point that reports back to the central master station has a set of exception reporting parameters associated with it. The type of exception reporting depend on the particular environment but could be:

- High and low alarm limits of analog value
- Percent of change in the full span of the analog signal.
- Minimum and maximum reporting time intervals

When an analog value changes in excess of a given parameter or an alarm occurs an exception report is generated. A digital point generates an exception report when the point changes state (from a '0' to a '1' or vice versa).

The advantages of this approach are quite clearly to minimize unnecessary (repetitive) traffic from the communications system.

The disadvantages are essentially:

- The master station may only detect a link failure after a period of time due to the infrequency of communication.
- The data in the system is not always the latest and may be up to 30 minutes old for example.
- There is effectively a filtering action on analog values by the master station, as small variations do not get reported once the analog values are outside the limits.
- The operator must manually institute a system update to gain the latest data from the RTUs.

Polling plus CSMA/CD with exception reporting

A practical and yet novel approach to combining all the approaches discussed previously is to use the concept of a slot time for each station. Assume that the architecture is for a master and a number of slaves, which need to communicate with the master station. There is no communication between slaves required (except possibly through the master).

The time each station is allowed to transmit is called a slot time. There are two types of slots:

- A slave (or a few slaves) transmitting to a master.
- A master transmitting to a slave

A slot time is calculated as the sum of the maximums of modem up time (30 milliseconds), plus radio transmit time (100 milliseconds), plus time for protocol message (58.3 milliseconds), plus muting time (25 milliseconds) of transmitter. Typical times are given in brackets after the description.

The master commences operations by polling each slave in turn (and thereafter every 3600 seconds say). Each slave will synchronize in on the master message and will transmit an acknowledged message. The time slots will alternate for the master transmitting and the master receiving. Hence, on a change i_ state of a slave node it will transmit the data on the first master receiver time slot. If two remote slaves try to transmit in the same time slot, the message will be corrupted and the slaves will not receive a response from the master. The slaves will then select a random master receiver time slot to attempt. a retransmission of the message. If the master continues to get corrupted messages, it may elect to do a complete poll of all the remote slaves (as the CSMA/CD type mechanism is possibly breaking down due to excessive traffic).

2.8 Typical considerations in configuring a master station

Before commencing with a detailed discussion, a few factors to bear in mind when designing the system are:

- Simplicity (the 'KISS' principle)
- Minimum response time
- Deterministic type operation (especially for critical signals from RTUs)
- Minimum cost
- Optimum efficiency of operation
- Data format and communication speed (baud rate/stop bits/parity)

While it is difficult to generalize all master stations/RTUs and communication system forming part of a SCADA system, a few considerations is discussed below:

- **Hardware handshaking**
  If a modem is not being used, select 'no handshaking'. If a modem is being used a full or half-duplex one should be considered. .

- **Station address**
  Every station (and RTU) must have a unique address.

- **Error detection**
  Block check (BCC) or cyclic redundancy check (CRC). Preferably select CRC as this gives the best error checking capability. This is discussed later in this book.

- **Protocol message retries.**
  How many retries or messages transmitted before the master station flags this RTU as unavailable? (Typically three retries are standard. It must be noted however that certain sensitive units may require just one retry before the master station flags it as unavailable.)

- **RTS send delay**
  This typically goes with the clear to send signal from the modem. This defines the amount of time that elapses before the message is transmitted. The clear to send line (from the modem) must als9 be asserted before transmission can occur.

- **RTS off delay**
  This is the time that elapses between the end of the message and the inhibiting of the RTS signal. It is important not to intermit the message prematurely by setting this RTS off delay, too short.

- **Timeout delay**
  The timeout delay for a message received from an RTU device.

- **Size of messages from RTU**
  This defines the maximum size of messages allowable from the RTU during a poll by the master station.

- **Priority message transmit**
  This defines when an immediate message is required to be transmitted by the master station, at the conclusion of a poll of an RTU station or when the master station appears in the poll sequence.

- **Poll sequence**
  Define the station addresses in the poll sequence for both priority and normal message transfers.

- **Addressing considerations**
  Each station on a network should have a unique address. One address (normally FF_{16} or 1111 1111) is reserved for broadcast address. Some protocols also reserve certain of the upper address for diagnostic purposes and they should also not be used.

CHAPTER 3

"SCADA systems, software and protocols"

3.1 Introduction

This chapter will focus specifically on SCADA systems and protocol with most emphasis placed on man-machine software.

The following points will be discussed in detail:

- The components of a SCADA system
- The SCADA software package
- Specialized SCADA protocols
- Error detection
- New technologies in SCADA systems
- The twelve golden rules.
-

3.2 The components of a SCADA system

The typical components of a SCADA system with emphasis on the SCADA software are indicated in the diagram below.

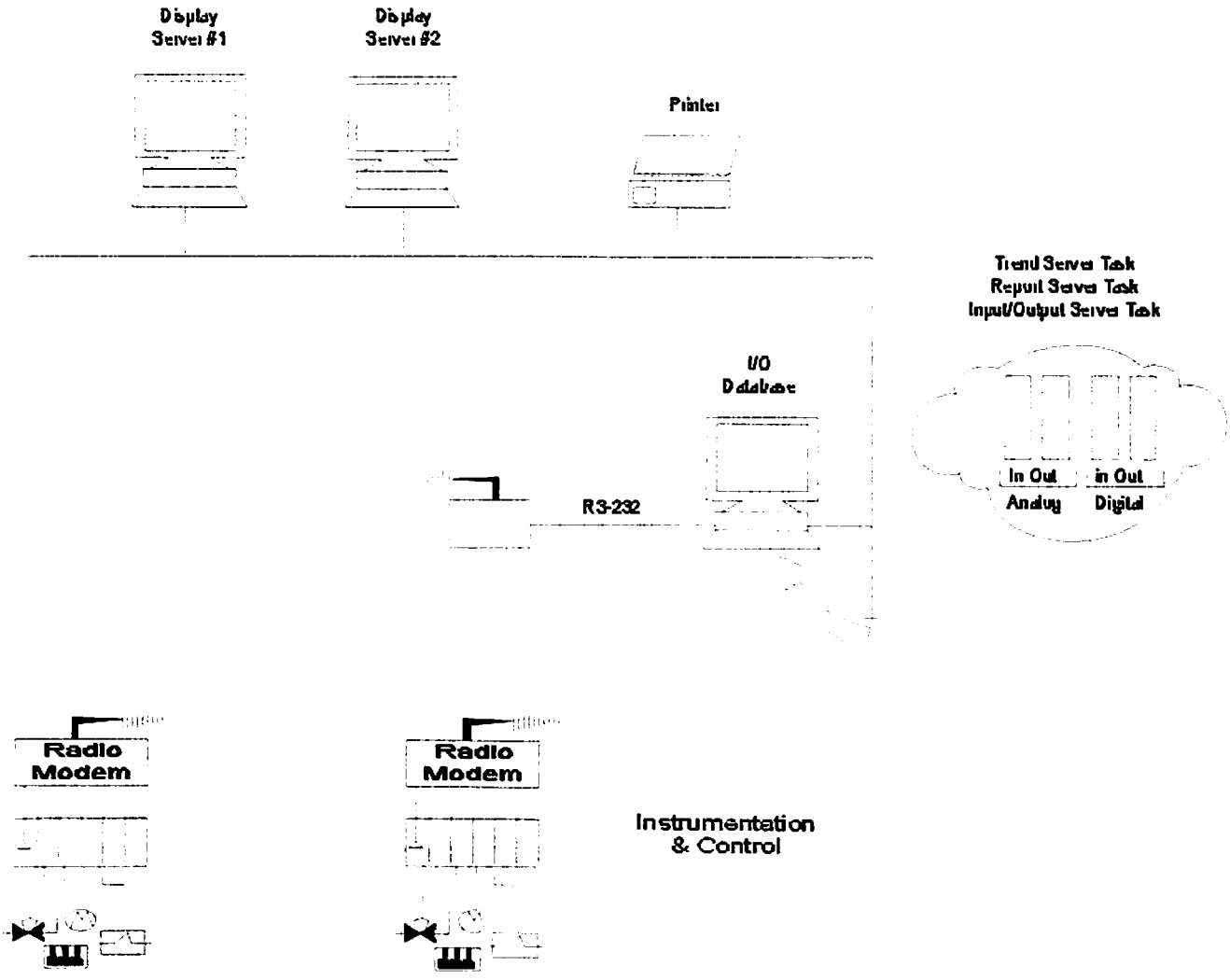


Figure 3.1: Components of a SCADA system

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

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 are 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 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
- XJY plot capability
- Event based trends
- Pop-up trend display
- Trend gridlines or profiles
- Background trend graphics
- Real-time multi-pen trending
- May be enabled via single check box, no configuration
- LAN licensing is 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 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.

3.3 The SCADA software package

While 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 as the requirement change and expandable 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 in the past. They are centralized and distributed.

Centralized, where a single computer or mainframe performs all plant monitoring and all plant data is stored on one database that resides on this computer. The disadvantages with this approach are simply:

- Initial up front costs are fairly high for a small system
- A gradual (incremental) approach to plant upgrading is not really possible due to the fixed size of the system
- Redundancy is expensive as the entire system must be duplicated
- The skills required of maintenance staff in working with a mainframe type computer can be fairly high.

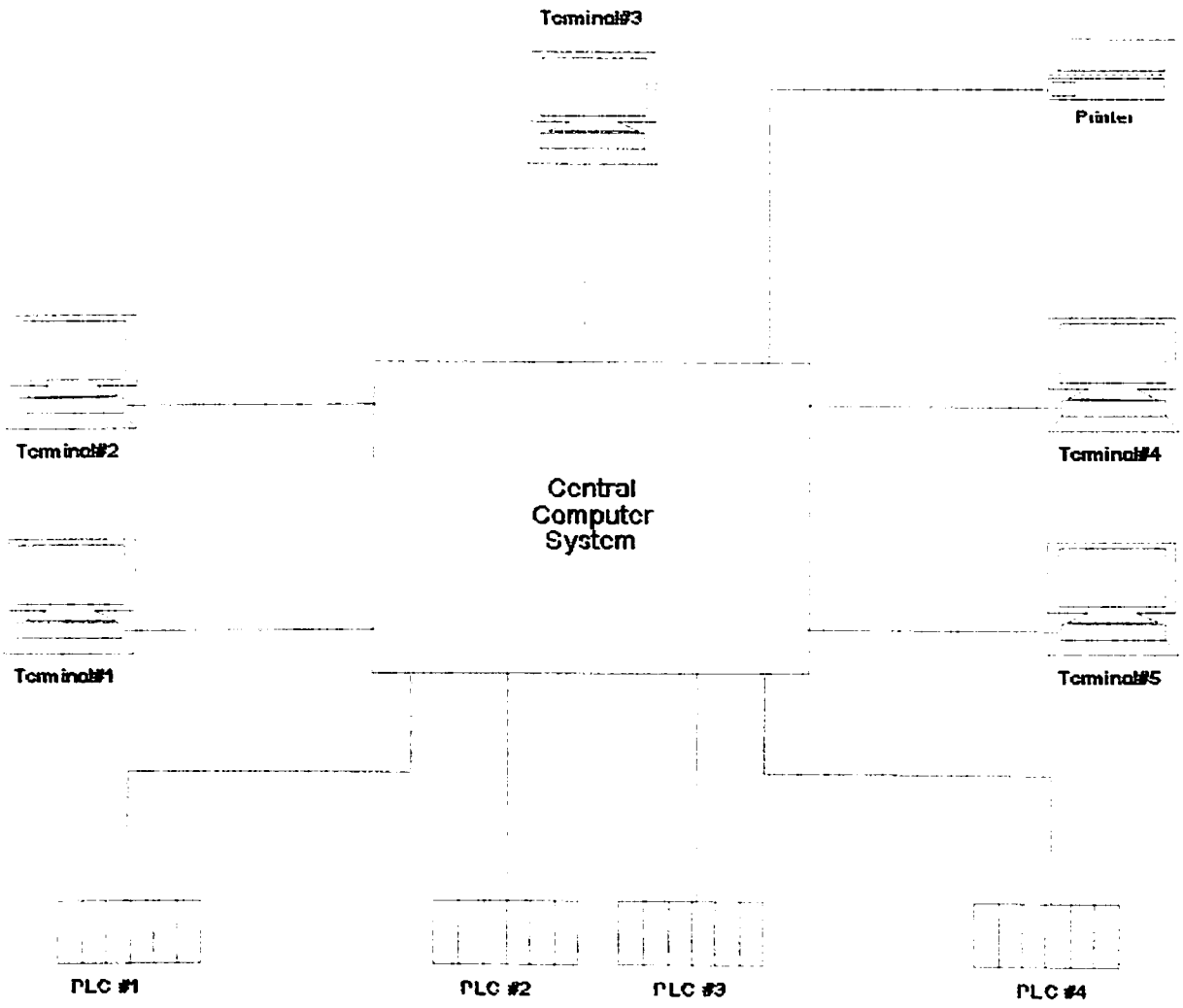


Figure 3.2: Centralized processing

Distributed: In this type, the SCADA system is shared across several small computers (usually PCs). Although the disadvantages of the centralized approach above are addressed with a distributed system, the problems are:

- Communication between different computers is not easy, resulting in configuration problems
- Data processing and databases have to be duplicated across all computers in the system, resulting in low efficiencies
- There is no systematic approach to acquiring data from the plant devices – if two operators require the same data, the RTU is interrogated twice

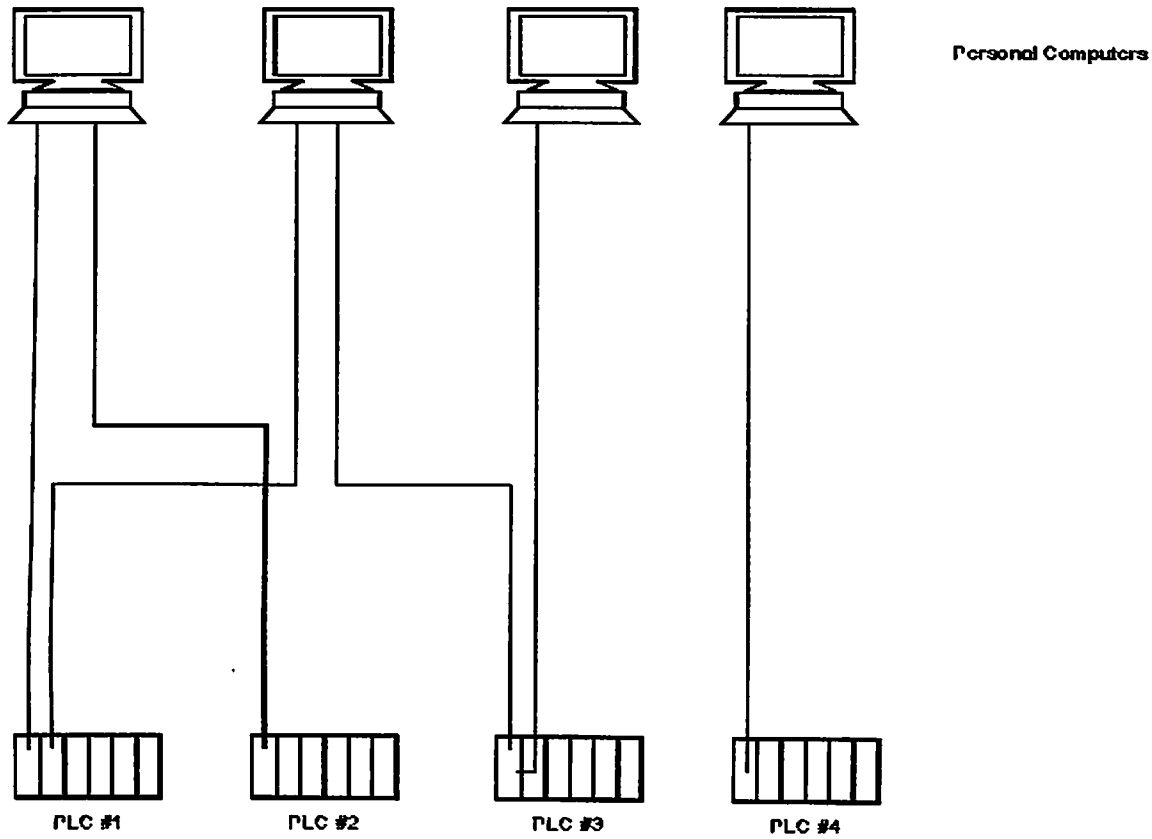


Figure 3.3: Distributed processing

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.
A client server system is understood as follows:
A server node is a device that provides a service to other nodes on the network. A common example of this is a database program. A client on the other hand is a node that requests a service from a server. The word client and server refer to the program executing on a particular node.

A good example is a display system requiring display data. The display node (or client) requests the data from the control server. The control server then searches the database and returns the data requested, thus reducing the network overhead compared to the alternative approach of the display node having to do the database search itself.
A typical implementation of a SCADA system is shown in the figure below.

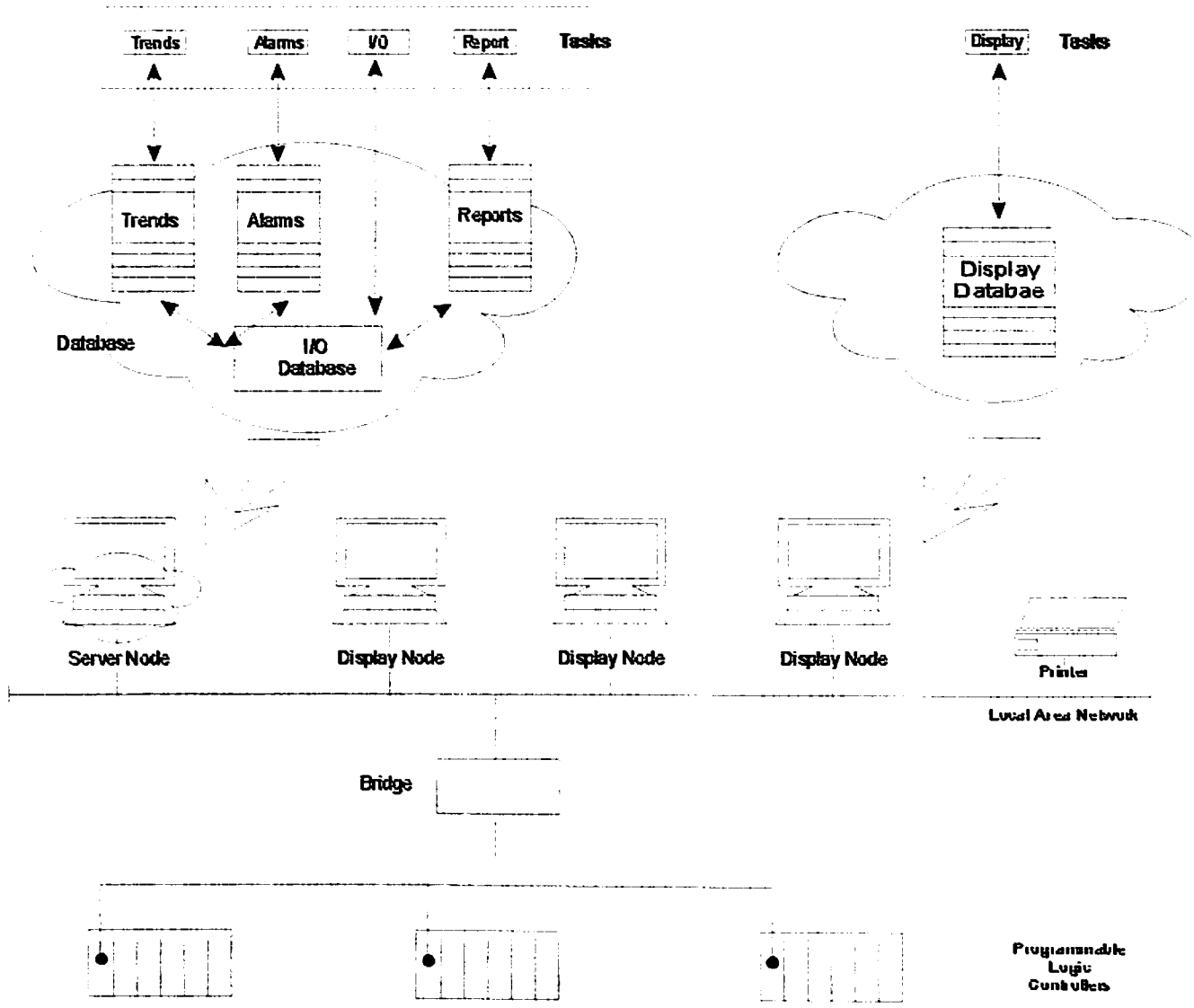


Figure 3.4: Client server approach as applied to a SCADA system

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.

3.3.1 Redundancy

A typical example of a SCADA system where one component could disrupt the operation of the entire system is given in the diagram below.

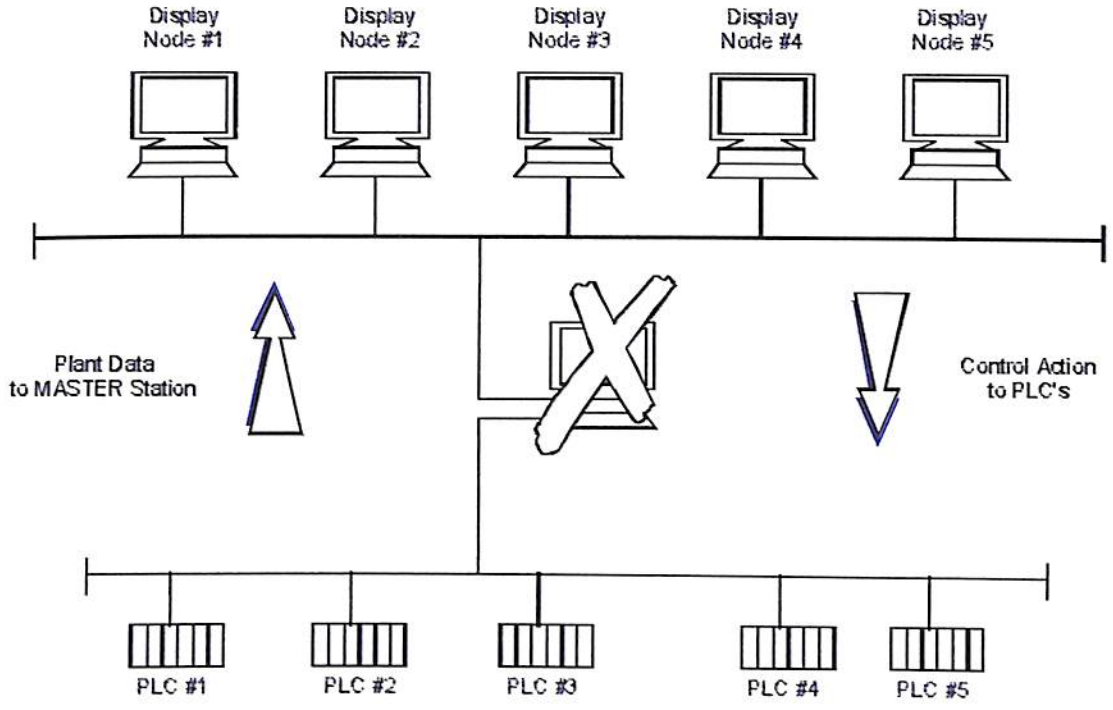


Figure 3.5 The weak link

If any processes or activities in the system are critical, or if the cost of loss of production is high, redundancy must be built into the system.

This can be done in a number of ways as indicated in the following diagrams. The key to the approach is to use the client-server approach, which allows for different tasks (comprising the SCADA system) to run on different PC nodes. For example, if the trend task were important, this would be put in both the primary and secondary servers.

The primary server would constantly communicate with the secondary server updating its status and the appropriate databases. If the primary server fails, the standby server will then take over as the primary server and transfer infom1ation to the clients on the network.

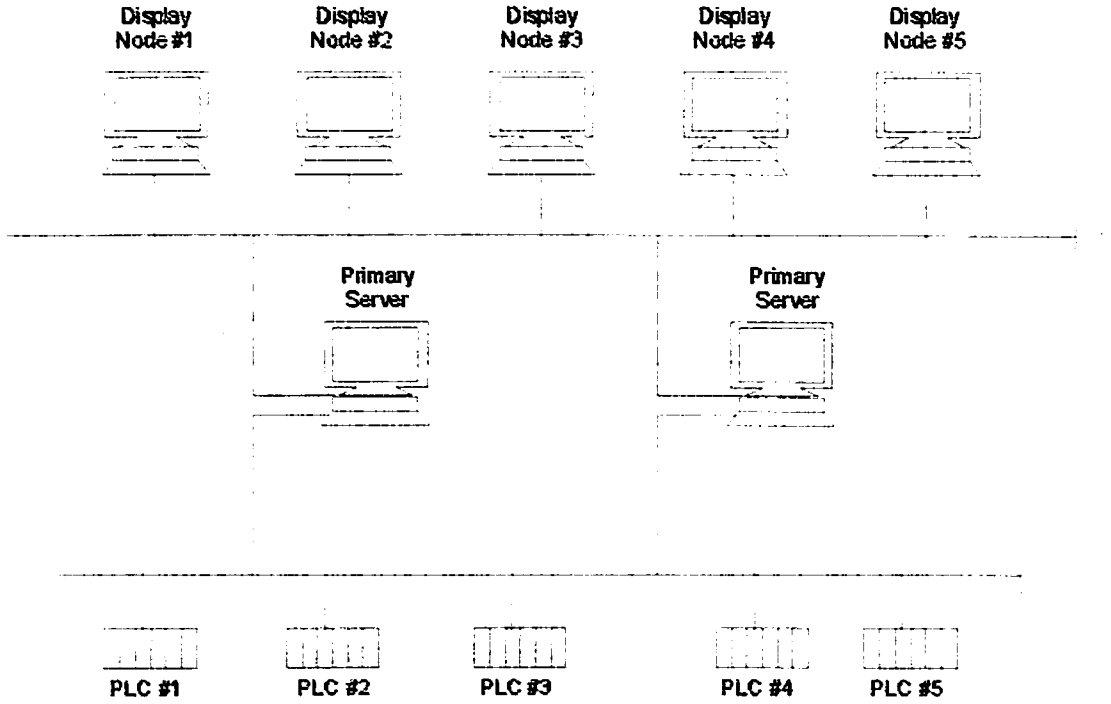


Figure 3.6: Dual server redundancy

3.4 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, MPT 1317 and Modbus protocols. The CSMA/CO protocol format is also used and this has been discussed in Section 2.6. This section will provide an introduction to protocols and also provide a description of a common protocol used in telemetry, the HDLC protocol.

3.4.1 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: This provides the signals to synchronize the receiver and transmitter.
- Information: This provides the data in a coded form to allow the receiver to decode the information and properly utilize it.
- Message termination: This 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.

The message establishment field has three components:

- An 8 millisecond (minimum) pre-transmission mark to condition the modern receiver for the synchronization bits.
- Synchronization: This consists of two bits: a space followed by a mark. The asynchronous interface is designed to start decoding bits after a mark-to-space transition. Therefore the change from the pre-transmission mark to the space provides this transition.
- RTU address: This allows a receiver to select the message addressed to it from the messages to all RTUs on a party line. To avoid any possible mix-ups on addressing the wrong RTU, it is recommended that each RTU in the system has a unique address.

The information field contains 20 bits, of which eight bits are a function code and 12 bits are used for data. For remote-to-master messages, this represents the first message in a sequence, additional messages directly following the first message also transmit information in the RTU address and function code spaces, so that 24 bits of data are transmitted. These 24 bits may contain two 12 bit analog values or 24 device statues. Additional discussion of the use of the information field is contained in the section 'information transfer'.

The message termination field contains:

- BCH (Bose-Chaudhuri-Hocquenghem) security code, which has five bits and allows the receiving logic to detect most message errors. If an error is detected, the message may then be retransmitted to obtain a correct message.
- End of message mark, which provides the last bit as a mark, so that another message can follow immediately after this message (due to the requirement for a mark-to-space transition for synchronization).

3.4.2 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. Other variations of this protocol include SDLC (synchronous data link control used by IBM) and ADCCP (advanced data communication control procedure used by ANSI). HDLC is a bit-based protocol. Other protocols are based on characters (e.g. ASCII) and are generally slower. It is interesting to note that it is a predecessor to the LAN protocols.

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.

3.4.2.1 Protocol operation

A typical sequence of operations is given below.

- In a multidrop link, the primary node sends a normal response mode frame 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 setup command a disconnected mode frame is returned.
- Data is then transferred with the information frames.
- The primary node then sends an unnumbered frame containing a 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.

3.4.2.2 Error control/flow control

The simplest approach for error control is for a half duplex flow of information frames. Each side of the link maintains a send and receive sequence variable. Whenever the receiving node receives a frame it acknowledges with a supervisory frame with a 'receiver ready' indication together with a receive sequence number acknowledging correct sequence of all frames up *to* one less than the receive sequence number. When the

The format of the frame can be briefly described as follows (with reference to each of the fields):

- **Preamble field**
  This allows the receiving electronics of the MAC unit to achieve synchronization with the frame. This field consists of seven bytes each containing the pattern 10101010.

- **Start of frame delimiter (SFD)**
  This contains the pattern 10101011 and indicates the start of a valid frame.

- **Destination and source address**
  Each address may be either 16 or 48 bits. This size must naturally be consistent for all nodes in a particular installation.

- **Date**
  The information to be sent.

- **Length indicator**
  This is a two-byte field, which indicates the number of bytes in the data field.

- **Frame check field**
  This contains a 32-bit cyclic redundancy check that is used for error detection.
  The following sequence is followed for transmission and reception of a frame.

- **Transmission of a frame**

  - Frame contents are first encapsulated by the MAC unit
  - Carrier sense signal is monitored by MAC unit for other transmissions on the media
  - If the media is free, bit stream is transmitted onto the communication medium via the transceiver
  - Transceiver monitor for collisions
  - If a collision, the transceiver turns on the collision detect signal
  - MAC unit then enforces collision by transmitting jam sequence (for LANs, but
  - not necessarily always for radio systems)
  - MAC unit terminates transmission and reschedules a retransmission after a
  - random time interval

- **Reception of a frame**

  - MAC unit detects the presence of an incoming signal from the transceiver
  - The carrier sense signal is switched on to prevent any new transmissions from the MAC unit
  - The incoming preamble is used to achieve synchronization
  - The destination address is checked to see if this is the correct node for reception of this frame.

- Hereafter, validation checks are performed on the frame to confirm that the FCS matches the frame's contents; and it is the correct length

3.5 Error detection

Error detection was briefly discussed earlier under protocols. Most error detection schemes involve having redundant bits transmitted with the message to allow the receiver to detect errors in the message bits (and sometimes to reconstruct the message without having to request a retransmission).

Causes of errors

Typically a signal transmitted across any form of transmission medium can be practically affected by four phenomena:

- Attenuation
- Limited bandwidth
- Delay distortion
- Noise

Each of these will be briefly considered.

- **Attenuation**
  As a signal propagates down a transmission medium its amplitude decreases. This is referred to as signal attenuation. A limit should be set on the length of the cable and one or more amplifiers (or repeaters) must be inserted at these set limits to restore the signal to its original level. The attenuation of a signal increases for its higher frequency components. Devices such as equalizers can be employed to equalize the amount of attenuation across a defined band of frequencies.

- **Limited bandwidth**
  Essentially the larger the bandwidth of the medium the closer the received signal will be to the transmitted one. The Nyquist formula to determine the maximum data transfer rate of a transmission line is:

  Max Transfer Rate (bps) = $2\ B\ \log_2 M$

  where:

  B is the bandwidth in hertz

  M is the number of levels per signaling element.

  For example, with a modem using PSK and four levels per signaling element (i.e. two frequencies) and a bandwidth on the public telephone network of 3000 Hz, the maximum data transfer rate is calculated as:

  Maximum Data Transfer Rate = $2 \times 3000\ \log_2 4$

  = 12 000 bits per second

- **Delay distortion**
  When transmitting a digital signal the various frequency components of the signal arrive at the receiver with varying delays between them. Hence the received signal is distorted with the effects of delay distortion. When the frequency components from different discrete bits interfere with each other, this is known as intersymbol interference. This can lead to an incorrect interpretation of the received signal as the bit rate increases.

- **Noise**
  An important parameter associated with the transmission medium is the concept of signal to noise ratio:

  $$\text{Signal to Noise Ratio} = 10 \log_{10} \frac{S}{N} \text{ dB}$$

  where:
  S = the signal noise power in Watts
  N= the noise power in Watts
  The theoretical maximum data rate *of* a transmission medium is calculated using the Shannon-Hartley Law, which states:

  $$\textit{Max Data Rate} = B \log_2 (1 + S/N) \text{ bps}$$

  where:

  B = the bandwidth in Hz

  S = the signal power in watts

  N = the random noise power in watts

  For example, with a signal to noise ratio *of* 100, and a bandwidth *of* 3000 Hz, the maximum theoretical data rate that can be obtained is:

  Maximum information rate = 3000 log2 (1 +. 100)

  = 19 963 bits per second

There are two approaches to coping with errors in the message; feedback error control in which the receiver detects errors in the message and then requests a retransmission *of* the message and forward error control where the receiver detects errors in the message and reconstructs the message from the redundant data contained in the message. Forward error control will not be discussed here; refer to the modem section for a full treatment *of* this subject. .

3.5.1 Feedback error control

Message security

It is essential to protect against fake control action and corruption *of* data resulting from communication noise. Security is achieved by adding a check code to each transmitted message. The concept is for the transmitting station to calculate the check code from the message pattern. The receiving station then repeats the same check code calculation on the message and compares its calculated check code to that *of* the message received. If they are identical it is assumed that the received message has not been corrupted. If they are different the message is discarded.

Typical security code formats used are:

- **Simple parity check**
  A single bit is added to each byte *of* the message so that *(for* example) each group of bits always adds up to an even number.

- **Block check calculation**
  This is an extension on the single parity check in that a new byte is calculated (at the end of the message), based on parity check or a simple arithmetic sum of bits.

- **2-out-of-5 coding**
  Two out of five bits out of each group of five are set at any given time.

- **BCH (Bose-Chaudhuin-Hacquengham)**

  Each block of data (26 bits) is divided by a complex polynomial and the remainder of the division is added to the end of the message block (typically as a 5-bit code).

- **Cyclic redundancy check (CRC-16 or CRC-CCITT)**

  This is similar in concept to the BCH in that the remainder is a 16-bit code, which is appended to the end of the message. The CRC-16 is probably the most reliable security check, which can easily be implemented.

Three of the most commonly used methods for error detection will be discussed in more detail below.

- **Character redundancy checks**

Before the transmission of the character, the transmitter uses the agreed mechanism of EVEN or ODD parity to calculate the parity bit to append to the character.

For example:

If ODD parity has been defined as the mechanism for transmission of ASCII 0 I 0000 1 this becomes 01000011 to ensure that there are an odd number of 1 s in the byte. For an

EVEN parity scheme the above character would be represented as 0 I 000010. At the receiving end, parity for the 7 bit data bytes is calculated and compared to the parity bit received. If the two do not' agree, an error has occurred.

Parity error detection is not used much nowadays for communication between different computer and control systems and the more sophisticated algorithms available, such as block redundancy parity check and cyclic redundancy check (CRC) are used.

- **Block redundancy checks**

  Character parity error checking discussed earlier is unacceptably weak in checking for errors. There are two methods of improving on this described below. The parity check on individual characters is supplemented by a parity check on a block of characters.

- **Parity check (vertical/longitudinal redundancy check)**

  In the block check strategy, message characters are treated as a two dimensional array. A parity bit is appended to each character. After a defined number of characters, a block check character (BCC), which represents a parity check of the columns, is transmitted. Although column parity (also referred to as vertical redundancy check) is better than the character parity error checking, it still cannot detect an even number of errors in the rows.

- **Arithmetic checksum**

  An extension of the vertical redundancy check is to use an arithmetic checksum, which is a simple sum of characters in the block. This provides even better error-checking capabilities and also increases the overhead as two bytes now have to be transmitted.

- **Cyclic redundancy check (CRC)**

  This provides a worse case probability of detecting errors of 99.9969%.

There are two types of CRC calculations performed.

- CRC-CCITT (popular in commercial systems)
- CRC-16 (popular in industrial systems)

The CRC checksum is calculated by dividing the message by a defined number (known by the receiver and transmitter of the message) and c' calculating the remainder. The remainder is known as the CRC checksum and is appended onto the end of the message.

CRC example
The following equation can be proven:

$$\frac{\text{Message} \times 2^{16}}{\text{Divisor}} = \text{Quotient} + \text{Remainder}$$

where:

Message is a stream of bits, for example; the ASCII sequence of H E L P with even parity.

[01001000] [11000101] [11001100] [01010000]
H E L P

- 2^{16} effectively (in multiplying) add on 16 zeros to the right hand part of the message.
- Divisor is a number, which is divided into the message x *i6* number.
- Quotient is the result of the division and is not used.
- The remainder is the value left over from the result of the division and is the CRC checksum (a two-byte number).

3.6 Distributed network protocol

3.6.1 Introduction

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 RS-232 (V.24), but it also supports other physical standards such as RS-422, RS-485 and even fiber optic. There is large support within the SCADA industry to use DNP as the universal *de facto* standard for data acquisition and control.

3.6.2 Interoperability

The distributed network protocol is an interoperable protocol designed specifically for the electric utilities, oil, gas, and water/waste water and security industries. As a data acquisition protocol, the need to interface with many vendors equipment was and is necessary. By having a certification process, the protocol ensures that different manufacturers are able to build equipment to the DNP standard. This protects the end user when purchasing a certified DNP device. As more and more manufacturers produce DNP certified equipment, the choices and confidence of users will increase.

3.6.3 Open standard

The DNP was created with the philosophy of being a completely open standard. Since no one company owns the DNP standard it means that producers of equipment feel that they have a level playing field on which to compete. This allows different manufactures to have equal input into changes to the protocol. In addition, it means that the cost to develop a system is reduced. The producer does not need to design all parts of the SCADA system. In a proprietary system, the manufacturer usually has to design and produce all parts of the SCADA system, although some of those parts may not be so profitable. One manufacturer is free then to specialize on a few products that are its core business. .

3.6.4 IEC and IEEE

DNP is based on the standards of the International Electro technical Commission (IEC) Technical Committee 57, Working Group 03 who have been working on an OSI 3 layer 'Enhanced Performance Architecture' (EPA) protocol standard for telecontrol applications. DNP has been designed to be as close to compliant as possible to the standards as they existed at time of development with the addition if functionality not identified in Europe but needed for current and future North American applications Recently DNP 3.0 was selected as a recommended practice by the IEEE C.2 task force, remote terminal unit to intelligent end device's communications protocol.

3.6.5 SCADA

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 then 1 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.

3.6.6 Development

The specification was first developed by the GE Harris Company but has been released under the DNP User Group since 1992. Now over 100 vendors offer DNP V3.0 products. These products range from master stations to intelligent end devices. The protocol is designed so that a manufacturer can develop a product that supports some but not all of the functions and services that DNP supports. The DNP 3.0 was derived from an earlier version of the IEC 870.5 specs. The DNP users group now controls the documenting and updating of the protocol. For users of the DNP a copy of the protocol can be purchased through http://www.dnp.org

3.6.7 Physical layer

The physical layer of DNP is a serial bit oriented asynchronous system using 8 data bits, 1 start bit, 1 stop bit and no parity. Synchronous or asynchronous is also allowed. It has two physical modes of operation, direct mode (point-to-point) or serial bus mode (multi-drop). The two modes are not usable at the same time. Both modes can be half or full duplex. With either mode, a carrier detection system must be used. The DNP protocol is a modified master/slave system. Multi-masters are allowed but only one device can be a master at a time. There are possible collisions on the system. The configuration of the physical layer determines the method of collision avoidance or recovery. The DNP can prioritize devices in a multi-master mode.

3.6.8 Physical topologies

The DNP protocol supports five communication modes, two-wire point-to-point, two wire multidrop, four-wire point-to-point, four-wire multidrop, and dial up modems. A system with only two nodes, a master and a slave is called a direct bus. If the system IS multidrop with multiple nodes, it is called a serial bus. Both of these systems can use two or four wire connection methods. The two wire method can only run half duplex while the four wire method can run either half or full duplex. The DNP supports multiple master, multiple slave and peer-to-peer communications.

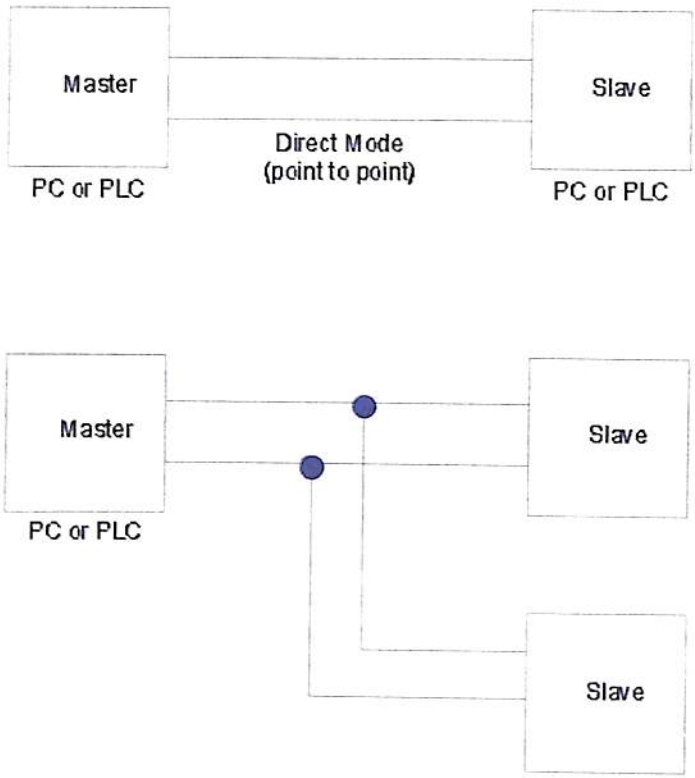


Figure 3.8: Direct and serial modes

3.6.9 Datalink layer

The datalink layer of the DNP defines the frame size, shape, length and contents. DNP uses the convention of the octet instead of byte. The DNP uses hexadecimal as a language within the frame. The frame is laid out as follows

3.6.10 Transport layer (pseudo-transport)

The distribution network protocol does not support a true transport layer as defined by the ISO open system interconnection model. It does support a pseudo-transport layer known as the super-data link transport protocol. This is because some of the functions of the data link layer do not strictly meet the ISO OSI model. These functions are then moved out of the data link layer and placed in this pseudo-transport layer. These data link functions

consist of breaking the transport service data unit (TSDU) into smaller sequenced frames called link service data units (LSDU). Each of these frames has transport protocol control information. The maximum size of an LSDU is 249 octets. This is done to reduce the length of Packets in case of errors. If a packet is in error, then a retry will be initiated. A shorter packet means that the retries will be quicker.

3.6.11 Application layer

The DNP supports an application layer by defining an extensive data object library, function codes and message formats for both the requestor and the response devices. These are used in the USER layer to build a final application. Once this application is built and the data objects function codes and message formats are absorbed the application becomes the application layer. A complete list of data objects and function codes can be found in the DNP version 3.0 standard documents available from DNP users group http://www.dnp.org. And other information can be found at Harris controls division. *http://www.harris.com/harris/search.html*

3.6.12 Conclusion

The distributed network protocol only supports the physical layer, data link layer and application layer within the open system interconnection model. The physical layer is the least supported. DNP is based on the enhanced protocol architecture (EP A), a protocol standard for telecontrol applications. It supports advanced RTU functions and messages larger than the normal frame length. It takes user data and breaks it up into several sequenced transport protocol data unit (TPDU) each with transport protocol control information (TPCI). The transport protocol data unit is sent to the data link layer as a link service data unit. The receiver receives multiple sequenced transport protocol data unit (TPD Us) from the data link layer and assembles them into one transport service data unit (TSDU).

There is no official compliance testing, but there is help online. If a vendor claims to comply with one of the DNP v3.00 subset definitions, then the device is definitely interoperable. Of course interoperable does not mean efficient. It is often best to stick with one supplier when possible. The distributed network protocol is truly an open non-' proprietary interoperable protocol.

3.7 New technologies in SCADA systems

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

3.7.1 Rapid improvement in LAN technology for master stations

LANs are increasingly forming a key component of the master stations with dual redundant LANs being able to provide very reliable systems. The movement to higher speed LANs (100 Mbit/sec up from 10 Mbit/sec) are providing faster response times.

3.7.2 Man machine interface

Typical areas where improvements are occurring are:

- Improved graphics on the VDUs with the operator planning and zooming on the system on-line to arrive at any given subset of the network.
- Improved response times on the operator interfaces.

3.7.3 Remote terminal units

- Decentralized processing of the data at the RTD rather than the master station.
- Further decentralized gathering of data from intelligent instruments, which transfer the data back to the RTD over a communication network
- Redundancy of RTUs is easily implemented on I/O, CPD, power supplies etc.
- Multiple communications with multiple masters with partitioned (separate) databases for each master station .
- User generated programs could be run in the RTD to reduce the number of alarm traffic to master station (by combining alarms, filtering or irrelevant alarms) .
- Checking on the validity of real-time data received
- Inter RTD communications (rather than through the master stations)
- Sophisticated man-machine interfaces directly connected to RTD

3.7.4 Communications

- Open standards (i.e. non-vendor specific) are appearing to interface RTUs to the master stations
- Spread spectrum satellite - an improved, low cost and low power method of transferring data over a satellite system for remote site RTUs
- Fiber optics - lower cost and ease of installation is making this an attractive option.
- Meteor trail ionization - this is becoming an effective technology today especially where it is difficult to justify the cost of a satellite system

3.8 The twelve golden rules

A few rules in specifying and implementing a SCADA system are listed below:

- Apply the 'KISS' principle and ensure that the implementation of the SCADA system is simple.
- Ensure that the response times of the total system (including the future expansion) are within the correct levels (typically less than one-second operator response time).
- Evaluate redundancy requirements carefully and assess the impact of failure of any component of the system on the total system.
- Apply the open systems approach to hardware selected and protocols communication standards implemented. Confirm that these are indeed TRUE open standards.

- Ensure that the whole system including the individual components provide a scaleable architecture (which can expand with increasing system requirements).
- Assess the total system from the point of view of the maximum traffic loading on the RTD, communication links and master stations and the subsequent impact on hardware, firmware and software subsystems.
- Ensure that the functional specification for the system is clearly defined as far as number of points are concerned, response rates and functionality required of the system.
- Perform a thorough testing of the system and confirm accuracy of all data transferred back, control actions and failure of individual components of system and recovery from failures.
- Confirm operators of individual components of the system in the (industrial) environment to which they would be exposed (including grounding and isolation of the system).
- Ensure that all configuration and testing activities are well documented.
- Ensure that the operational staffs are involved with the configuration and implementation of the system and they receive thorough training on the system.
- Finally, although the temptation is there with a sophisticated system, do not overwhelm the operator with alarm and operational data and crowded operator screens. Keep the information of loading to the operator clear, concise and simple.

Chapter 4

"Telemetry in Pipelines"

4.1 Data transmission and Telemetry

In modem measurement systems, the various components comprising the system are usually located at a distance from each other. It, therefore, becomes necessary to transmit the data, or information between them through some form of communication channels.

The terms *data transmission* and *telemetry* refer to the process by which information, regarding the quantity being measured, may be using a transducer and a signal conditioning equipment, is transferred to a remote location, perhaps to be processed; recorded and displayed. Telemetry is the technology which enables a user to collect data from several measurement points at inaccessible or inconvenient locations, transmit that data to a convenient location, and present the several individual measurements in a usable form.

4.2 Methods of Data Transmission

The transmission of a measured variable to a remote point is an important function in Instrumentation systems because of the size and complexity of modern industrial plants. The most common variables encountered in industrial plants are temperature, pressure, and flow. Most measuring devices for these variables such as mercury thermometers, pressure gauges or flow rate meters would require fluid-line connections of great length from the place of measurement to the place of data recording or display. This will result into excessive *measurement lags.* Hence, there is a need for fast transmission of data.

The methods employed for data transmission depend upon the variable and the distance over which it has to be transmitted. The following methods may be used for data transmission:

(i) Hydraulic transmission,
(ii) Pneumatic transmission, and
(iii)Electrical and Electronic transmission.

The electrical and electronic methods of data transmission are extensively used in Instrumentation and measurement systems.

4.3 General Telemetry System

Telemetry may be defined as measurement at a distance. A general telemetering system is shown in Figure 4.1. The primary detector and the end device of the telemetering system have the same position and functional roles as in a generalized measurement system.

However, there are three system elements in the intermediate stage which are peculiar to a telemetering system, they are:
(i) telemeter transmitter
(ii) telemeter channel and
(iii) telemeter receiver.

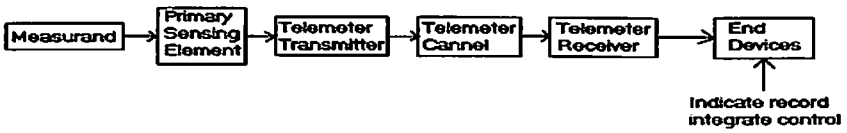


Figure 4.1: General telemetering system

The function of the telemeter transmitter is to convert the output of a primary sensing element into an electrical signal and to transmit it over a telemetering channel. This signal is in electrical format and is received by a receiver placed at a remote location. This signal is converted into a usable form by the *receiver* and is indicated or recorded by an end device which is graduated in terms of the measurand. The end device may be a control element which may be used for the control of the input quantity (measurand), through a feedback loop to produce desired output.

4.4 Types of Telemetry system

Two types of telemetering systems are used:
(i) Land Line Telemetry
(ii) Radio Frequency Telemetry

4.4.1 Land Line Telemetering System

A land line telemetering system requires a telemeter channel which is a physical link between the telemeter transmitter and receiver. This physical link may be a cable, a specially laid out wire, existing telephone and telegraph, cables or a power line carrier. The land line telemetering is, in fact, a direct transmission of information through cables and transmission lines. The direct transmission via cables employs current, voltage, frequency, position or impulses to convey the information. Current, voltage and position type systems can be used only for short distances while for long distance telemetering pulse and frequency type of systems are used. The information may be in the form of analog or digital signals. While current; voltage, position, frequency and pulse types of signals can be used for analog telemetry, only pulse signals can be used for digital telemetry.

The land line telemetry systems can be classified as :

(i) voltage telemetering systems
(ii) current telemetering systems, and
(iii) position telemetering systems.

4.4.2 Radio Frequency Telemetry

The telemetry, earlier on, has been defined, as a technology that enables the user to collect data from several measurement points at inaccessible or inconvenient locations. This is very true of applications which require Radio Frequency (R.F.) telemetry, as in such applications; there is no physical link between the transmitting and receiving stations. The link, between the transmission station (where the actual measurements are being carried out) and the receiving station (where the measurand is measured, recorded and information used for control purposes) can only be established through radio links.

R.F. telemetry is usually more suitable if the data is to be transmit over distances greater than 1 km. Certain parts of the radio-frequency spectrum have been allocated for telemetry, and microwave links about 4 MHz.
Radio waves, at these frequencies tend to travel in straight lines, requiring repeater stations with disc like antennas on high buildings and towers (every 30 to 60 km)

Radio links with airborne instrumentated flight vehicles often use Pulse Duration Modulation (PDM) --- Frequency Modulated (FM) systems, with pulse duration varying from a minimum of about 700 micro-seconds.

4.5 Modulation techniques

In essence, the modulation process modifies the characteristics of a carrier signal. The carrier signal can be represented as a sine wave:

$f(t) = A \sin (2 ft + \cos)$

Where:
$F(t)$ = instantaneous value of voltage at time t
A = maximum amplitude
F = frequency
Phi = phase angle

The various modulation techniques are as follows:

4.5.1 Amplitude modulation (or amplitude shift keying)

The amplitude of the carrier signal is varied in correspondence with the binary stream of data coming in.

ASK or amplitude shift keying is sometimes still used for low data rates; however, it does have problems with distinguishing the signal from noise in the communications channel, as noise is amplitude based phenomena.

4.5.2 Frequency modulation (or frequency shift keying - FSK)

This approach allocates different frequencies to the logic 1 and logic 0 of the binary data messages. This is primarily used by modems operating at data rates up to 300 bits per second (bps) in full-duplex mode and 1200 bps in half-duplex mode.
The Bell 103/113 and the compatible CCITT V.21 standards are indicated in Table 4.1.

Specifications	Originate(Mark)	Originate(space)	Answer(Mark)	Answer (Space)
CCITT.21	980 Hz	1180 Hz	1650 Hz	1850 Hz
BELL 103	1270 Hz	1070 Hz	2225 Hz	2025 Hz

Table 4.1 CCITT V.21 and BELL system 103/113 modems frequency allocation

The Bell 103/113 modems had to be set up in either 'originate' or 'answer mode'. Typically, terminals were connected to originate modems and main frame computers were connected to answer type modems. It is thus easy to communicate when originate modems are connected to answer mode modems. Similar modems cannot communicate with each other as they expect different frequencies (e.g. two originate modems connected together).
Because of the two different bands of frequencies in which the sets of signals operate full duplex operation is possible with these modems. Note that they fit into the allowable bandwidth of the communications channel.

4.5.3 Phase modulation (or phase shift keying (PSK)

This is the process of varying the carrier signal by phase. There are various forms of phase modulation. In quadrature (four phases) phase shift keying (QPSK) four phase angles are used for encoding: 0°, 90°, 180° and 270° as indicated in Figure 4.2 .
There are four phase angles possible at any possible time; thus allowing the basic unit of data to be a 2-bit pair (or digit). The weakness with this approach is that a reference signal is required as shown in the figure below:

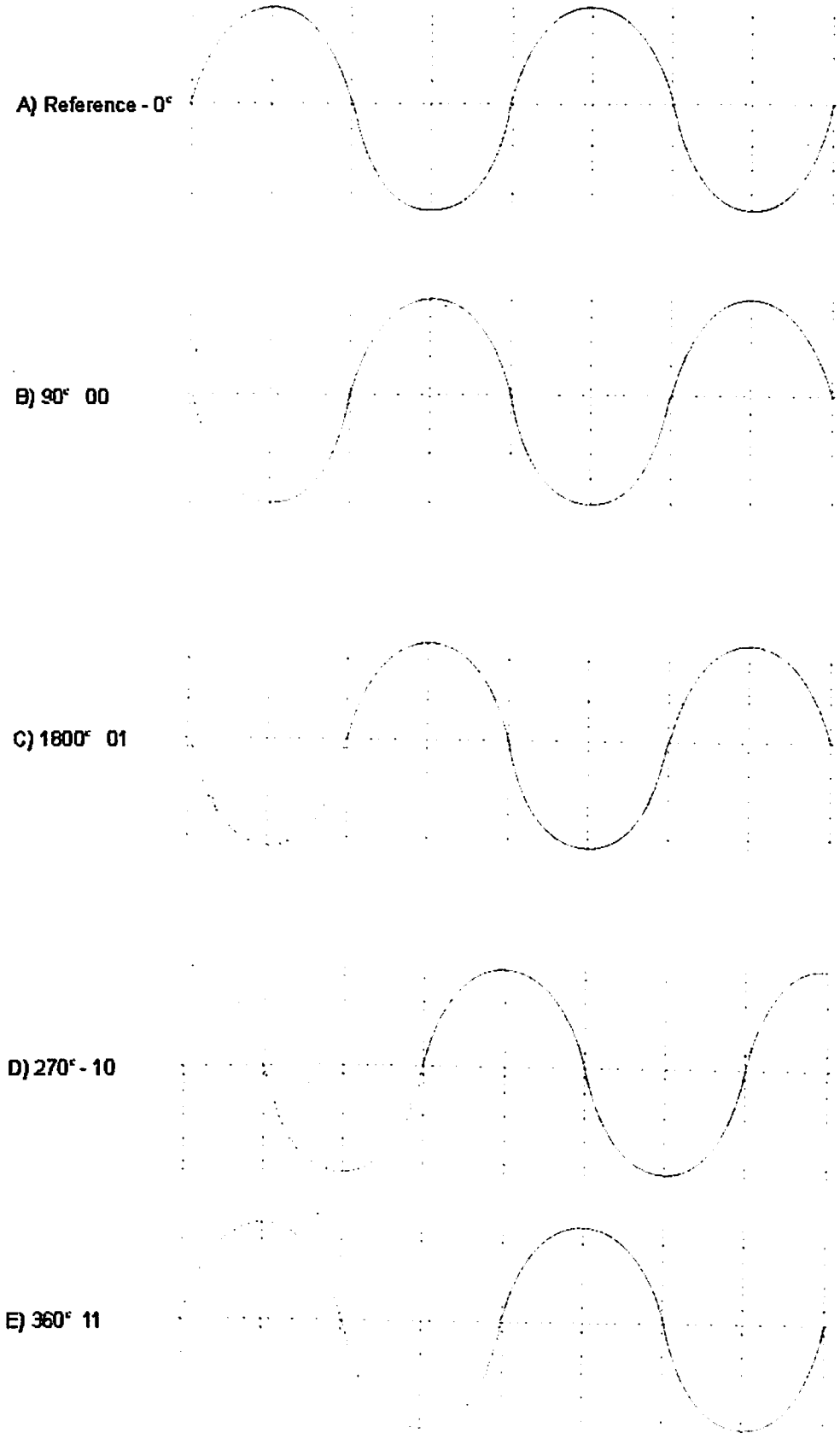


Figure 4.2 Quadrature phase shift keying

The preferred option is thus to use differential phase shift keying where the phase angle for each cycle is calculated relative to the previous cycles as shown in Figure 4.3.

A modulation rate of 600 baud results in a data rate of 1200 bits per second using two bits for each phase shift.

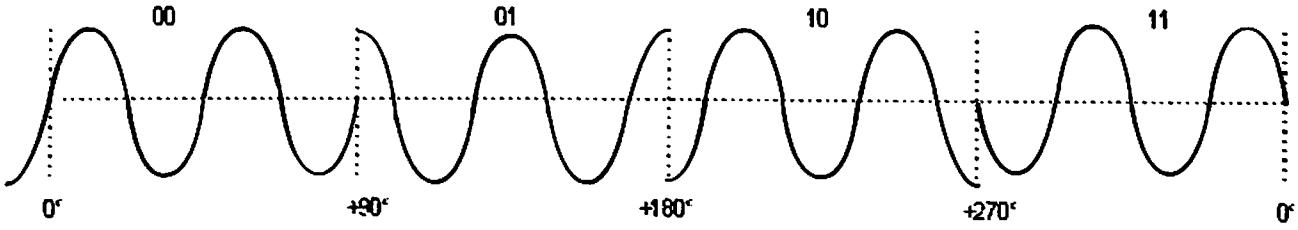


Figure 4.3 Differential phase shift keying

4.5.4 Quadrature amplitude modulation (or QAM)

Two parameters of a sinusoidal signal (amplitude and phase) can be combined to give QAM. This allows for 4 bits to be used to encode every amplitude and phase change. Hence a signal at 2400 baud would provide a data rate of 9600 bps. The first implementation of QAM provided for 12 values of phase angle and 4 values of amplitude.

QAM also uses two carrier signals. The encoder operates on 4 bits for the serial data stream and causes both an in-phase (IP) cosine carrier and a sine wave that serves as the quadrature component (QC) of the signal to be modulated. The transmitted signal is then changed in amplitude and phase resulting in the constellation pattern.

4.5.5 Trellis coding

QAM modems are susceptible to noise; hence, a new technique called trellis coding was INtroduced. These allow for 9600 to 56 k bps transmission over the normal telecom lines. In order to minimize the errors that occur when noise is evident on the line, an encoder adds a redundant code bit to each symbol interval.
Only certain sequences are valid. If there is noise on the line, which causes the sequence to be different from an accepted sequence, the receiver will then select the valid signal point closest to the observed signal without needing a retransmission of the affected data.

A typical comparison in performance would be that of a conventional QAM modem that might require 1 of every 10 data blocks to be retransmitted, could be replaced by a modem using trellis coding with only one in every 10 000 data blocks to be in error.

4.5.6 DFM (Direct Frequency Modulation)

This is mentioned as a separate form of modulation for completeness. It is one method of modulating digital information with an analog modulator. However it can be considered to be a form of FSK. It is widely referred to in radio communications. The correct technical name is 'Gaussian minimum shift keying' (GMSK)
It is possible to directly modulate the data directly onto the radio frequency carrier. This cannot be done within the normal telephone lines because of bandwidth limitations (3 kHz as opposed to radio channel bandwidths of 12.5 kHz). Simple filtering of the square wave (binary) data signal ensures that the channel spectrum is indeed limited to 12.5 kHz. This method of modulation is used in some radio systems that claim to be 'digital radio'. In reality, it is a hybrid of digital and analog systems and not a true digital transmission technique.

Comparison of FM, PAM & PCM

COMMENTS	FM	PAM	PCM
Efficiency in use of radio or tape recorder bandwidth	Medium	Best	Worst
Cost of a small transmitting system	Lowest	Low	Highest
Size	Smallest	Small	Largest
Cost of a large transmitting system	Highest	Lowest	Medium
Size	Largest	Smallest	Large
Cost of small receiving system	Lowest	Higher	Highest
Cost of large receiving system	Highest	High	High
Accuracy	Poor	Poor	Excellent
Percent of use(Approximate)	20	15	65

Table 4.2 Comparison of FM, PAM & PCM

Chapter 5

"Central site computer facilities"

5.1 Introduction

The central site computer facilities have to be designed and installed to ensure the satisfactory operation of the hardware and software and to ensure that the operators and other users can use the system effectively and safely.

This chapter discusses the requirements for the central site computer facilities with reference to the following:

- Recommended installation practice
- Ergonomic requirements
- Design of the computer displays
- Alarming and reporting philosophies

5.2 Recommended installation practice

There are a number of requirements, which have to be carefully adhered to in installing the computer system in a building. These are reviewed in the following paragraphs.

5.2.1 Environmental considerations

The environment in which the system is installed must be appropriate to the computer system and the associated electronics systems. Typical environmental conditions that are considered suitable for the standard and the industrial environment are listed in Table 7.1. Obviously, the environment in a control room should not have these extremes; but the equipment should be rated for these ranges. Typical control room environmental ranges are discussed under ergonomic requirements. Industrial computer systems may be mounted in a less stringent environment than for the standard air-conditioned control room.

Environmental Condition	Recommended	Range
Operating Temperature	Industrial 0oC to 60oC	Standard 0oC to 50o C
Storage Temperature	Industrial -40oC to 85o C	Standard -10o C to 60o C
Relative Humidity	Industrial 5 to 95% RH	Standard 5 to 90% RH

Table 5.1 Environmental Conditions

The enclosure should be large enough to allow space to work on the system and to observe diagnostic lights/LEDs etc.

5.2.2 Earthing and shielding

Ensure that all hardware is securely earthed. The earth electrode is the central point for all electrical equipment and AC power within the facility. Use the maximum size copper wire (say, 8 A WG) for the earth.

Certain connections require shielded cables to reduce the effects of electrical noise. Ensure that only one end of the shield is earthed. As discussed in a previous chapter, earthing at both ends of a shielded cable should be avoided, as it will cause an earth loop in the cable.

5.2.3 Cabling

Full details on allowable distances for separating power and communications cables are given in Chapter 4. Some points to emphasize when installing communications cabling between the different computers and systems in the control room are listed below:

- Calculate the actual distance the cable is being run - i.e. both the horizontal and vertical distances. Select the shortest possible path away from sources of noise.
- Route the cables well away from potential sources of electrical interference, harsh chemicals, excessive heat, wet environments and sources of physical damage.
- Ensure that no one will walk or drive on the cable.
- Ensure that the cable is not put under undue tension (such as hanging between two points).
- Do not bend the cable excessively in the installation process.

5.2.4 Power connections

For installations near sources of electrical interference, an isolation transformer is a recommended approach. Note that the output devices being controlled should draw power from the original source of the voltage unless the secondary of the isolation transformer (which is supplying the computers) has been specifically rated for these additional devices.

Where the AC power source has variations, a constant voltage (CV) transformer can stabilize the voltage for short periods of time, thus minimizing shutdowns. It is worth noting here, that CY transformers are very sensitive to variations in main frequency and will not operate successfully with unstable mains frequency supplies.

For both the constant voltage transformer and the isolation transformer the operating frequency and the operating voltage should be carefully specified (e.g. 240 Y AC + 1 0% -15% or 50 Hz ± 2%).

It is important to size transformers correctly:

- If the transformer is too small it will clip the peaks off the sine wave (due to saturation) resulting in a lower rms value of the voltage. The power supply could sense this as a low voltage and shutdown. The transformer may also overheat and burn out.

- Excessively large transformers do not provide as much isolation as a correctly sized transfom1er, due to higher capacitive coupling.

Useful techniques to reduce the electromagnetic interference and switching transients are given in Figure 5.2

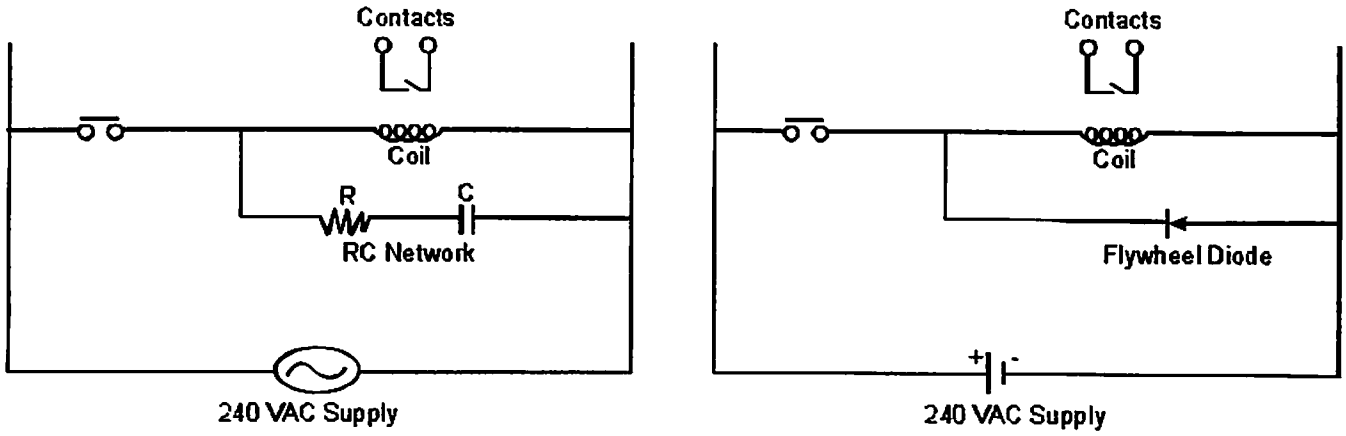


Figure 5.1 Techniques for reducing EM interference and surges

5.3 Ergonomic requirements

The main reason for considering ergonomic requirements is to improve the working environment of control room personnel. In the long run this should improve the productivity and reliability of the overall system.

The majority of tasks in a computer control room can be broken down into the following:

- Monitoring of the system
- Control adjustments
- Alarm/emergency procedures
- Staying awake

5.3.1 Typical control room layout

A typical layout is given in Figure 5.2

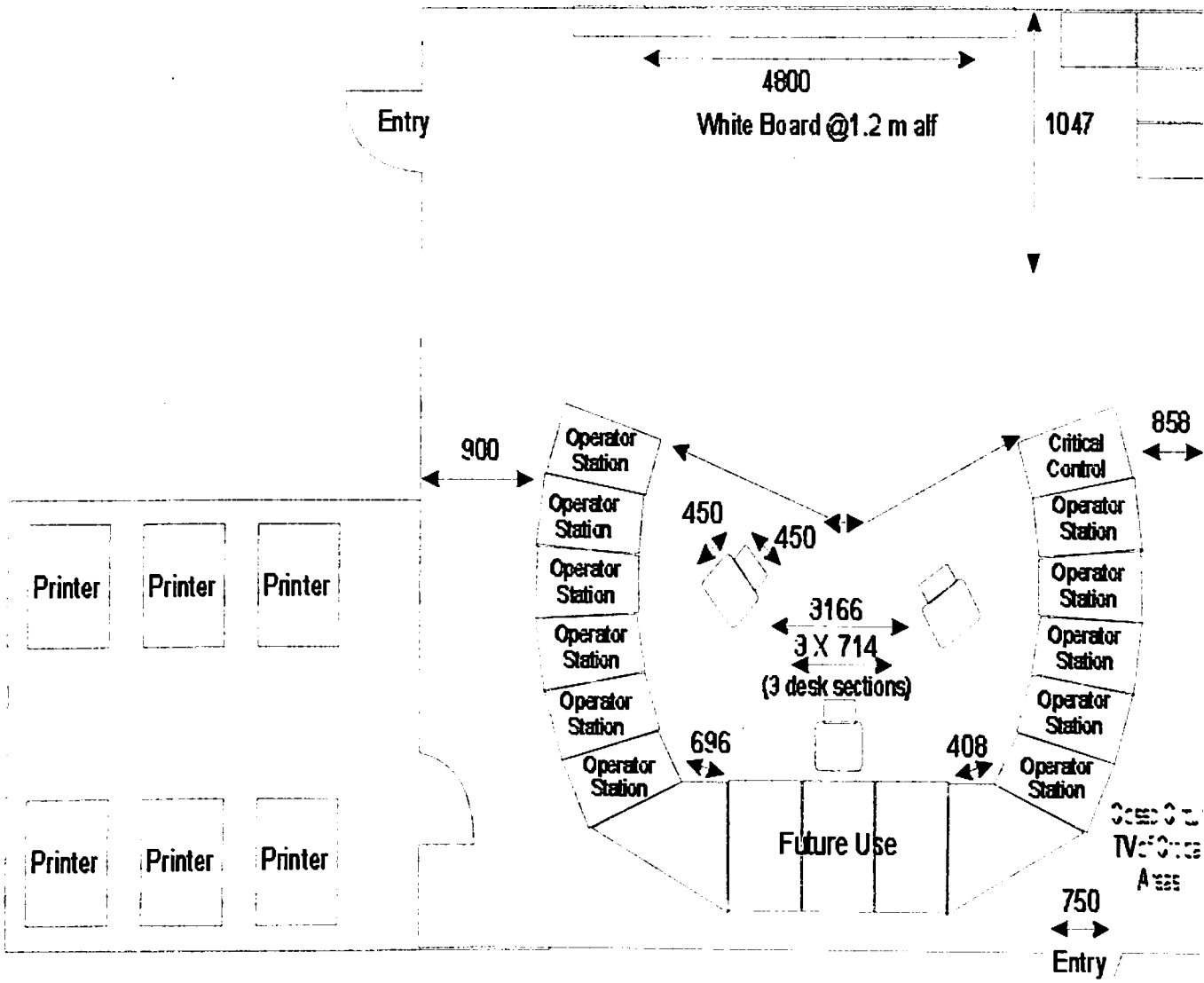


Figure 5.2 Typical layout of the computer control room

The horseshoe control *room* layout is designed so that anyone in the center can see all the screens. Operators at any *of* the operator displays should be able *to* view the entire control room's screens without undue difficulty as well.

Although the focus in a control room is normally on the equipment and computers, the amount *of* space *for* the operators should also be maximized to avoid congestion (particularly when there is a change over *of* shifts). Operators will spend a considerable amount *of* time in front *of* their consoles and the layout should ensure that the operator can see anyone coming into the control *room* and not have people peering over their shoulders.

Similar areas in the system that are being monitored should be situated close together to avoid unnecessary movement by the operators *to* see what is going on.

The voice communications system (either radio or telephone) should be situated as close as possible *to* the operators and *for* other persons entering the control room. For the control room indicated in the diagram at least three internal telephones should be provided *for* easy access (with frequently used numbers programmed into the system).

The amount *of* desk space should not be compromised. Space should be allowed for manuals and other items *to* be left on the desk without unnecessary clutter.

The printers for the system are situated in a separate *room to* isolate the operators from the associated (rather repetitive) noise. The associated inconvenience *of* having to walk *to* the printer *room* to view alarms can be minimized by providing on-screen alarm reports.

A separate meeting room should be. provided to avoid holding meetings in the control room which are *of* no interest to the operator but which disrupt his \\ork. The following specific issues should also be considered in the design *of* the computer control room.

5.3.2Lighting

Tungsten halogen light sources produces warm lighting while the light life of 2000 to 4000 hours is reasonable. They are also not diffused and can produce significant shadowing. If longer life is required tubular fluorescent lamps have a life *of* 5000 to 10000 hours but may have variable color rendering and variable apparent color if the correct color tube is not chosen.

The luminaries should be fixed overhead and provide direct lighting. Desk lighting can be installed *to* provide localized lighting over the keyboard. A general level *of* lighting of 400 lux is recommended throughout the control room with a personal level of 200 to 600 lux set by the operator.

An average reflectance level of 30 to 60% is recommended for the walls. The ceiling should have a reflectance *of* at least 75% with floors an average of 40°10.

5.3.3 Sound environment

A maximum noise level *of* 54 *to* 59 dB (A) is recommended.

5.3.4 Ventilation

The air temperature should be between 20oe and 26°e with relative humidity range *of* 40 to 60% RH fresh air should flow at the rate *of* 7 liters/see per person throughout the control room.

5.3.5 Colors of equipment

Colors for walls and equipment should have a matt finish (i.e. no shiny surfaces) to avoid irritating reflections from the operator displays. Strong contrasts in color should also be avoided to minimize glare.

Where the general light level is low (less' than 300 lux) warm color schemes are more acceptable than th9se in which cold colors pre dominate. A pleasant color scheme can be achieved with warm colors backed up with cool secondary colors.

5.4 Design of the computer displays

The objective of this discussion is to provide a useful set of guidelines for the design of an effective operator display system. The approach should be to ensure that the displays are as easy to read and understand as possible. This reduces the decoding process in the human brain to a minimal level and maximizes the decision-making processes of the brain. This ensures that the operator can react quickly and effectively without having to work out where the problem is.

Typical hardware that is provided is:

- One or more operator displays (which may be of the touch type)
- Industrial (or Mylar) type keyboards which have audible or tactile feedback
- Operator panels consisting of highlighted keys to bring up predefined graphic displays
- Printers (one for alarms and one for reports)
- Alarm buzzers (or external sirens)

(A useful addition although possibly expensive option is a video copier for reproducing the operator screens in color.)

5.5 Alarming and reporting philosophies

Alarm processing is an important part of the operator station. Error codes identifying the faults are normally included with the description of the failed device.

No other part of the operator display has as much impact on the health of the plant (and that of the operator). The alarm function should be viewed as an integral part of the operator interface and not as a stand-alone feature. Figure 5.4 gives a view on the actions that occur on an alarm being activated.

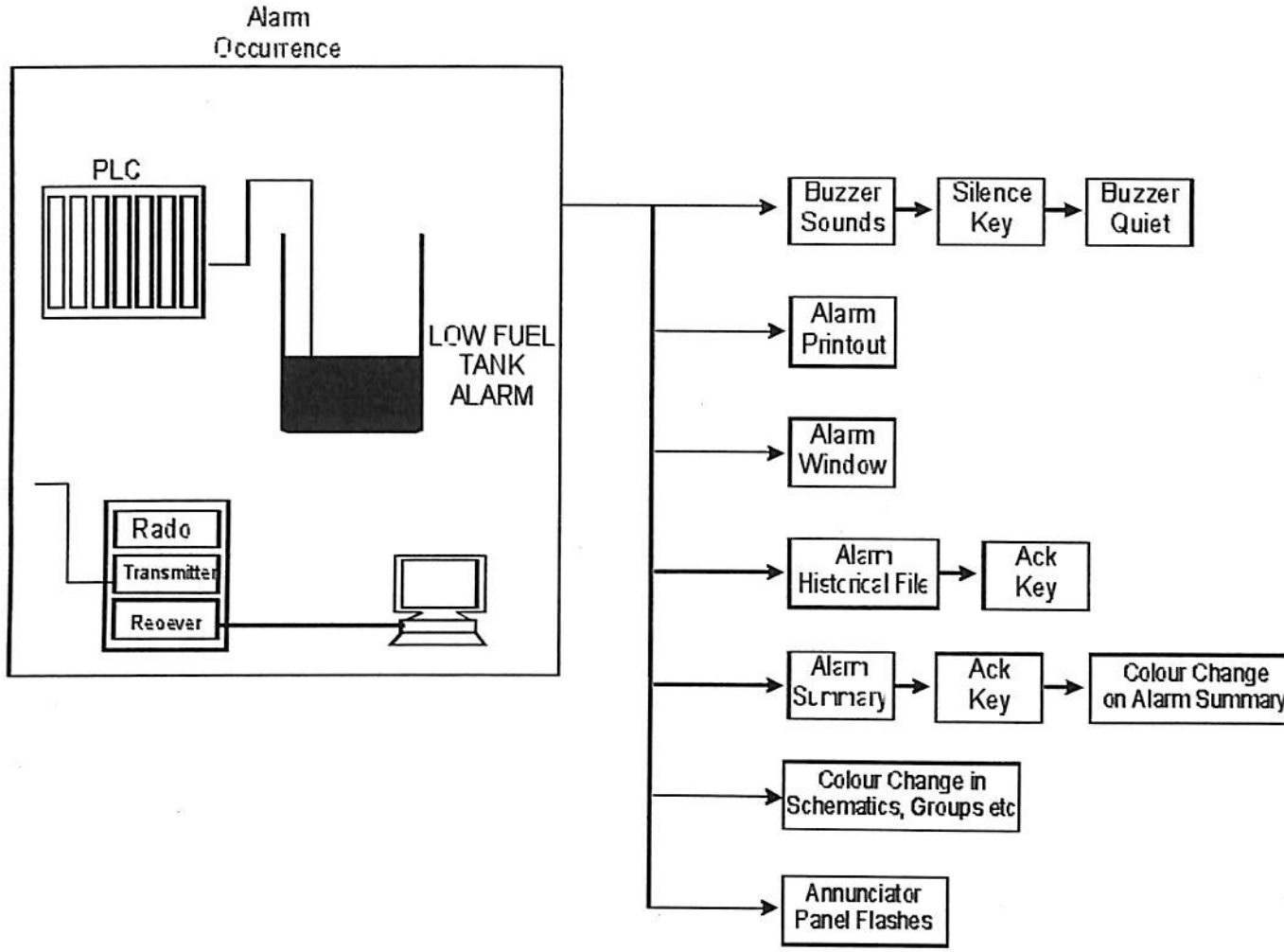


Figure 5.3: Alarm actions in an operator display

Another approach as opposed to the pure screen listing of alarms is to have an associated enunciator panel (situated next to the operator display) with illuminated pushbuttons. Each pushbutton would indicate the area from which the alarms originate and also when depressed would cause the appropriate schematic to appear on the operator display.
Only four alarm priorities should be implemented. These are:

- **High priority**
  Alarms that warn of dangerous conditions that could cause a shutdown of a major Activity.
- **Medium priority**
  Alarms that should be acted on as quickly as possible; but will not cause a shutdown.
- **Low priority**
  Alarms that should be dealt with when time permits.
- **Event only**
  Statistical or technical information. No enunciator sounds for these.

The limiting of the number of types of alarms is to keep the system straightforward and with easy interpretation of the alarms. Higher priority alarms should be louder; lower pitched and have a higher pulse frequency than the lower priority alarms. Alarms are classified as unacknowledged (and flashing on the screen) until the operator acknowledges them via the keyboard. They then become an accepted alarm. One weakness in many alarm systems is the occurrence of trivial alarms, which irritate and confuse the operator. Typical trivial alarms are summarized in the table below:

Type of alarm	Symptom	**Remedy**
Consequential	Repetitive alarms caused by a condition that the operator is aware of	Inhibit the alarm until the condition is remedied
Out of service	Alarms are caused by equipment not in service	Inhibit the alarms
No action alarms	Operator unable to rectify the problem	Delete the alarm from the system
Equipment changes	Regular equipment maintenance etc causes alarms	Ensure the alarms are suppressed for this period by added alarm logic
Minor event	Operator constantly being notified about trivial events	Delete alarm and replace with event recording
Multiple	Many alarms triggered by one fault	Use first up alarming to reduce the alarm information
Cycling	Signal close to alarm level moves the alarm in and out of alarm condition	Expand the range of signal before moving into alarm
Instrument drift	Drift of instrument causes alarm	Ensure there is tight control on the calibration of instruments

Table 5.2 List of trivial alarm

It is important to continuously audit, maintain, and improve on the alarm through analysis and review with the operators on the performance of the system. For every alarm the following should be documented:

- Type of alarm
- Alarmed tag
- Description of tag
- Reasons for alarm
- Relationship to related alarms (consequential relationships)
- Description of the logic in the generation of the alarm
- Possible causes of the alarm
- Action steps to take to remedy the alarm situation

Alarms should be able to be disabled provided the operator has the relevant key. Suggested colors for alarms could be:

RED	High Priority
MAGENTA	Medium Priority
YELLOW	Low

Table 5.3 Colour coding

CHAPTER 6

"PROBLEMS IN SCADA & SOLUTIONS"

6.1 Cyber Security

Cyber security is the protection of enterprise information systems from outside or inside attack. The reliance of a typical wastewater utility on its automated systems is substantial: many operators rely on the Supervisory Control and Data Acquisition (SCADA) system to aid in running the plant, the financial system maintains fiscal equilibrium, and several other systems facilitate most business processes. Financial pressures have decreased the staff at most facilities to the point where few, if any, utilities can run in "manual mode" for log. In short, if the information systems do not work, the enterprise will not operate.

Problem Description:

Cyber Intruder Attack Methods and Consequences

Information system failure can have catastrophic repercussions to a utility. Compromise of the financial system can result in millions of dollars of lost revenue. Corruption or destruction of operational data can lead to fines due to late or inaccurate regulatory reporting. A sabotaged Web site has the potential to shake public trust during a time of crisis. Interruption of plant processes because of a SCADA system malfunction can lead to a wide range of health implications for the community. With millions of Internet attacks recorded daily, there is no shortage of potential intruders to the enterprise. For the purposes of the following cyber security discussions, intruders are defined as:

• Hackers: The primary goal of hackers is unauthorized entry; their motivation is thrill-seeking or criminal opportunity.

• Attackers: The primary goal of attackers is to destroy enterprise operations; their motivation is often political.

• Insiders: The primary goal of insiders—typically disgruntled employees—is to disrupt enterprise operations; their motivation is personal vengeance or financial gain. To maintain consistency with discussions of physical security in other sections of this document, the Exhibit 5-1 provides a correlation between physical intruders and cyber intruders. Information systems are more vulnerable than ever before. Today's information management trends point to a technology convergence resulting in standardized system architecture. A demanding regulatory environment and the need for defensible decision-making push today's utilities to integrate previously isolated information systems onto standardized platforms. In addition, employees increasingly request round-the-clock access to internal information systems. Taken together, these trends create more opportunities for intruders to access and affect the entire enterprise information structure.
Correlation between Physical and Cyber Intruders.

Physical Intruder Equivalent Cyber Intruder

Vandal Hacker
Criminal Hacker
Saboteur Attacker
Terrorist Attacker
Insider Insider

Gaining unauthorized entrance to an organization's information infrastructure is no longer the province of a small cadre of skilled intruders. The specific vulnerabilities of widely used platforms, like Microsoft WindowsTM, are detailed on numerous web sites. An arsenal of hacking tools is readily available on the Internet at no cost. These "freeware" programs are easy to operate and effective at gaining entrance to organizations via the Internet, radio, telephone, or wireless. Novice hackers can generate destructive virus code from special applications with no knowledge of programming. This shorter learning curve benefits an attacker intent on intrusion and destruction. Cheap laptops, anonymous Internet accessibility, and readily available hacking tools offer political organizations a potent tactical weapon.

Cyber Security Policies and Procedures

The most effective course of action available to utility management is the creation of a cyber security plan (often done within the context of a physical security plan). A cyber security plan provides the policies, procedures, and direction for system enhancements that minimize intrusion risk as well as insider malfeasance. It is, however, an unfortunate reality that even the most vigorous anti-intruder security may not thwart a determined attacker. The SCADA system is of particular concern. Any disruption to the accurate operation of the SCADA system could have adverse health repercussions to the community. A specialized assessment of the SCADA system is recommended due to its marked difference from a more traditional information technology (IT) system. It is worth noting that the trend in automation systems is to use a more "open architecture" that does not rely on proprietary vendor protocols. The result is a more publicly available standardized operating platform, which increases the odds that its vulnerabilities are more widely known. The centerpiece of a cyber security plan is its policies. Publicized and enforced policies an reduce the opportunity for an insider to anonymously sabotage any portion of the information system. Elements of this plan should include:

- A process for granting/revoking access to information systems
- Password policies
- Restricted information flow between the business and control networks
- Comprehensive system documentation
- Outlawing of unauthorized wireless or modem connections
- A Disaster Recovery Plan
- Incident response goals.

A forward-looking plan also provides a method for continuous security improvements. In this rapidly evolving field, it is essential to stay current. Several organizations are in the process of formulating cyber security standards.

Vulnerability Assessment

A valuable tool for management to understand those portions of the enterprise system that are at greatest risk is the cyber security VA. A VA is a focused examination of the entire business and control network from a security perspective. Each component is evaluated for its degree of susceptibility to outside or inside attack. Based on analysis of the utility's DBT, specific recommendations aimed at preventing the most likely types of attacks are developed. Given that the typical wastewater utility often deploys an array of specialized information systems, the vulnerability assessment should consider systems residing on the business network as well as systems on the control network. These systems are defined below for the purpose of this document.

Business Network

The business network generally hosts software applications and databases that facilitate enterprise business, scientific, and engineering processes, such as:

- **Enterprise Resource Program.** A comprehensive financial program that includes modules for General Ledger, Accounts Payable, Accounts Receivable, Payroll, and possibly Human Resources.

- **Laboratory Information Management System.** A repository of laboratory result information and process data to support regulatory compliance and treatment plant operations.

- **Computerized Maintenance Management System.** A work order system to provide preventative maintenance on assets, such as pumps.

- **Customer Information System.** A financial system that facilitates customer invoicing and collection, and resolving customer complaints.

- **Internet/Intranet.** A network of networks that provides customers and employees with the ability to interact around-the-clock from any computer.

Additional systems might include e-mail, permitting, geographic information system, fuel sage, and others.

Control Network

The SCADA system consists of numerous electronic components distributed in the plant and over a large geographic area. The system's main function is to oversee and operate the pumps, valves, and instruments that control the collection, treatment, and disposal of wastewater. Operable elements of the SCADA system are located in wide range of facilities, including the treatment plant, pump stations, lift stations, vaults, and pretreatment facilities. Though SCADA systems vary widely in their composition, the following represents a typical list of components, grouped by function:

• **Computers**
- SCADA servers
- SCADA Human Machine Interface (HMI) programming workstations
- SCADA HMI workstations and view nodes

• **Networking**
- Switches (optical and Ethernet)
- Routers
- Hubs
- Firewalls
- Modems
- Serial interfaces (connecting telephone lines to SCADA devices)

• **Data Conveyance**
- Ethernet cabling
- Optical cabling (e.g., plant loop)
- Telephone lines (leased or owned)
- Radio transmitters and antennas
- Wireless transmitters and antennas
• Distributed Control Components
- Programmable logic controllers (PLCs)
- Remote terminal units (RTUs)

Operational Solution: Intrusion Defense

Cyber intruders can gain access to an enterprise network via one of four broad avenues: external attacks via the Internet, the telephone system, wireless transmitters, and internal attacks via normal modes of access. The following subsections outline methods of preventing unauthorized entry from each avenue. It should be noted that management, operational, and design considerations for cyber security should coordinate with planning for the security of the overall organization. For example, card-reader access systems may have been specified in the physical security plan to regulate access to restricted areas. Card readers can also benefit cyber security by doubling as a log-on device that can record who has logged in and out of a computer.

Internet Intrusion
Internet access to the enterprise is not always under the control of the utility IT department. It is common for a utility's umbrella municipality to administer all security aspects of the Internet gateway, including firewall configuration and intrusion detection system (IDS) oversight. In that case, it is important for utility staff to participate in municipal IT matters via technical committees or similar intra-organization forums in order to participate in security matters.

Protection against Outside Hackers
The outside hacker is most easily deterred at a firewall. If no entry point is penetrable, the hacker will likely move on and choose an easier target. To improve prevention:

• Coordinate with the enterprise or utility IT department to allow penetration tests on the Internet firewall. These tests are designed to uncover "open ports" commonly used by hackers to gain entrance to the enterprise network. Once inside, a hacker is free to access

any computer on the business network, including SCADA computers if the business and control networks are connected.

• Restrict general user access to critical applications. For example, locate the financial servers on a separate network segment with tightly restricted access.

Protection against Outside Attackers

Even the most daunting security at the Internet gateway may succumb to the efforts of a determined attacker. Additional steps are necessary to further secure the SCADA system if connections exist between the business and control networks. All network traffic between the two networks should be strictly controlled to regulate legitimate connections. The most secure option is to separate the networks. However, there may be business advantages to keeping them linked. If the networks are linked, the link may be programmed to activate automatically at certain times of the day or week for a specified duration to perform certain functions such as backing up data onto access-controlled portions of the business network server.
Methods of securely segmenting the business and control networks include:

• **Virtual Air Gap.** Allows one-way data traffic from a control network server to a business network server by means of an optical isolator.

• **Dual-homed Server.** Directs SCADA process data into a database server via one network card on the control side; allows access to the database only from the other network card on the business network.

• **Router.** Restricts traffic to a small number of destinations as regulated by an Access Control List (ACL). The policy governing the router ACL should ensure that only appropriate Internet Protocol (IP) addresses (such as a designated printer or the email server) can be accessed across the business and control system networks.

• **Firewall.** Of particular value in the case where utility IT department has no control over the enterprise Internet gateway.

Devices such as firewalls and routers, if properly configured, can effectively insulate a utility's networks from outside attack. It is recommended that the utility appoint an appropriately skilled staff member or consultant to determine the current best practice in Internet intrusion design because these technologies are evolving rapidly. Important design elements at the time of this writing are listed below:

• Ensure the firewall is either "stateful packet inspection" or "proxy" served. For additional security, these two firewall types can be implemented together in a "layered" approach.

• Install an IDS at the Internet gateway and regularly audit IDS logs for evidence of unauthorized entry. An IDS system, properly monitored, can identify when a firewall is under attack and provide valuable information about intrusion attempts. Other IDS tools can detect system configuration changes and log file anomalies.

• Contract for periodic evaluation of firewall and IDS effectiveness by a third-party security specialist to continuously maintain and improve operational performance.

• Consider using a Virtual Private Network (VPN) solution to ensure secure access to inside the enterprise from the Internet. A VPN is a private network that uses a public network, such as the Internet, to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. Well-designed VPNs use firewalls, encryption, and other techniques to improve security. In addition to segmenting the business and control networks to protect against Outside Attackers, conduct server and workstation software audits to ensure the operating systems are "hardened" with the most current upgrades and security-related patches. The Microsoft WindowsTM operating system, for example, is a favorite target of hackers because of its widespread use and well-docum entedsecurity flaws. Some specific activities associated with this audit might require that utility es:

• Verify anti-virus software is updated with the latest virus patterns. Verify all servers have latest security patches applied for applications (e.g., database programs, and email) as well as the operating system.

• Review system logs for inappropriate activity.

• Confirm that all administrator passwords for operating system and HMI have been changed from the default passwords.

Telephone System Intrusion

The most common method of telephone system intrusion is via dial-up modem. Most SCADA systems employ a modem to facilitate maintenance of the HMI by vendor or in-house SCADA technicians. Traditionally, these modem connections have little or no security, making them anattractive target for "war-dialing" (a common technique used by telephone hackers that uses a software program to automatically call thousands of telephone numbers to look for any that have a modem attached).
The following operational and design tips can help the utility protect against intrusion via modem:
• Most modems can be configured to only allow dial-up access to a restricted set of telephone numbers. Consider also setting up a dial-back system to verify numbers.

• Leave modems connected to the SCADA system turned off. Turn on only for use by verified personnel (vendor or SCADA technician).

• Use a timer device to turn off modems after a preset period of time (e.g., one hour) if not in use.

• Coordinate with the enterprise IT department to verify security on non-SCADA modems connected to the business network.

• Create policies designed to prevent the installation of unauthorized modems on enterprise equipment. Those modems are often used in conjunction with remote control software to facilitate working from home. The security risks to the business usually outweigh the convenience for the individual. Commercial telephone-scanning software can usually identify modem connections not sanctioned by the utility.

• Equip all SCADA modems with "lock and key" hardware devices. Distribute the "keys" to SCADA technicians and trusted vendors only. This solution provides flexibility as well as a higher degree of security. Many utilities appreciate the benefits of allowing vendors to access their systems remotely. For example, vendors of gas monitoring equipment can troubleshoot, calibrate, and maintain their equipment remotely, saving the utility money and irritation. "Lock and key" modem options allow technicians needing access to call at any time and from any telephone (e.g., a SCADA technician on travel), thus retaining flexibility while decreasing security risk.

• Instruct employees not to divulge user information—especially passwords—over the telephone. Hackers have a high success rate of obtaining passwords from unwary employees by posing as an IT technician needing user account information. This technique is known as "social engineering." Train employees to report any attempt to elicit password information via social engineering.

• Telephone lines are also sometimes used to connect RTUs from the field. Consider encrypting commands to prevent interference from attackers "tapping" into leased or owned lines.

Wireless Intrusion

The explosion of wireless networking at home and in the workplace has created an enormous security risk for network administrators. Many wireless installations in the workplace exist without the knowledge of the IT group. These installations generally have little or no security and can be accessed by anyone within signal range.

The well-documented security flaws of wireless networking increase operational and design requirements for a secure implementation. To bolster system security against a wireless attack:

• Eliminate unauthorized wireless networking—use wireless detection software and appropriate antenna/laptop to identify unauthorized installations. A wireless access point using the default settings is very vulnerable to network attack. Many wireless products are capable of configuration to acceptable levels of transmission security.

• Specify wireless networking configurable to the appropriate security level. Turn off "beaconing" and minimize broadcast area through a combination of antenna-type/placement and wireless access point configurations.

In addition to local wireless networks, many utilities rely on radio transmission to interact with remote SCADA components in the field. RTUs in the field exchange monitor and control information in "plain text." These unencrypted broadcasts can be intercepted and retransmitted with different— potentially harmful—information. To prevent interception.

• Encrypt radio traffic between RTUs (or PLCs with radio units) to master unit with scrambler/descrambler devices. As an alternative, modify radios with appropriate capabilities to spread spectrum frequency-hopping. This technology can be used for voice networks as well.
• Provide "hardened," lockable enclosures for all remote control system units. Many of these units are in located in isolated areas with few protective measures to deter vandalism.
• Provide signal supervision and tamper alarms to detect loss of signal and tamper attempts.

Insider Intrusion

Although an inside attacker has a decided advantage by possessing access privileges to the enterprise system, a more stringent security environment renders all operational staff activities less anonymous. A well-designed cyber security plan seeks to minimize inadvertent or intentional damage to the SCADA system by former or current employees and contractors (i.e., "insiders"). At the core of any security plan is an enforceable security policy and accompanying procedures that promote operational accountability and auditability. An effective policy reduces the chances of acting anonymously, and restricts potential damage through limited access privileges, both physical and electronic. The wastewater utility industry is often staffed by long-term employees. The introduction of more stringent security procedures can be perceived that the utility no longer trusts its employees. The current security-minded national environment, however, supports the perception that procedural changes to protect the enterprise are inevitable. Several security practices that promote accountability and auditability are part of this mainstream movement, including:

• Developing security policies and posting them in all control rooms.

• Requiring individual logon credentials to access the SCADA system.

• Configuring HMI log-on privileges to match responsibility level.

• Ensuring HMI log files associate user log-on credentials with actions and changes made to the HMI (creating a non-refutable audit trail of operator actions).

• Requiring appropriate password strength rules for user access (i.e., more "complex" passwords for higher access privileges).

• Automatically deactivating passwords after a certain time has passed without use.

• Immediately removing a user account from the HMI if the account becomes inactive due to voluntary, and especially involuntary, termination.

• Configuring an inactivity timeout log-out (or proximity sensor log-out) to protect the control system if no one is present in the control room or the user has stepped away from a remote workstation.

• Safeguarding laptops used for onsite programming of remote PLCs or RTUs against theft or unauthorized use.

• Requiring a password to make software programming changes to RTU/PLCs.

• Programming set point ranges to reject potentially harmful out-of-range adjustments.

Physical Security of SCADA Components

While extensive efforts may be undergone to secure cyber portals to SCADA and business networks, sensitive electronic components are often completely accessible to anyone in the plant. The utility can reduce crimes of opportunity by:

• Locking PLC cabinets.

• Providing exposed outdoor RTUs with protective, lockable casing.

• Securing SCADA servers in locked, climate-controlled areas.

• Restricting access to the control room (and network/server room) with entry system that stores information about who has entered and departed. Consider biometric devices for areas requiring the highest levels of security.

• Hardening control rooms using techniques presented in other sections of this document, including physical improvements to doors, windows, and walls.

• Install third-party software—or upgrade current HMI version—to enable change propagation capability that monitors revisions to programming by date/time and login credentials. This software can also "undeploy" programming changes and revert to a previous version.

• Install safeguards for laptops used for onsite programming of remote PLCs or RTUs against theft or unauthorized use.

Operational Practices

The following operational practices supplement the detailed recommendations above to make the business network and SCADA systems more secure and lessen the consequences of a failure.

• Back up SCADA servers and programming workstations to tape every night. Verify that backup system consistently captures a "snapshot" of designated servers and workstations. Provide offsite storage of selected backups necessary for disaster recovery purposes.

• Routinely back up all SCADA programs for PLCs, distributed control units, RTUs, SCADA servers, and similar programmable devices to provide for rapid recovery in the event of loss of program or need to install new devices. Store programs offsite.

• Install anti-virus software and configure for daily virus pattern updates on all servers and workstations.

• Reset all operating system and HMI passwords away from default settings.

• Set passwords to automatically expire, prompting users to develop new ones on a regular basis.

• Provide an uninterruptible power supply (UPS) for all servers, networking components, and vital workstations. Consider the addition of a backup generator if warranted by system criticality. Provide individual UPSs for any critical SCADA devices not protected by the main UPS system.

• Provide a secondary method to collect data from the remote systems in case of a communications failure. If, for example, a spread-spectrum radio network is the main method of remote SCADA communication, then telephone lines could be used for dial-up access in case of radio failure.

• Configure identical SCADA servers for "fail-over" redundancy.

Cyber Security Training

Training activities also ensure a higher level of cyber security. User acceptance is an important part of adherence to security policies. Training sessions help review security procedures and impart to users the importance of individual responsibility.
The general user population must be trained to understand all security policies and procedures. Specific topics should include the following:

• Do not share passwords with others. A common technique, called social engineering, has intruders posing as network administrators to extract passwords from trusting users.
• Do not write passwords down.

• Do not set up wireless networks or wired connections between networks without authorization.

• Password-protect home machines used to connect to the enterprise.

• Network administrators should analyze log files to pinpoint unauthorized activity accounts.

• Operators should log out of the HMI whenever out of the control room.

6.2 Generation of Tags

Another problem which is faced in IGL, New Delhi is the generation of tags.

6.2.1 What is a tag?

A tag is a logical name for a variable in a device or in local memory(RAM). Tags that receive their data from an external source such as programmable controller or a DDE server are referred to as device tags. Tags that receive their data internally from RS View 32 are referred to as memory tags.

Tags are stored in the tag database and their names are then used in other parts of RS View 32. One can create tags in several ways or combinations of ways.

One can:

- Create tags as needed
- Create many tags at once
- Import tags from an Allen- Bradley PLC or SLC database.

Tag Types:-

RS View uses the following tag types:

Analog tags store a range of values
Digital tags store 0 or 1
String tags store ASCII strings, a series of characters, or whole words. The maximum string length is 82 characters.
System tags stores information generated while the system is running, including alarm information and the system time and date. RSView 32 creates system tags when a project is created and stores the tags in the system folder in the tag database. One cannot edit or write to system tags, but one can use them anywhere one would use any other tag.

6.2.2 Creating tags as needed

One can create tags as needed them while working in other editors. To create a tag, following things can be done:

- In any field requiring a tag or an expression, type a tag name. If the tag doesn't exist in the tag database, one will be prompted to create the tag when he try to save or close. The tag name can be used without creating the tag but be sure to create the tag later or errors will occur at runtime.

- Click the tags or .....(Selection) button, whichever is available, to open the tag browser. Use the Tag browser to select, create, and edit tags.

6.2.3 Creating many tags at once

To create many tags at once, use the Tag Database editor. One can organize tags into groups using folders. Using folders speeds up database creation because you can duplicate a folder and its tags in a single operation. For example, if one has several similar machines that require the same tags, one can create a folder called Machine1 and define its tags. To create the tags for Machine2, duplicate the folder.

CHAPTER 7

"PROPOSED SCHEME FOR IGL, NEW DELHI"

7.1 Introduction

As we know that Indraprastha Gas Limited, New Delhi is in the business of supplying Compressed Natural Gas and Piped Natural Gas.

They are soon going to implement SCADA in their operations.

Based on the above discussed concepts, we can propose the ladder logic and different screens used in SCADA if the analog and digital inputs along with the interlocking is known.

After getting the inputs as mentioned in Table 7.1(from IGL), following things can be done:

- Drawing the line diagram
- Designing the Ladder logic
- Preparing the Main Menu Screen,
- Alarm Screen,
- Trend Screen,
- Prepared Report Screen &
- History Screen etc.

Besides these one can also show the maintenance screen along with some other desired schematics.

PARAMETERS THAT WILL BE MONITORED AND CONTROLLED THROUGH SCADA IN IGL, DELHI.

DATA TO BE CAPTURED BY CNG STATION

S. No.	Parameter	Equipment	Remarks	Type
1	Gas Inlet Pressure	Compressor		AI
2	Gas Inlet Temperature	Compressor		AI
3	Final Discharge Pressure	Compressor		AI
4	Gas Outlet Temperature	Compressor		AI
5	RPM	Engine		AI
6	Compressor Coolant Temperature	Compressor		AI
7	Engine Coolant Temperature	Compressor		AI
8	Compressor Lube Oil Pressure	Compressor		AI
9	Engine Lube Oil Pressure	Compressor		AI
10	Engine Fuel Consumption	Engine		AI
11	Inlet Gas Flow	Compressor		AI
12	Interstage Pressure – 1st Stage Discharge	Compressor		AI
13	Interstage Pressure – 2nd Stage Discharge	Compressor		AI
14	Totalizer Reading	Dispenser		AI
15	Compressor Status (Stop/Start)	Compressor		DI
16	Running hrs/Stop hrs of Compressor	Compressor		AI
17	Cascade Pressure – High Bank	Cascade	Presently only PG provided. Is it essential to provide PT ?	AI
18	Cascade Pressure – Medium Bank	Cascade		AI
19	Cascade Pressure – Low Bank	Cascade		AI
20	Lube Oil Level	Compressor		AI

21	Lube Oil Level	Engine		AI
22	Coolant Level	Compressor		AI
23	Coolant Level	Engine		AI
24	LCV Loading/Filling Point Flow Rate	General	Provision should be kept if FT is provided	AI

Table 7.1 Parameters used for monitoring through SCADA
Source: Indraprashta Gas Limited, New Delhi

7.2 CNG SUPPLY MECHANISM

The CNG supply mechanism of IGL is shown below:

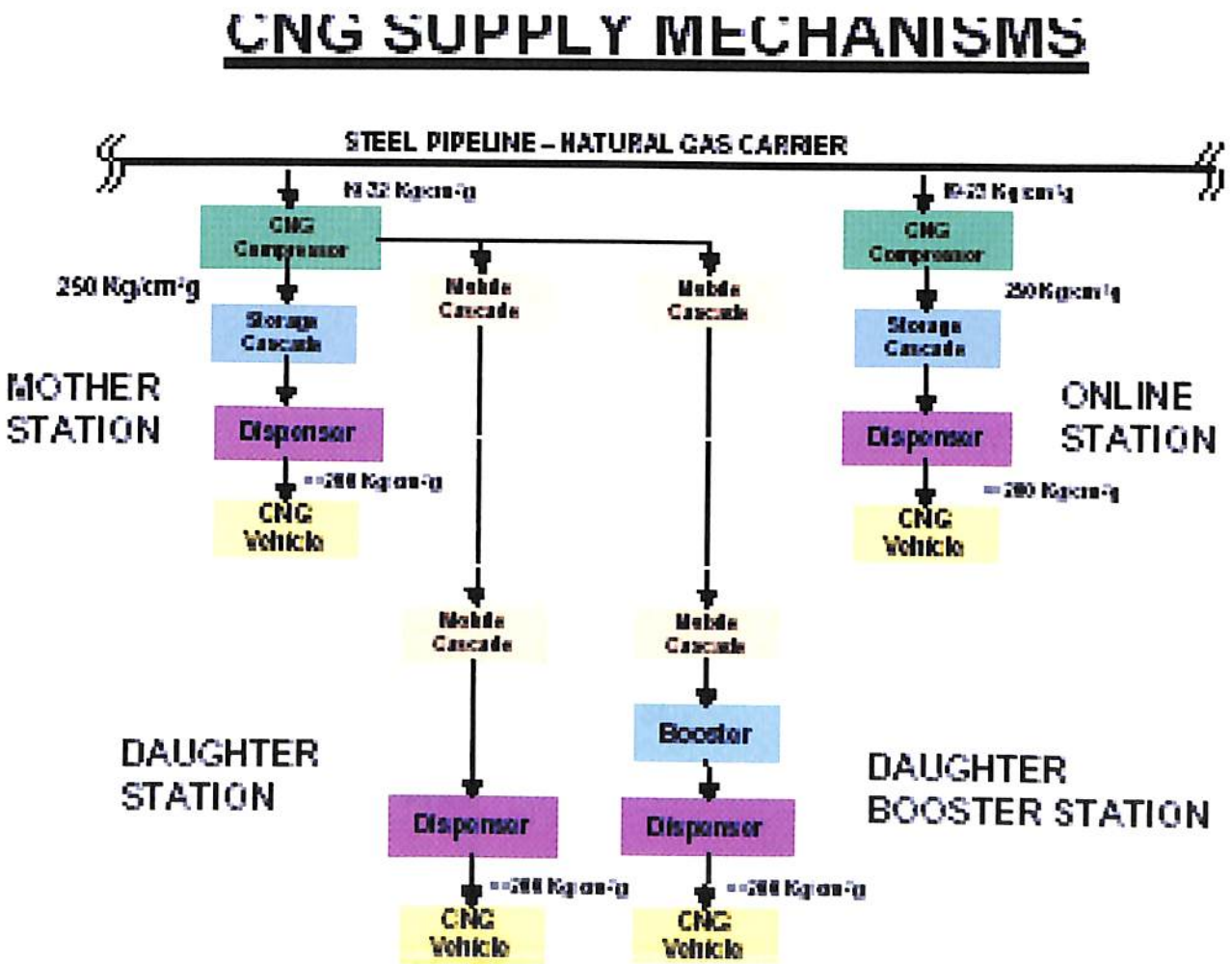


Figure 7.1 CNG Supply Mechanism
Source: Indraprashta Gas Limited, New Delhi

From the Figure 7.1, the line diagram of CNG supply mechanism can be drawn as under:

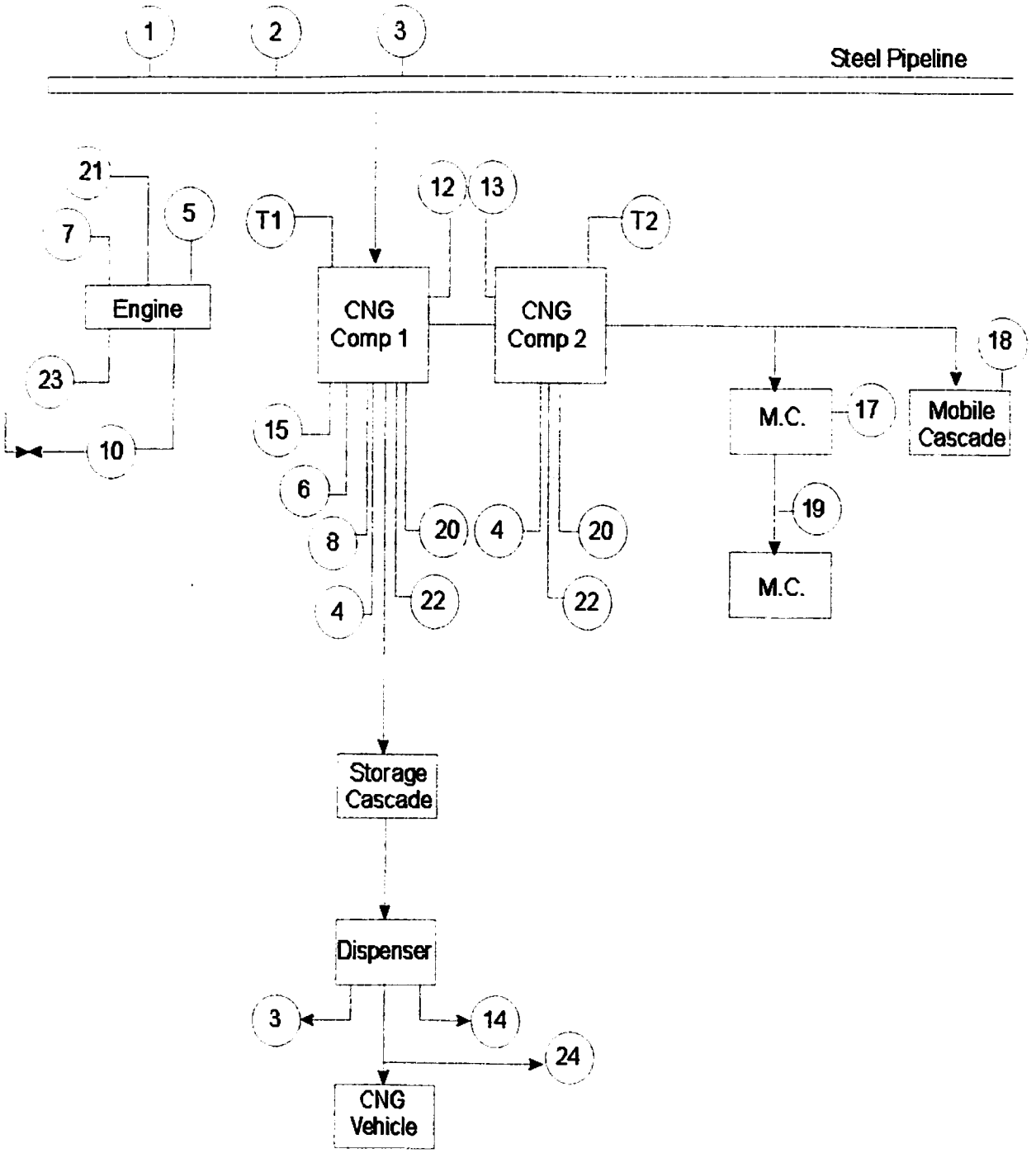
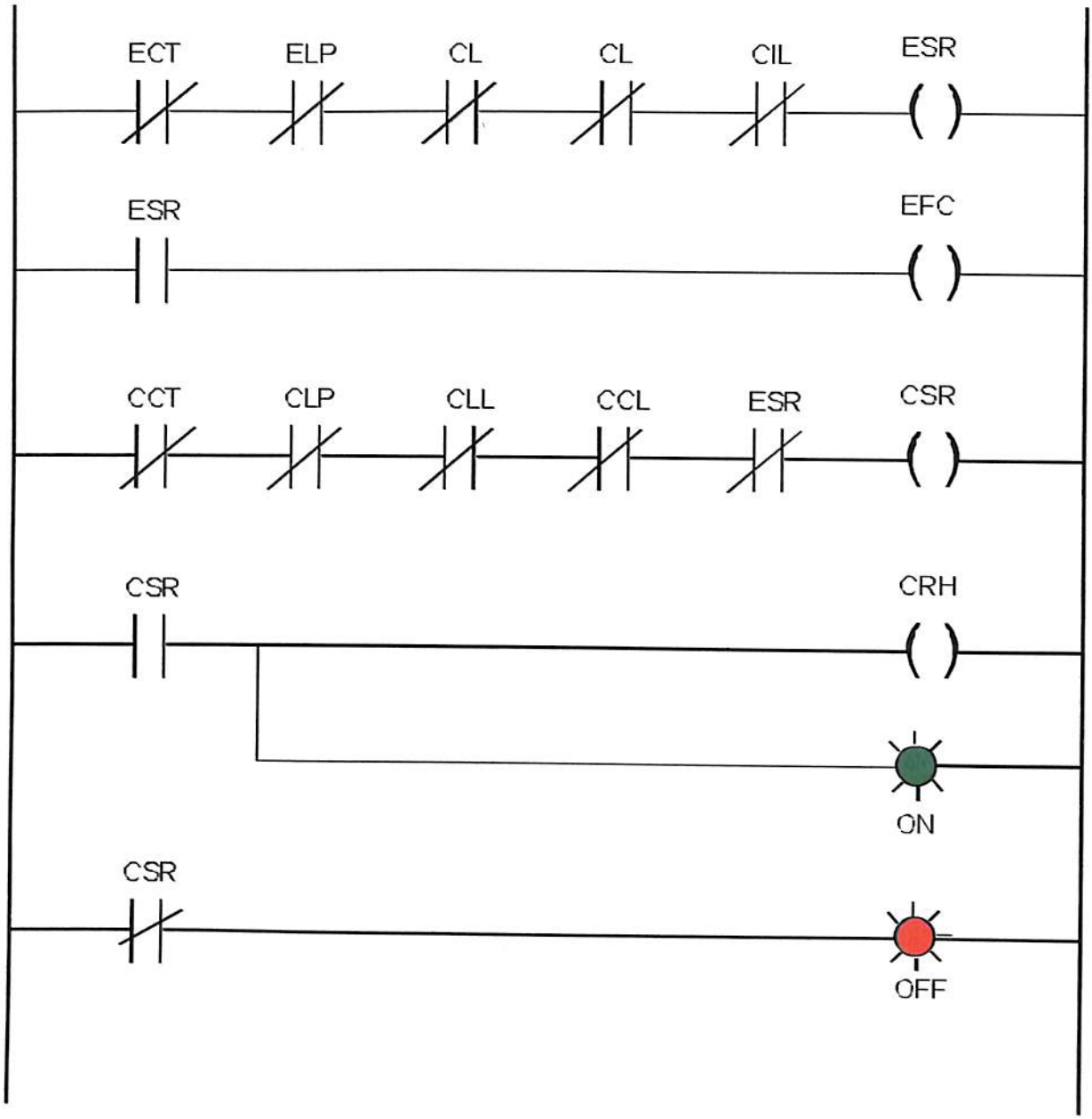


Figure 7.2 : Line Diagram of CNG Supply Mechanism

Note: Notations 1 to 24 are as per Table 7.1

The ladder logic can be drawn as under:



Where

ECT = Engine Coolant Temperature
ELP = Engine Lube Oil Pressure
CL = Coolant Level
LL = Lube Oil Level
ESR = Engine Start Relay
EFC = Engine Fuel Consumption
CCT = Compressor Coolant Temperature
CLP = Compressor Lube Oil Pressure
CLL = Compressor Lube Oil Level
CCL = Compressor Coolant Level
CSR = Compressor Start Relay
CRH = Compressor Running Hour.

(Fig: 7.3)

The Main Menu screen is shown as below:

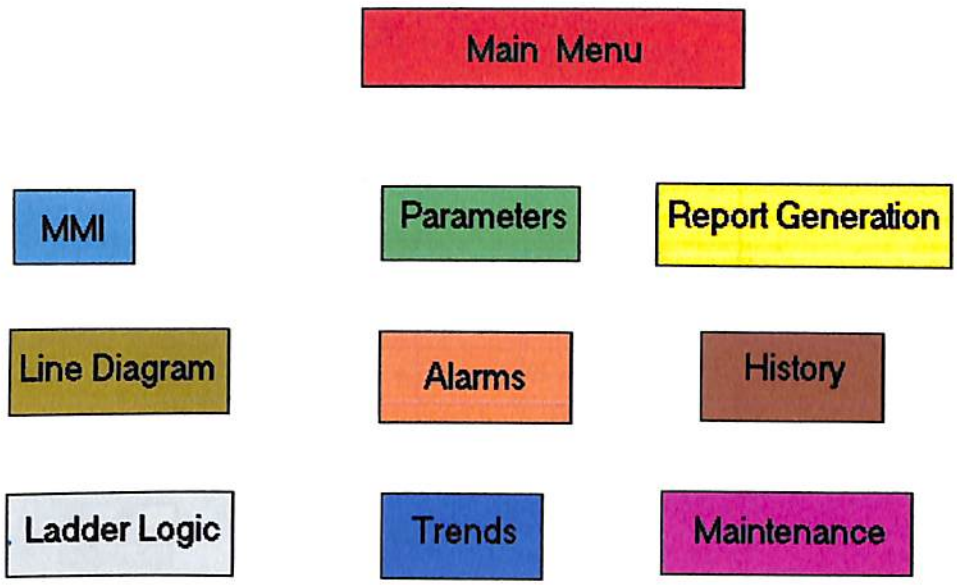


Figure 7.4 Main Menu Screen

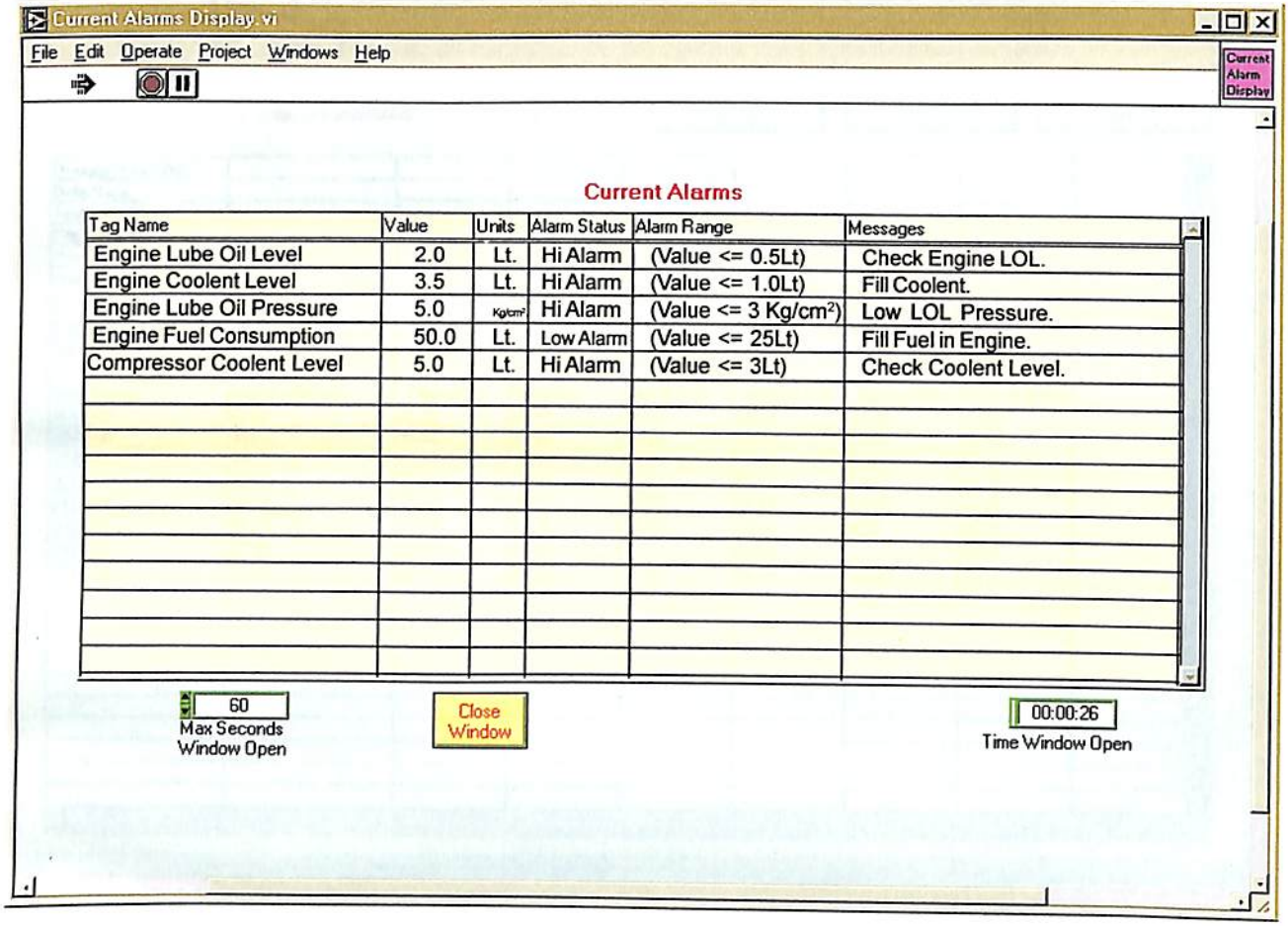


Figure 7.5: Alarm Screen

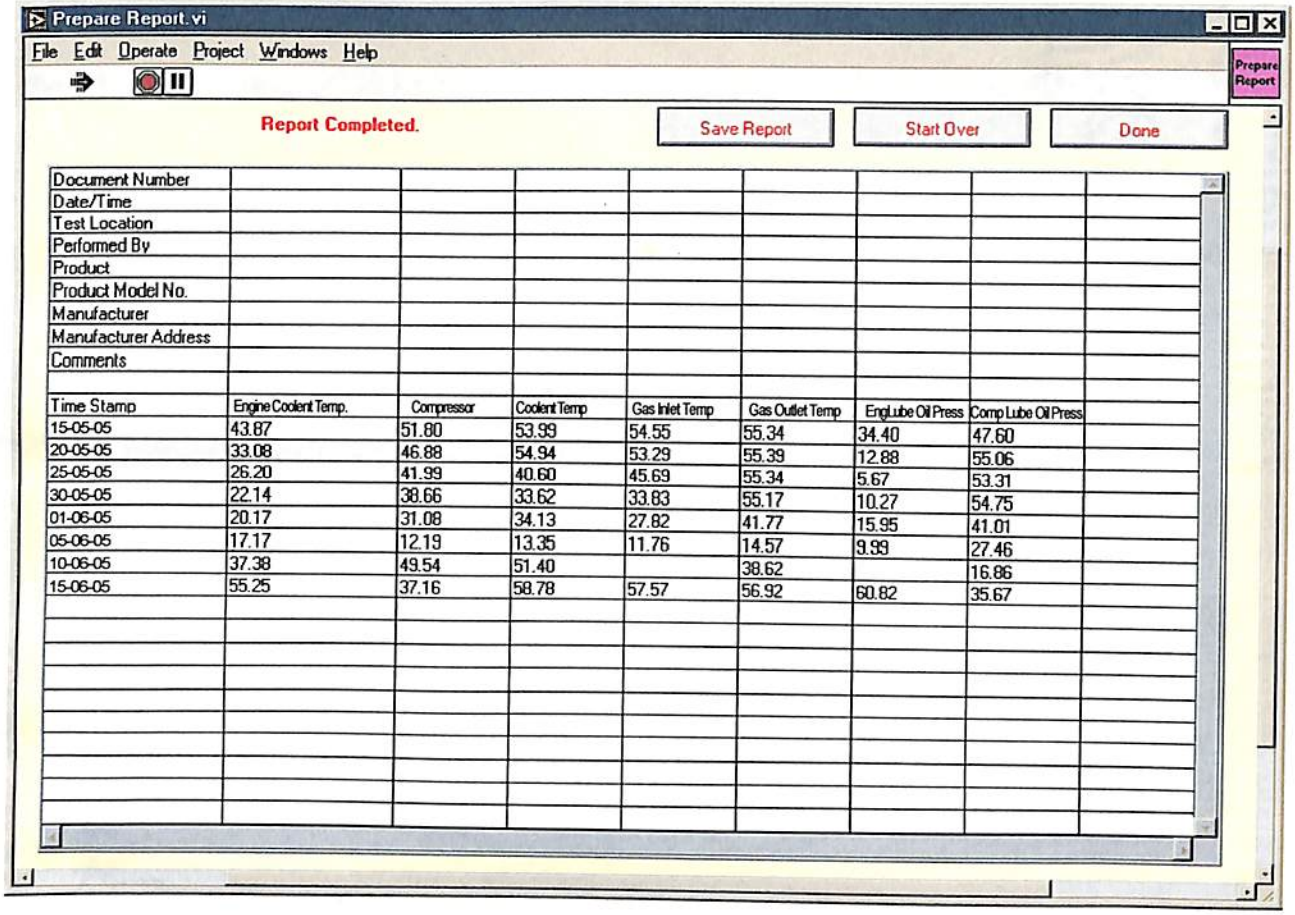


Figure 7.6: Prepare Report Screen

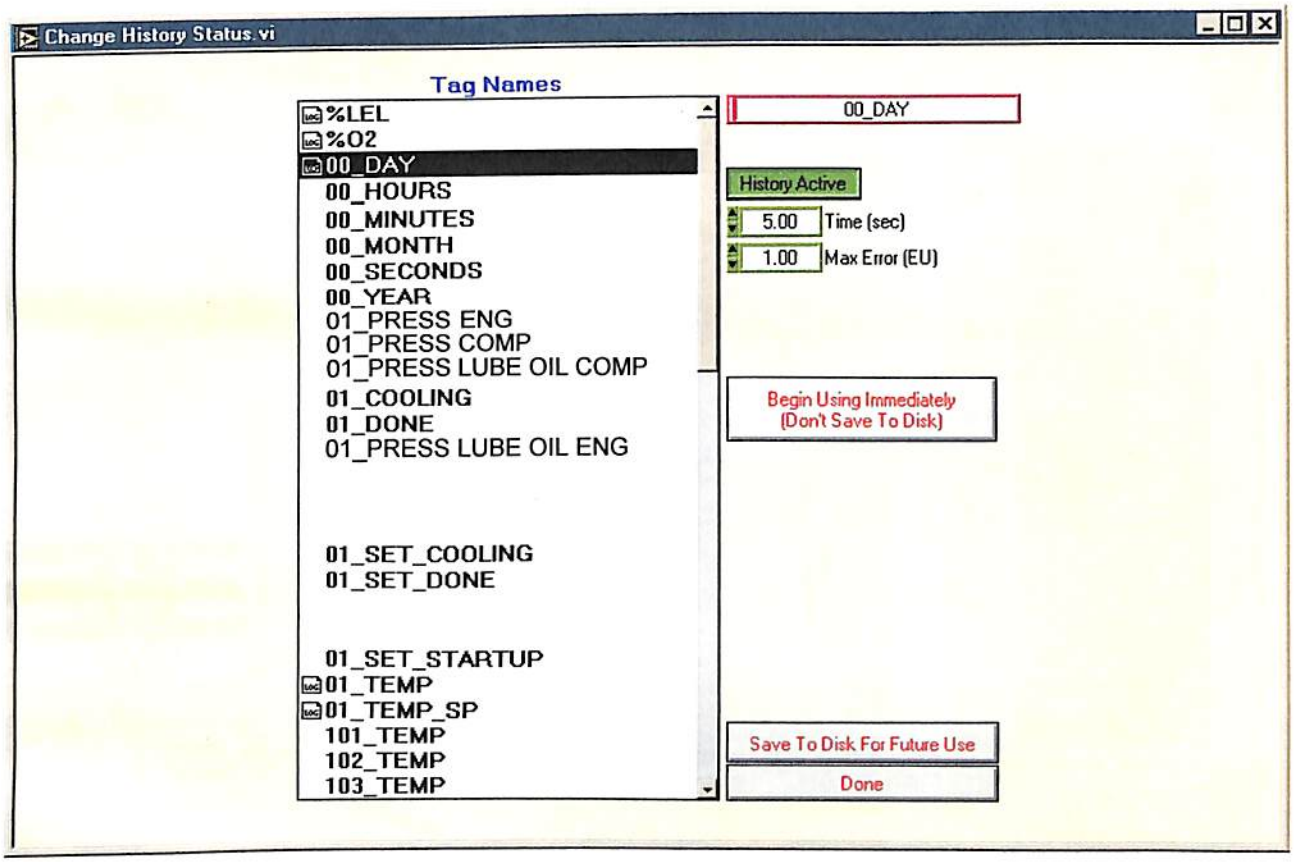


Figure 7.7: History Screen

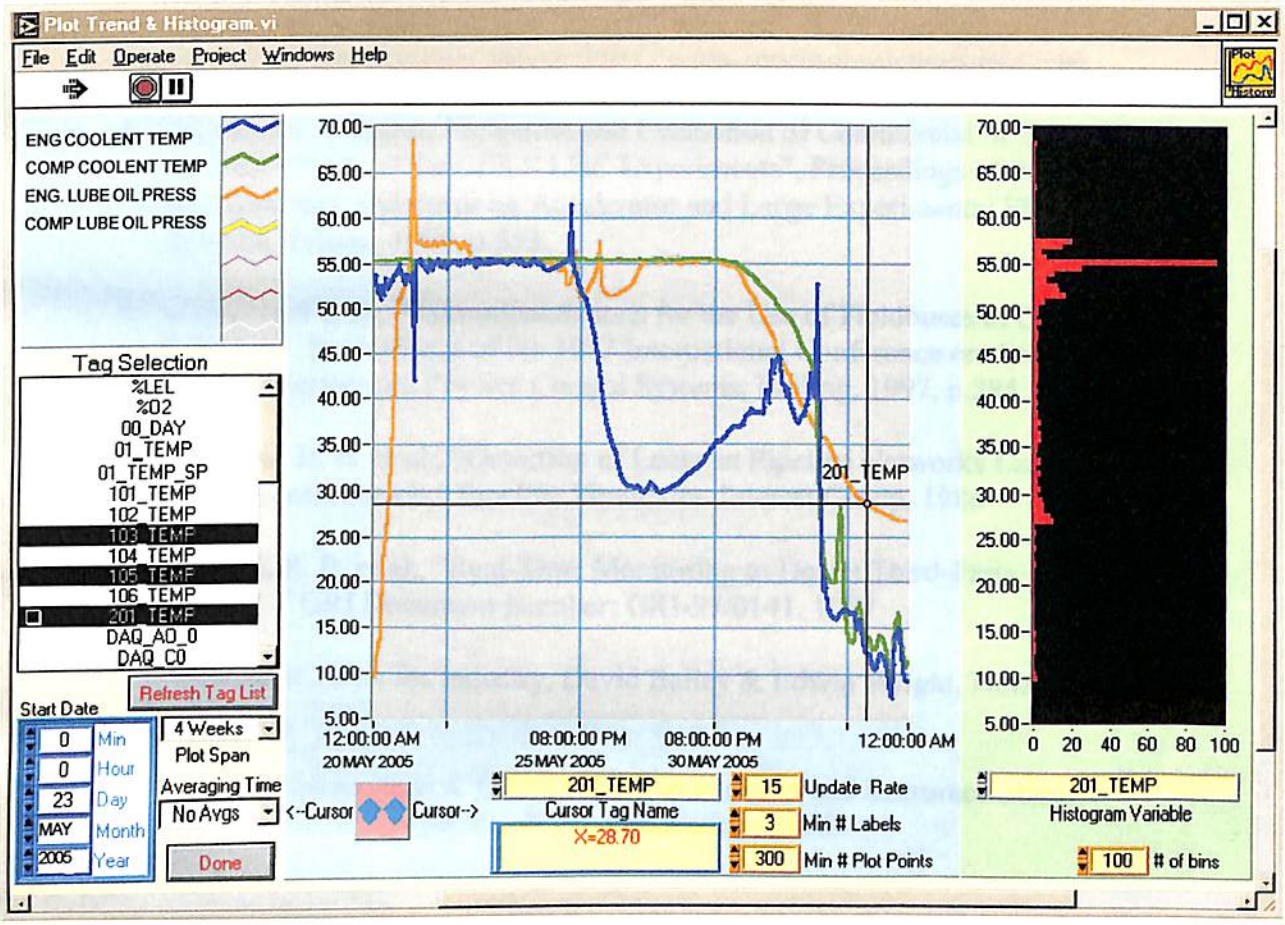


Figure 7.8: Plot Trend & Histrogram Screen

REFERENCES

1. Paper presented at the 2nd International Pipe Line Week Conference and Exhibition, organized by Gulf Publishing Co. and *Pipe Line & Gas Industry* magazine, held in October 1998, in Houston, Texas.

2. Pipeline & Gas Journal / March 2003 / www.pipelineandgasjournal.com

3. A.Daneels, W.Salter, "Selection and Evaluation of Commercial SCADA Systems for the Controls of the CERN LHC Experiments", Proceedings of the 1999 International Conference on Accelerator and Large Experimental Physics Control Systems, Trieste, 1999, p.353.

4. G.Baribaud et al., "Recommendations for the Use of Fieldbuses at CERN in the LHC Era", Proceedings of the 1997 International Conference on Accelerator and Large Experimental Physics Control Systems, Beijing, 1997, p.285.

5. Rachford, H. H. et al., "Detection of Leaks in Pipeline Networks Using Standard SCADA Information," Pipeline Simulation Interest Group, 1986

6. Francini, R. B. et al., "Real-Time Monitoring to Detect Third-Party Damage: Phase II.," GRI Document Number: GRI-97/0141, 1997

7. Practical SCADA for Industry, David Bailey & Edwin Wright, Newness publishers, 2003.

8. A course in Electrical & Electronic Measurements and Instrumentation, A.K.Sawhney, Dhanpat Rai & Co. publications,2005.

9. www.google.co.in

10. www.spe.org

LIST OF FIGURES

LIST OF TABLES

APPENDIX A:INTERFACE STANDARDS

Recommended Standards (RS-) for Data Communications:

Transmitter		RS-232	RS-423	RS-422	RS-485
Mode of operation		Unbalanced	Unbalanced	Differential	Differential
Max No. of Drivers & Receivers on line		1 Driver 1 Receiver	1 Driver 10 Receivers	1 Driver 10 Receivers	32 Drivers 32 Receivers
Maximum cable length		15 m	1,200 m	1,200 m	1,200 m
Maximum data rate		20 kbps	100 kbps	10 Mbps	10 Mbps
Maximum Common Mode Voltage		±25 V	±6 V	+6 V to -0.25 V	+12 V to -7 V
Driver Output Signal		±5.0 V min ±25 V max	±3.6 V min ±6.0 V max	±2.0 V min ±6.0 V max	±1.5 V min ±6.0 V max
Driver Load		> 3 kohm	>450 ohm	100 ohm	60 ohm
Driver Output Resistn	Power On	n/a	n/a	n/a	≤ 100 microA -7 Vcm ≤ 12V
High-Z state	Power Off	300 ohm	≤100 microA @ ±6V	≤100 microA -25V≤ Vcm ≤ 6V	≤100 microA -7 Vcm ≤ 12V
Receiver input resistance		3 kohm to 7 kohm	>4 kohm	> 4 kohm	> 12 kohm
Receiver sensitivity		±3.0V	±200mV	±200mV -7≤ Vcm ≤ 7V	±300mV -12V≤ Vcm ≤ 12V
Dataforth's Line Drivers and Converters		DCP35 LDM30 LDM35 (RML35) LDM70 (RML70) LDM80 LDM85	LDM85	LDM422 * LDM85	DCP485 * LDM485 * (RML485 *) LDM2485 * SCM9B-A1000/A2000 * * Converters

Table A.1 Interface Standards