UNIT - V

SCADA

- SCADA stands for "**Supervisory Control and Data Acquisition**".
- SCADA is a type of process control system architecture that uses computers, networked data communications and graphical Human Machine Interfaces (HMIs) to enable a high-level process supervisory management and control.

HISTORY

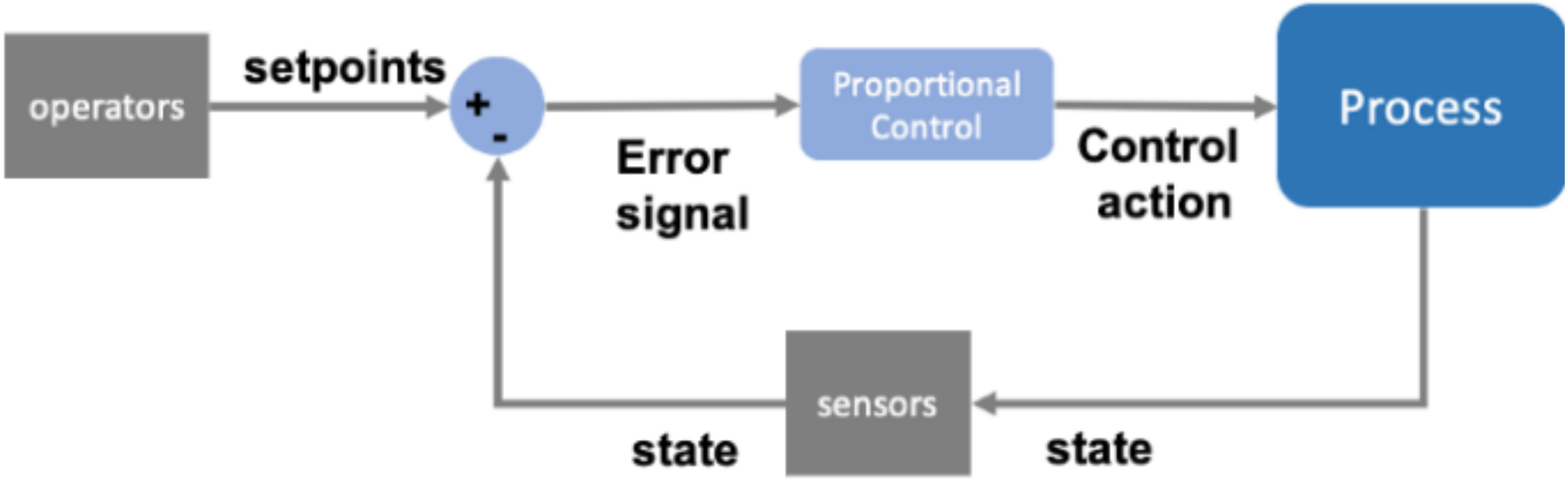
- In the early 1950s, **computers** were first developed
- In the 1960s, **telemetry** was established for monitoring, which allowed for automated communications to transmit measurements and other data from remotes sites to monitoring equipment
- The term “SCADA” was coined in the early 1970s, Also rise of microprocessors and PLCs during that decade increased.
- In the 80s and 90s, SCADA continued to evolve with Local Area Networking (LAN) technology, and PC-based HMI software. Unfortunately, these systems were incapable of communicating with systems from other vendors. These systems were called distributed SCADA systems.
- In the 1990s and early 2000s, building upon the distributed system model, SCADA adopted an incremental change.

Functions of SCADA Systems

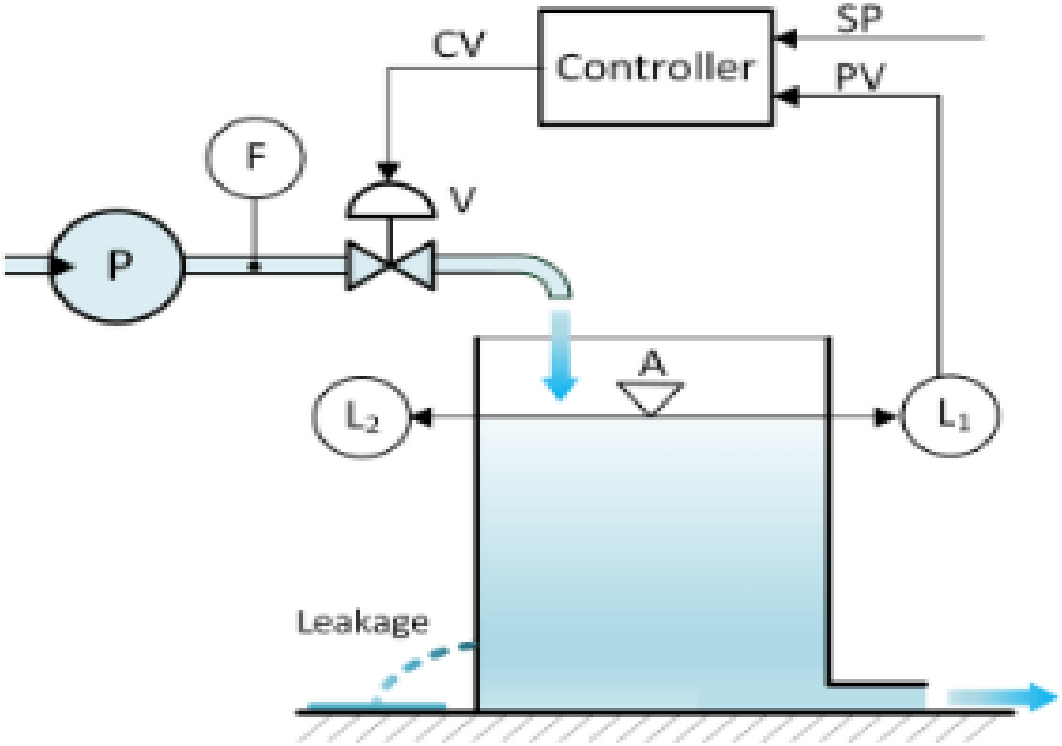
SCADA system is a collection of hardware and software components that allows the manufacturing units to perform specific functions.

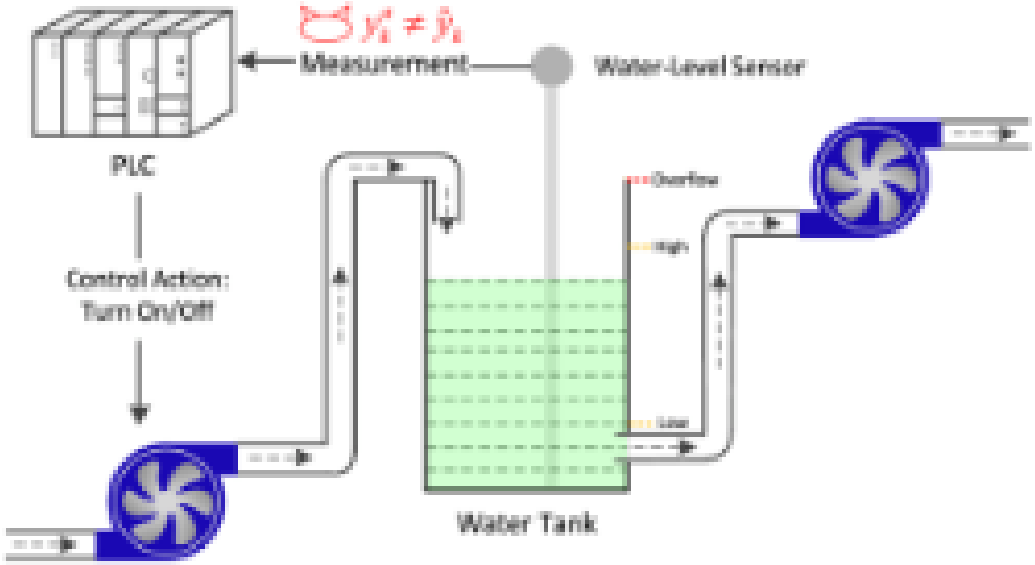
- To **monitor** and **gather data** in real-time
- To **interact with field devices** and **control stations** via Human Machine Interface (HMI)
- To **record systems events** into a log file
- To **control manufacturing process** virtually
- Information Storage and **Reports**

Closed Loop

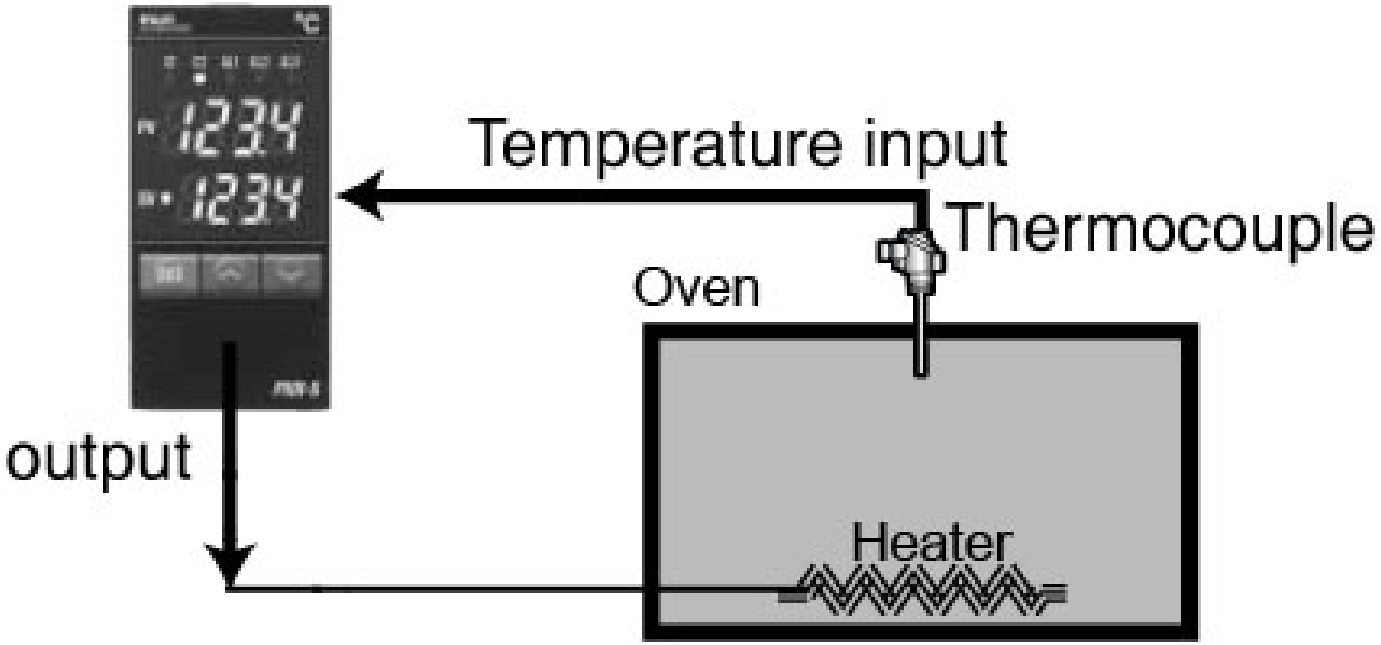

operators
setpoints
+
-
Error
signal
Proportional
Control
Control
action
Process
sensors
state
state

Level Control

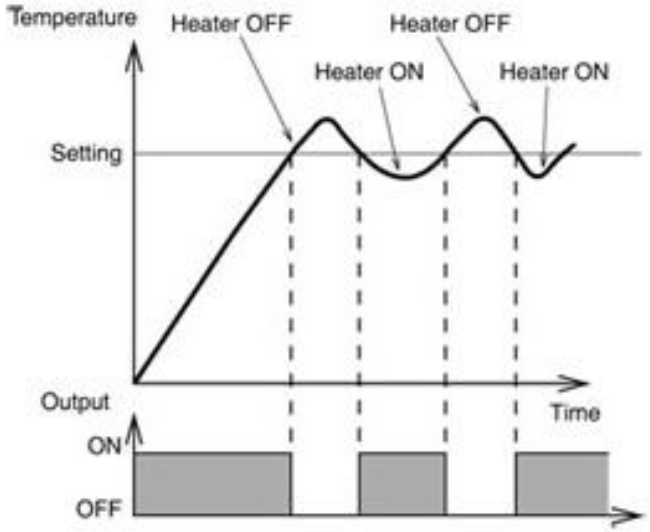


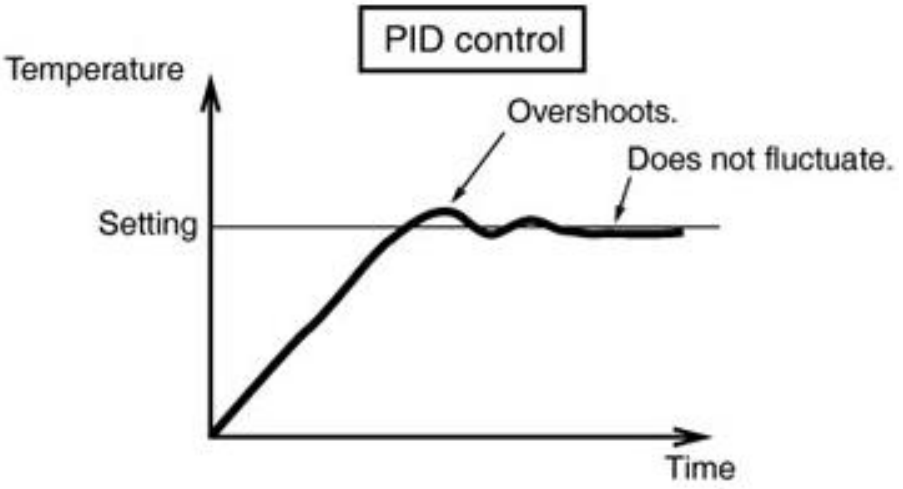


Temperature Control

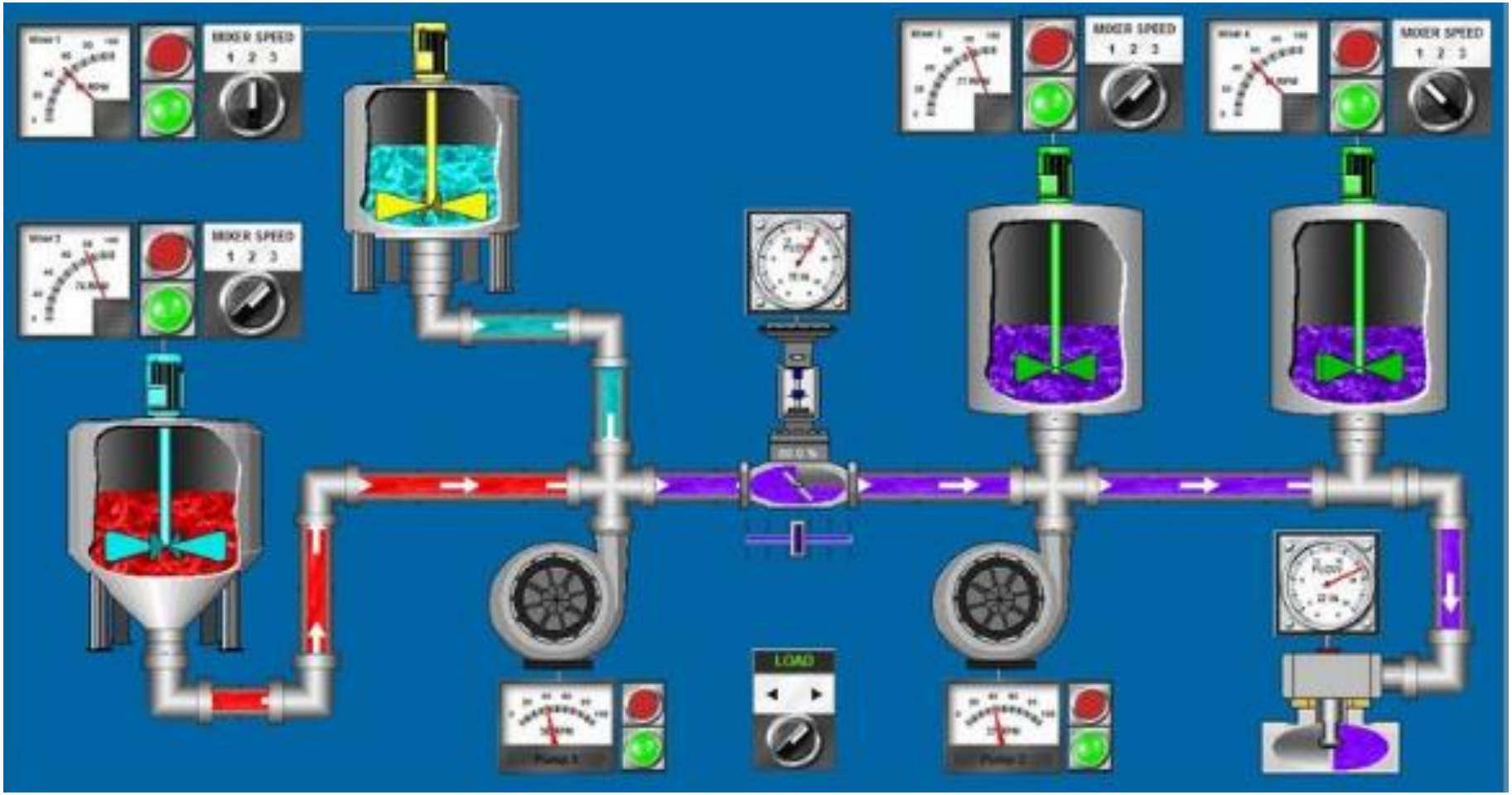


ON/OFF Control





SCADA



Application

Groups of small hydroelectric generating stations that are turned on and off in response to customer demand are usually located in remote locations, they can be controlled by opening and closing valves to the turbine, they must be monitored continuously, and they need to respond relatively quickly to demands on the electric power grid.

Oil or gas production facilities—including wells, gathering systems, fluid measurement equipment, and pumps—are usually spread over large areas, require relatively simple controls such as turning motors on and off, need to gather meter information regularly, and must respond quickly to conditions in the rest of the field.

Application

Pipelines for gas, oil, chemicals, or water have elements that are located at varying distances from a central control point, can be controlled by opening and closing valves or starting and stopping pumps, and must be capable of responding quickly to market conditions and to leaks of dangerous or environmentally sensitive materials.

Electric transmission systems may cover thousands of square kilometers, can be controlled by opening and closing switches, and must respond almost immediately to load changes on the lines.

Irrigation systems often cover hundreds of square miles, can be controlled by opening and closing simple valves, and require the gathering of meter values for the water supplied to consumers.

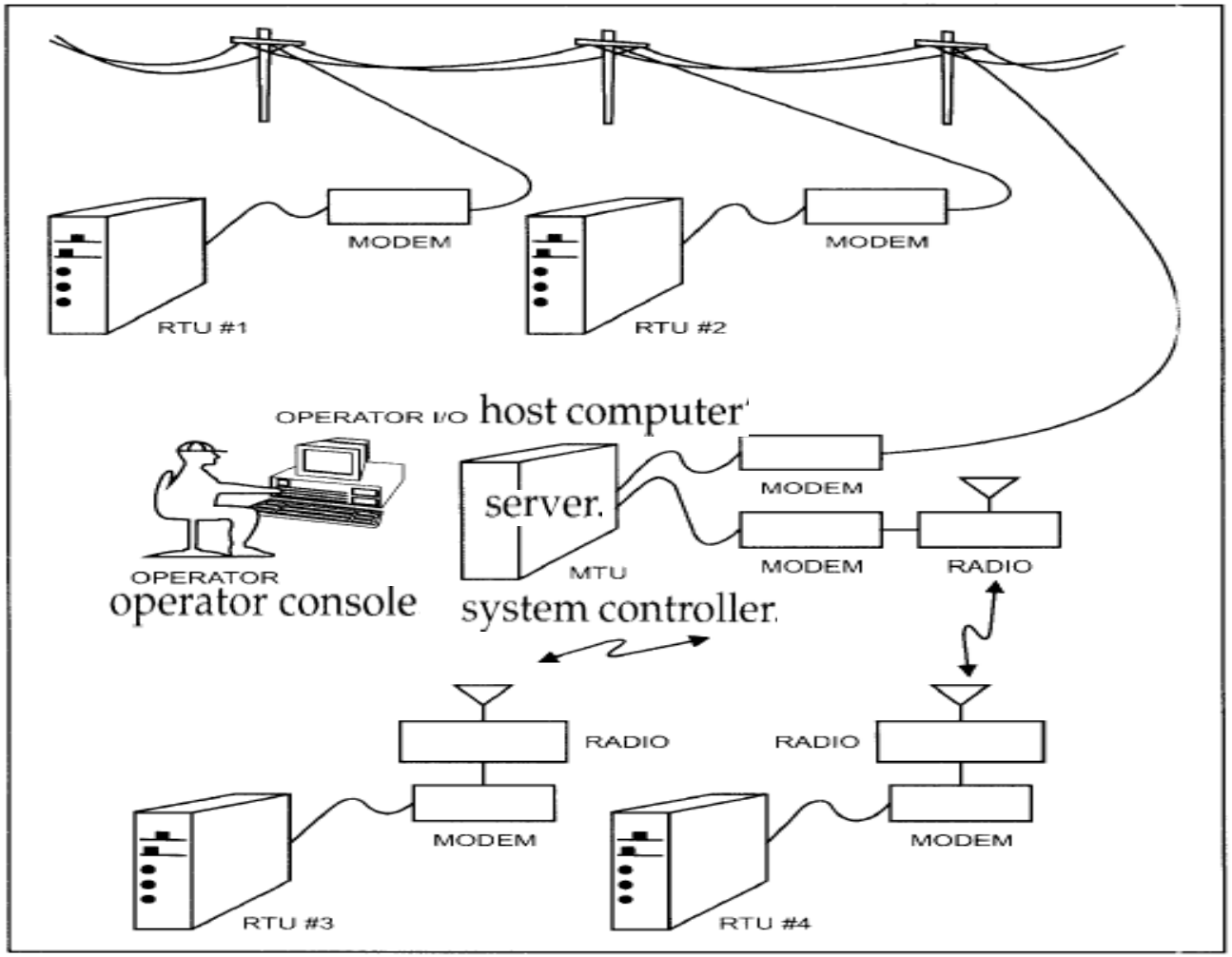
SCADA system Adv.

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

Components of a SCADA system

- Master Terminal Unit (MTU)
- Remote Terminal Unit (RTU)
- Communication Network



Major Components of a SCADA System

SCADA system

In SCADA system there are essentially five levels or hierarchies:

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

Remote Terminal Unit (RTU)

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**.

Specific **protocols and error detection** philosophies are used for efficient and **optimum transfer of data**

The **master station** gather data from the various RTUs and generally provide an operator interface for **display of information and control** of the remote sites

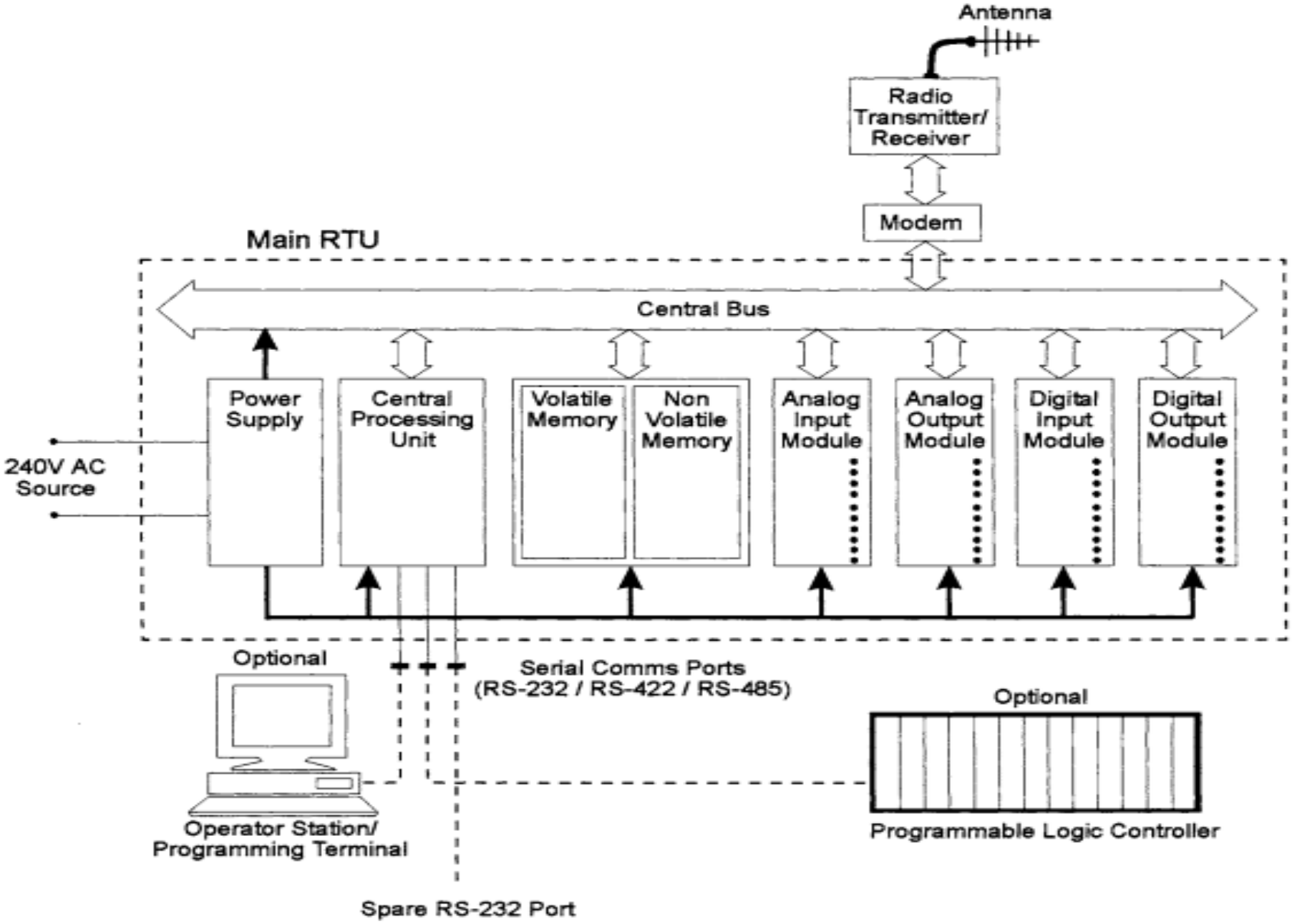
Master Terminal Unit (MTU)

- MTU is the **core** of the SCADA system.
- It comprises a computer, PLC and a network server that helps MTU to communicate with the RTUs.
- MTU begins communication, collects and saves data, helps to interface with operators and to communicate data to other systems.

Remote Terminal Unit (RTU)

- Remote Terminal Unit (RTU) is **connected** with **sensors and actuators**.
- RTU is used to **collect information** from these sensors and further sends the data to MTU.
- RTUs have the **storage** capacity facility. So, it stores the data and transmits the data when MTU sends the corresponding command.
- Recently developed units are employed with systems, that utilize **PLCs as RTUs**. This helps for direct transfer and control of data without any signal from MTU.
- RTUs sometimes referred to as a remote telemetry unit

RTU hardware module



Control Processor (or CPU)

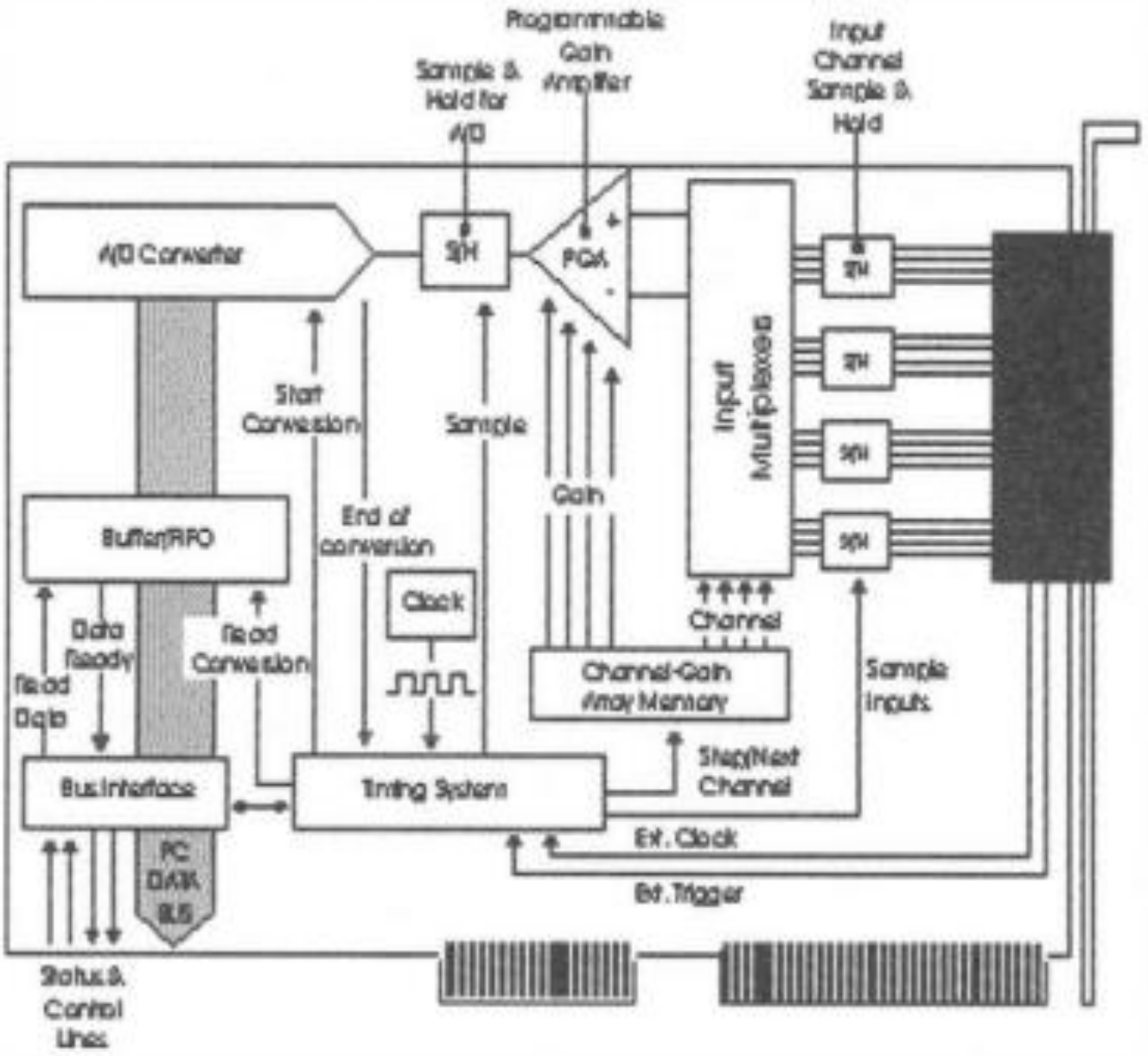
- This is generally microprocessor based (16 or 32 bit)
- **RAM** is **volatile memory** that temporarily stores the files you are working on.
- **ROM** is non-**volatile memory** that permanently stores instructions for your computer.
- **Diagnostic LEDs** provided on the control unit ease **troubleshooting** and **diagnosis** of problems (such as CPU failure/failure of I/O module etc).
- The **real-time clock** is useful for accurate time stamping of events.
- A **watchdog timer** is also required to provide a check that the RTU program is regularly executing.

Analog input modules

There are five main components making up an Analog input module. They are

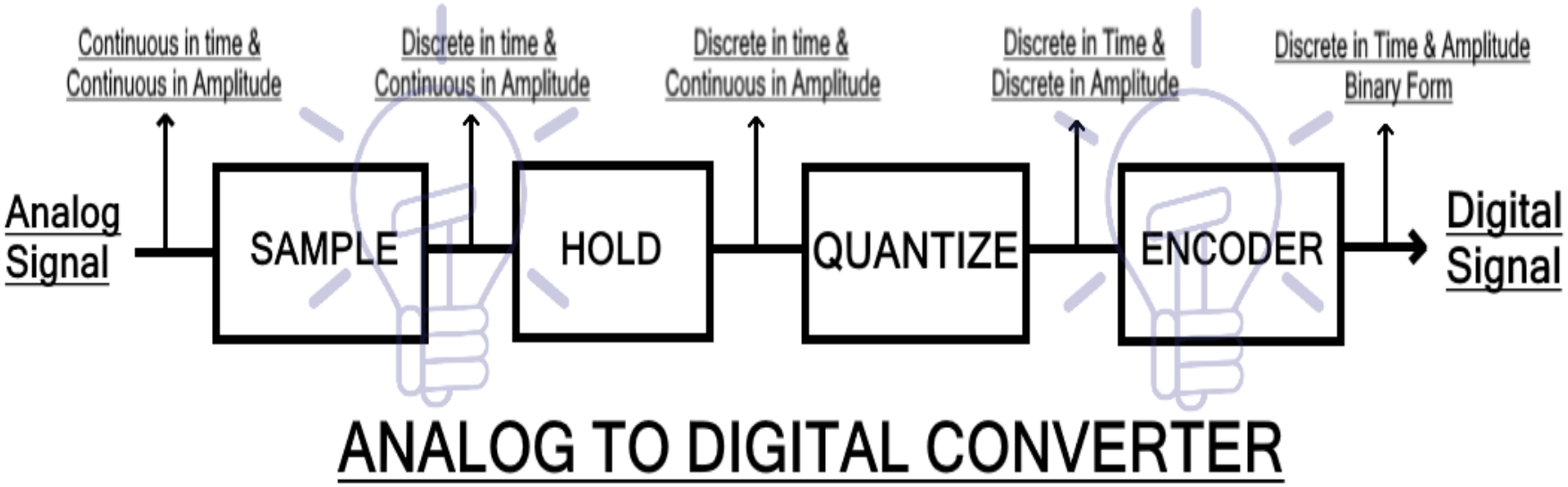
- The input multiplexer,
- The input signal amplifier,
- The sample and hold circuit,
- The A/D converter and
- The bus interface and board timing system.

Typical analog input module



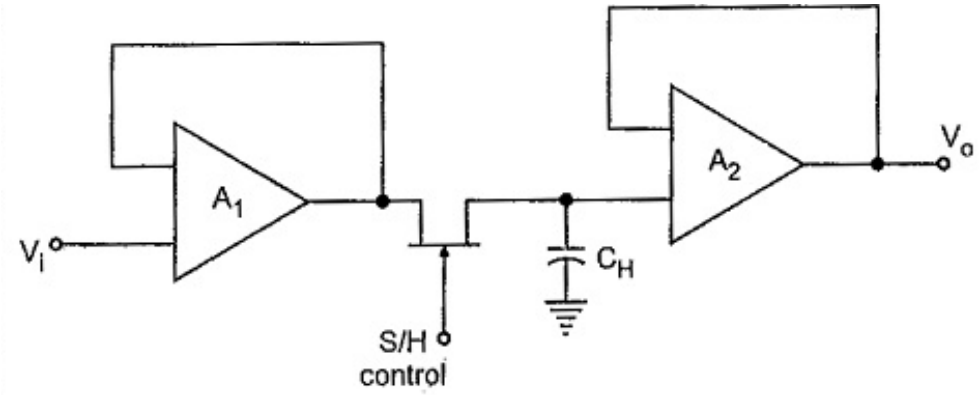
ADC

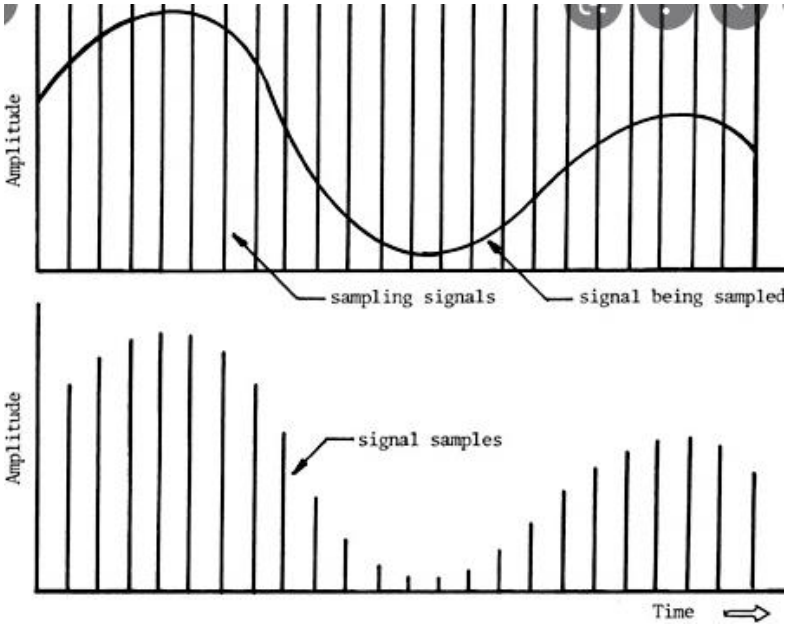

Analog
Input
(Analog
Signal)
ADC
Analog To Digital
Converter
0
1
1
0
Binary
Output
(Digital
Signal)
ctricaltechnology.org


Continuous in time &
Continuous in Amplitude
Discrete in time &
Continuous in Amplitude
Discrete in time &
Continuous in Amplitude
Discrete in Time &
Discrete in Amplitude
Discrete in Time & Amplitude
Binary Form
Analog
Signal
SAMPLE
HOLD
QUANTIZE
ENCODER
Digital
Signal
ANALOG TO DIGITAL CONVERTER

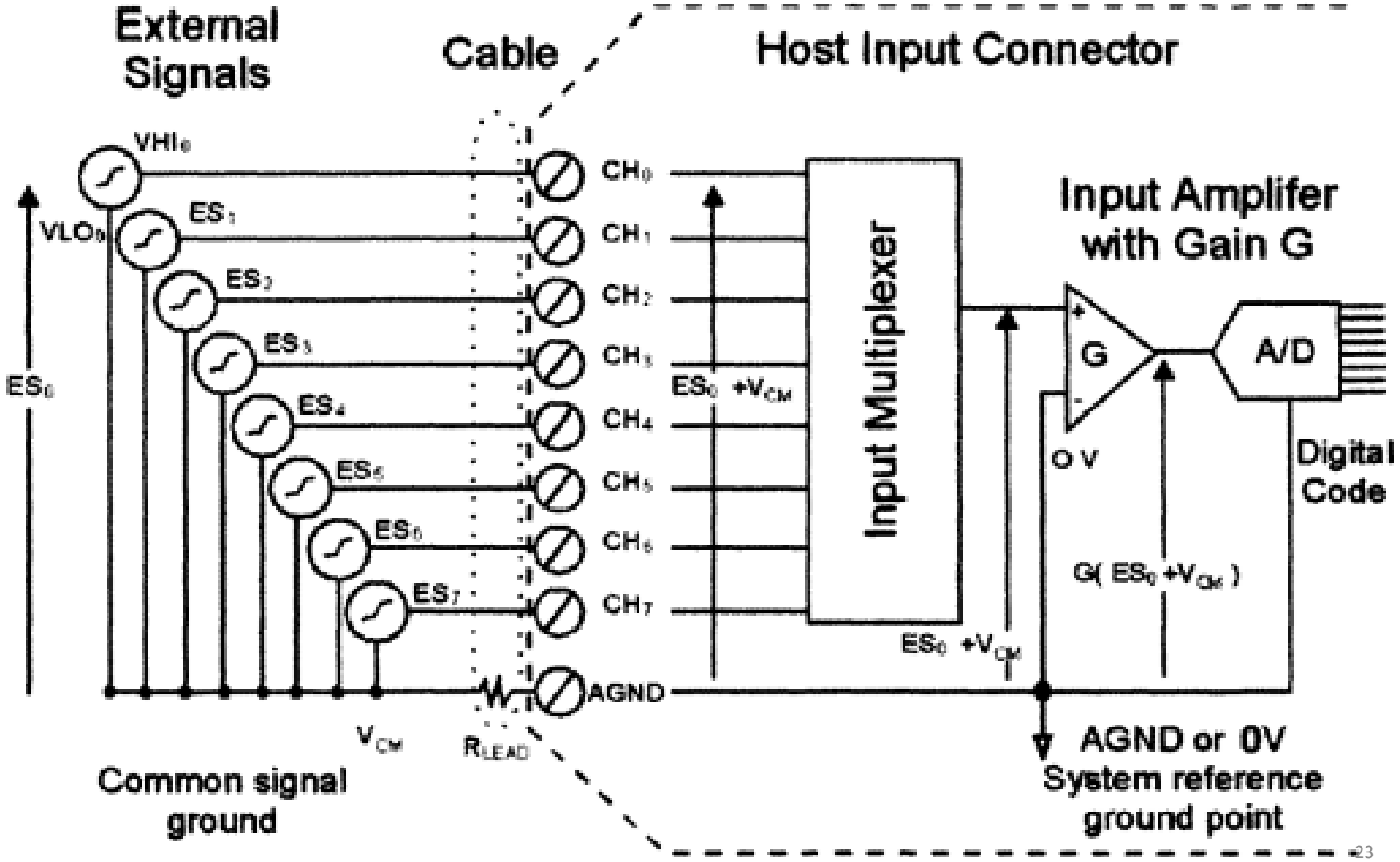
Sample & Hold

Most A/D converters require a fixed time during which the input signal remains constant (the aperture time) in order to perform an A/D conversion.





Eight single-ended inputs



Typical analog input modules

These have various numbers of inputs. Typically there are:

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

Analog output module

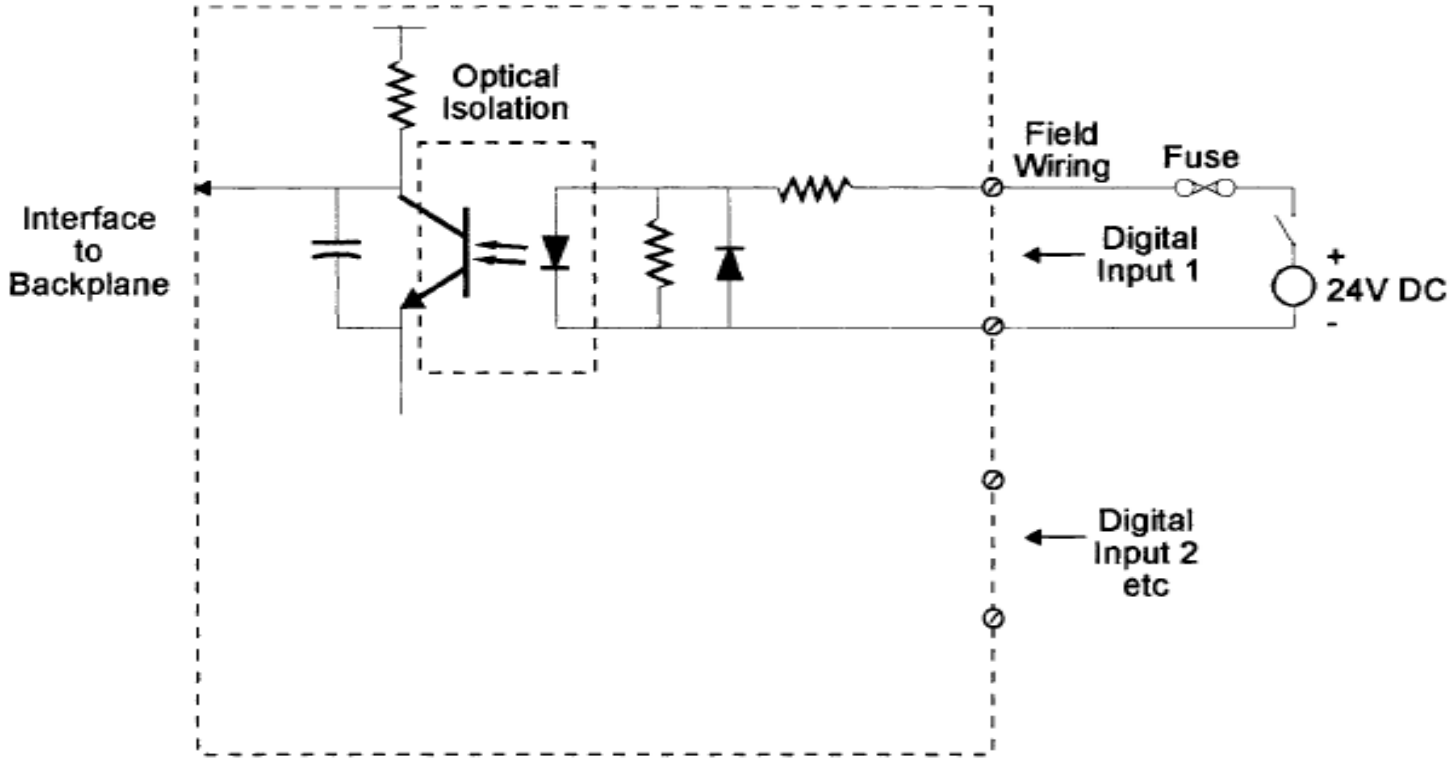
Typically the analog output module has the following features:

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

Digital input module

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 110/240 VAC and 12/24/48 VDC
- Optical isolation provided for each digital input



Digital output module

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

- Triac switching
- Relay switching
- TTL voltage outputs

Typical digital output modules consists of

- 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 for each output

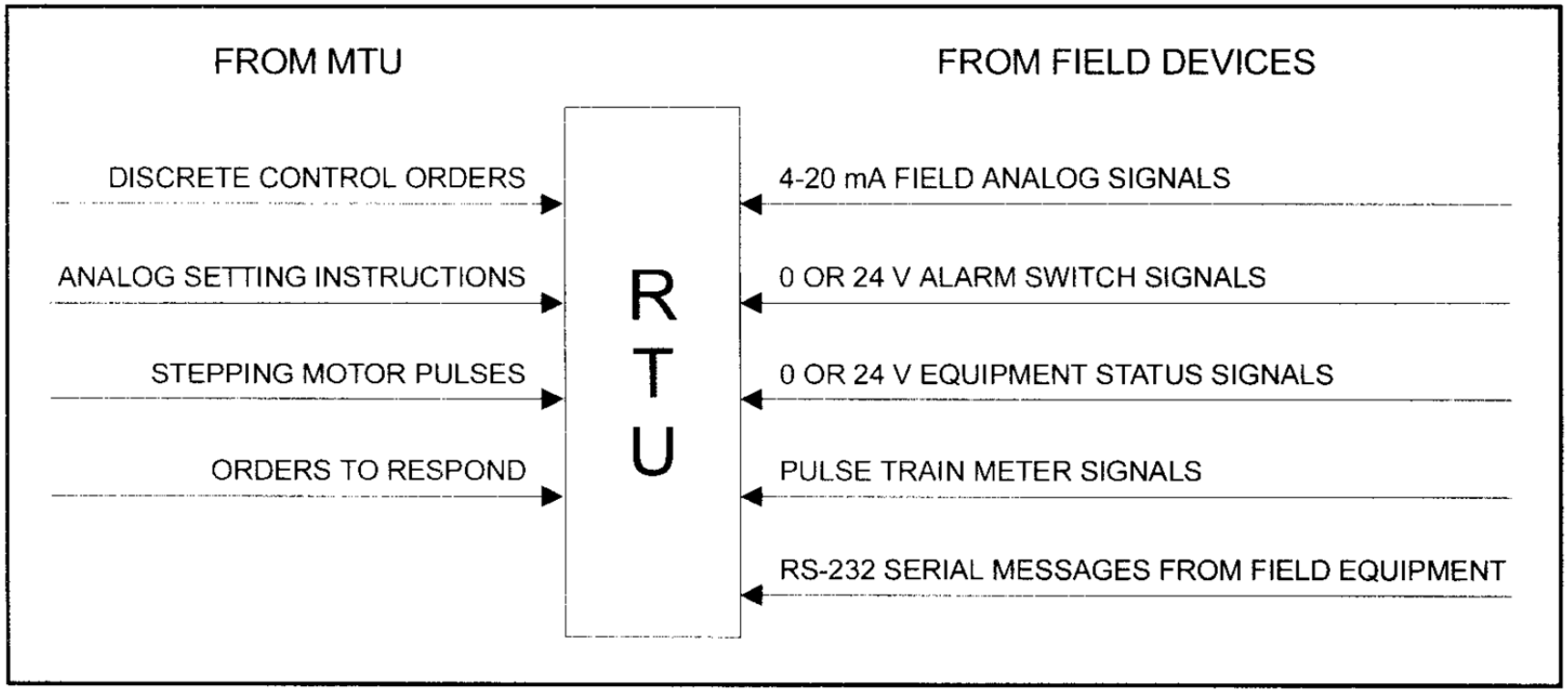
Amplifier

low-level voltages need to be digitized, they must be amplified to match the input range of the A/D converter.

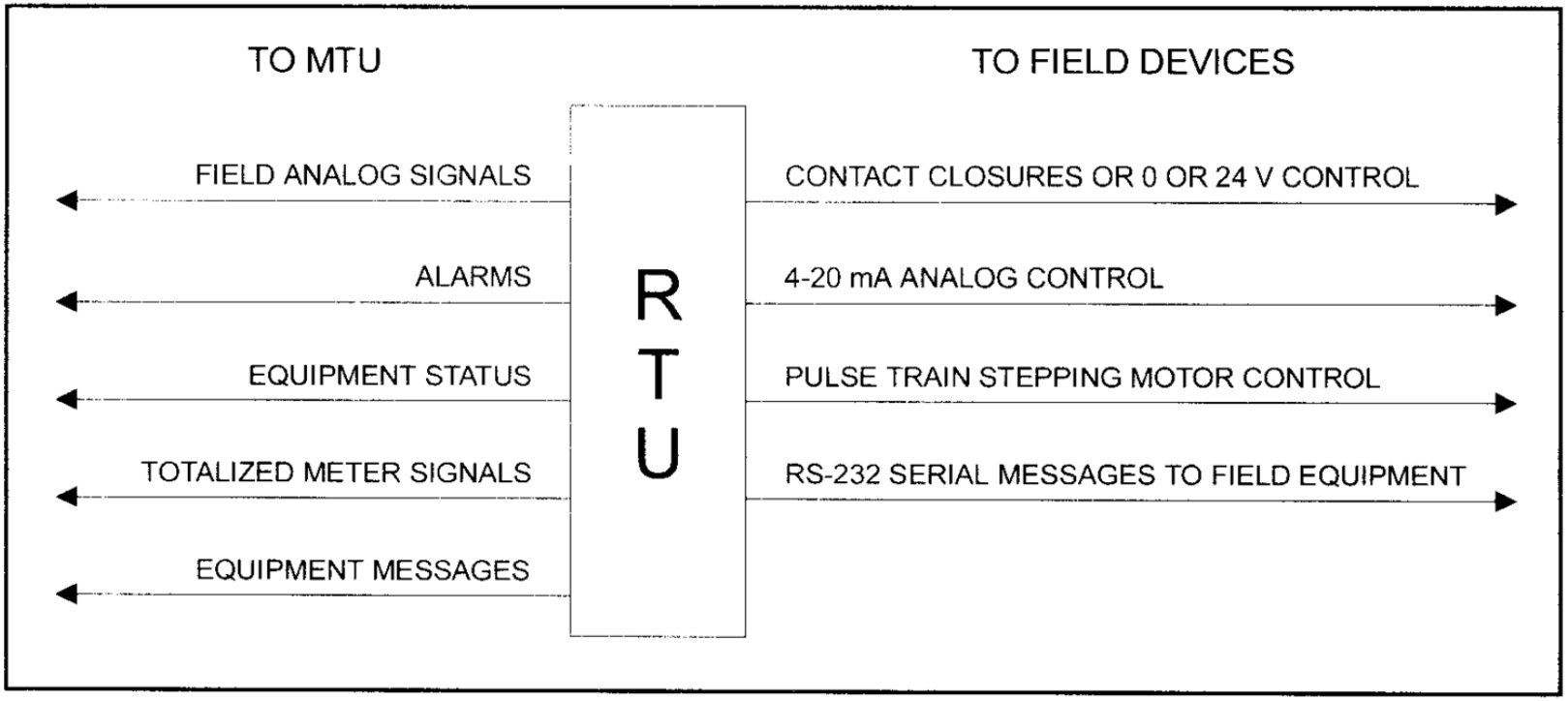
If a low-level signal is fed directly into a board without amplification, a loss of precision will be the result.

common mode voltages do produce error outputs in real-world amplifiers.

The Signals That Come into the RTU



The Signals That Leave the RTU



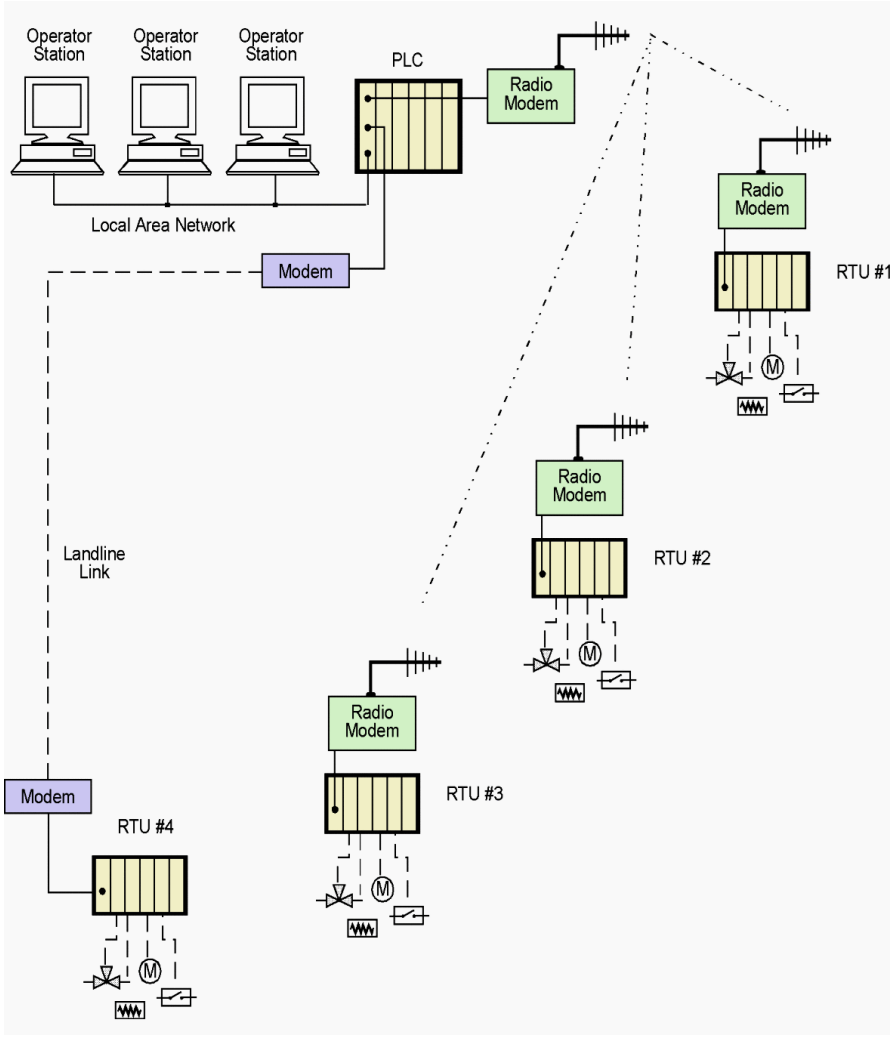
Communication Network

- It is defined as a link between RTU in the field to MTU in the central location.
- The bidirectional wired or wireless communication channel is used for networking purposes.
- Various other communication mediums like fiber optic cables, twisted pair cables, etc. are also used.

SCADA communication

Communications is the movement of data or intelligence from one location to another. For communications to happen, several things must be in place. First, a communications path must exist; some medium must be selected over which the data will travel. Second, equipment must exist at the sending end of the communications path to condition the data and to put it into a form that can be sent over the communications medium. Third, equipment must exist at the receiving end of the path to extract the message from the medium and understand its meaning.

SCADA system



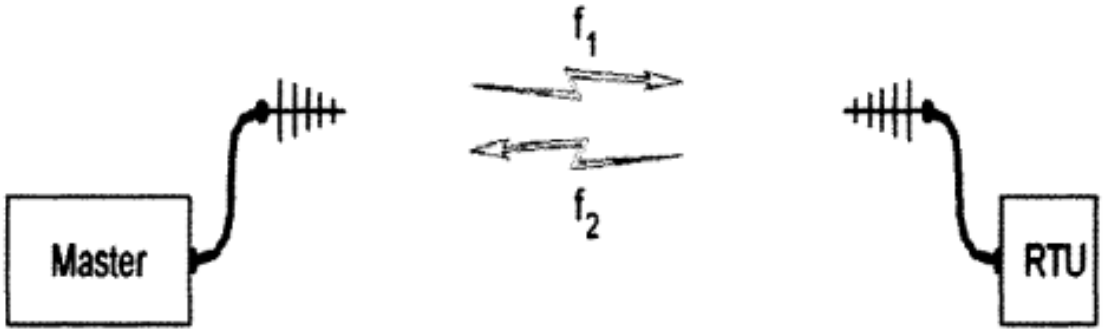
Communication architectures

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.



Multipoint (or multiple stations)

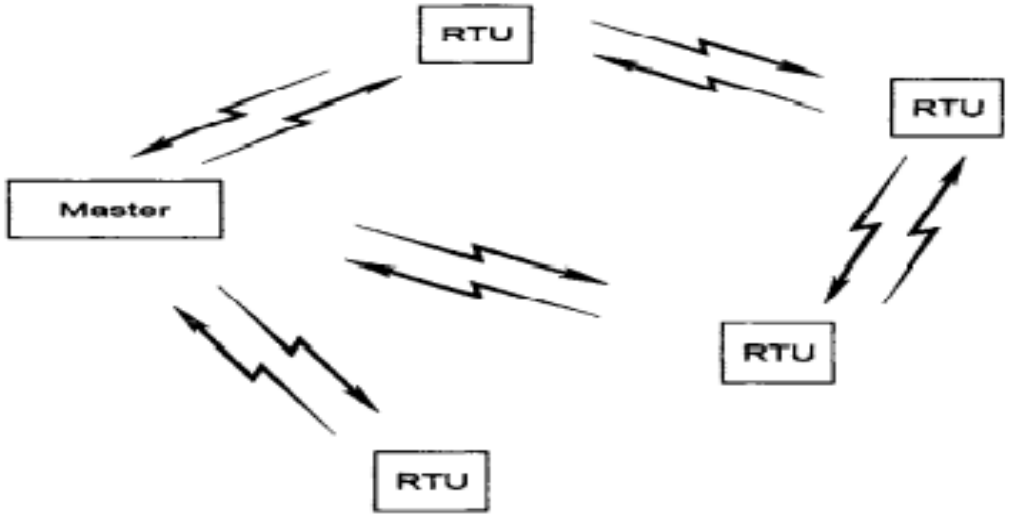
In this configuration, there is generally **one master and multiple slaves**.

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.



Relay Stations

Store and forward relay operation

This can be a component of one station **retransmits** messages onto another station **out of the range** of the **master station**.

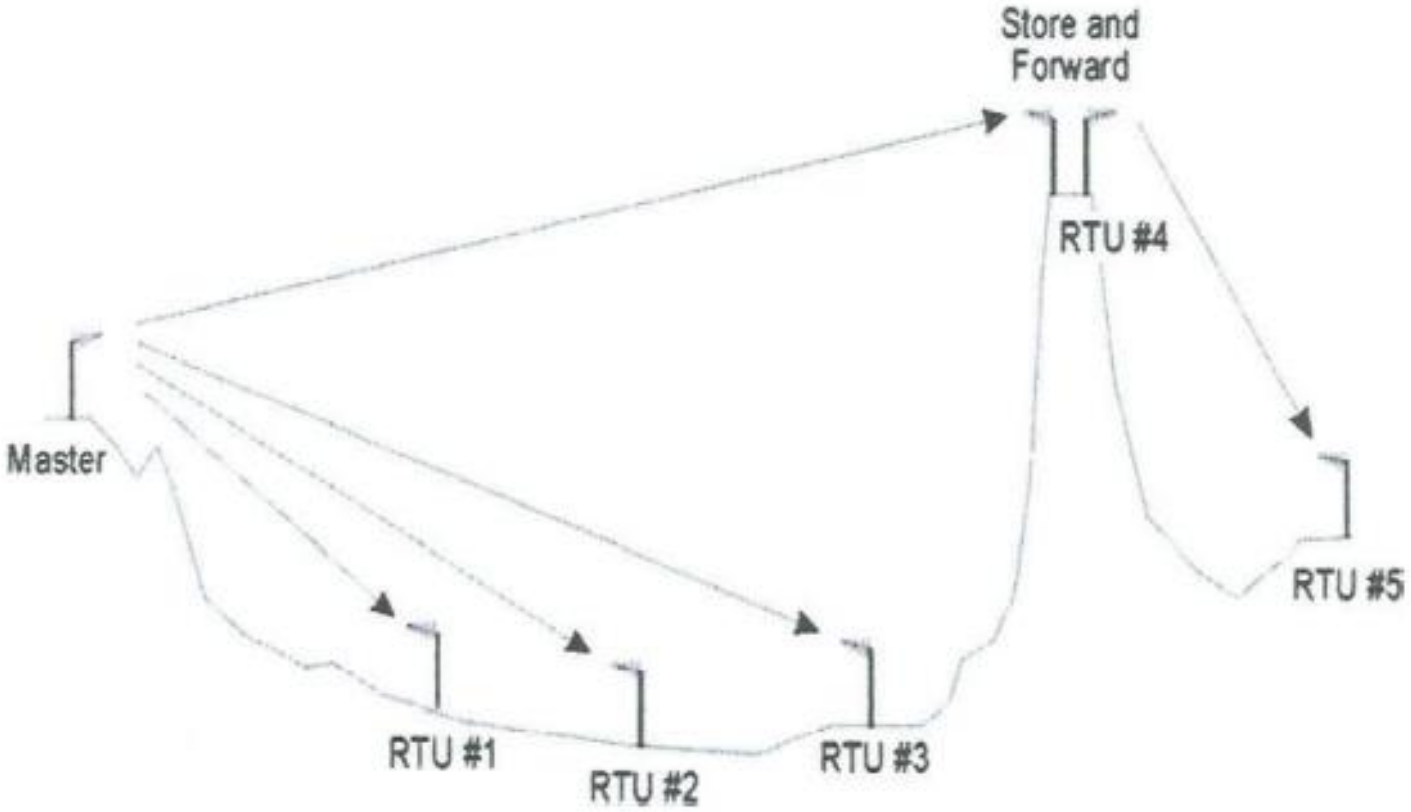
This is often called a **store and forward relay station**.

There is **no simultaneous transmission** of the message by the store and forward station.

It **retransmits the message at the same frequency** as it received it after the message has been received from the master station.

This approach is **slower** than a talk through repeater as each message has to be sent twice. The advantages are considerable savings in mast heights and costs.

Relay Stations



Talk through repeaters

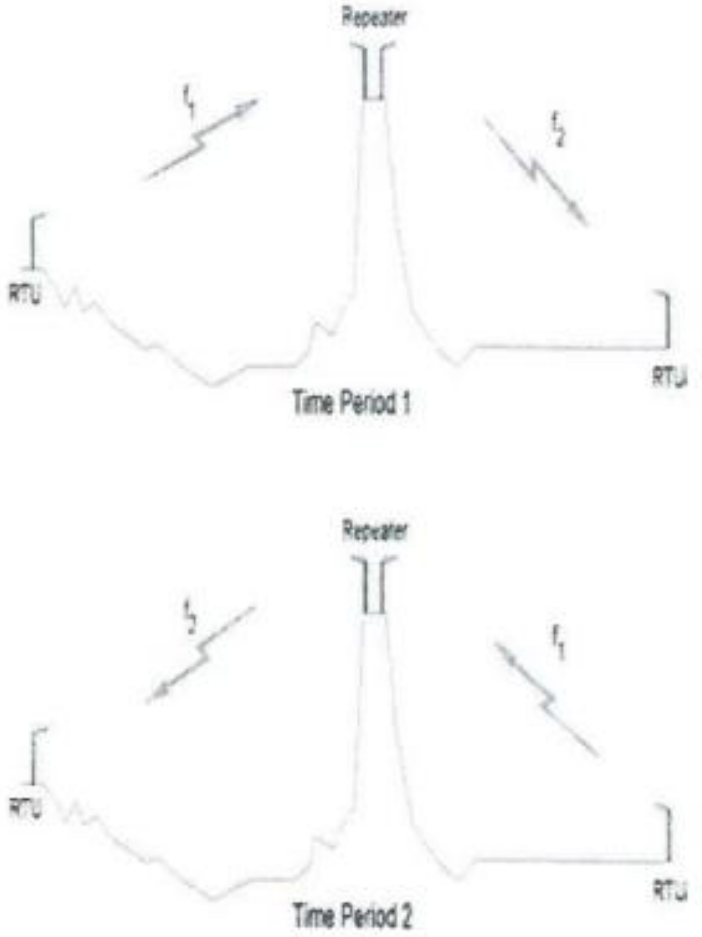
This is the generally preferred way of increasing the **radio system's range**. This retransmits a radio signal received simultaneously on another frequency.

It is normally situated on a **geographically high point**.

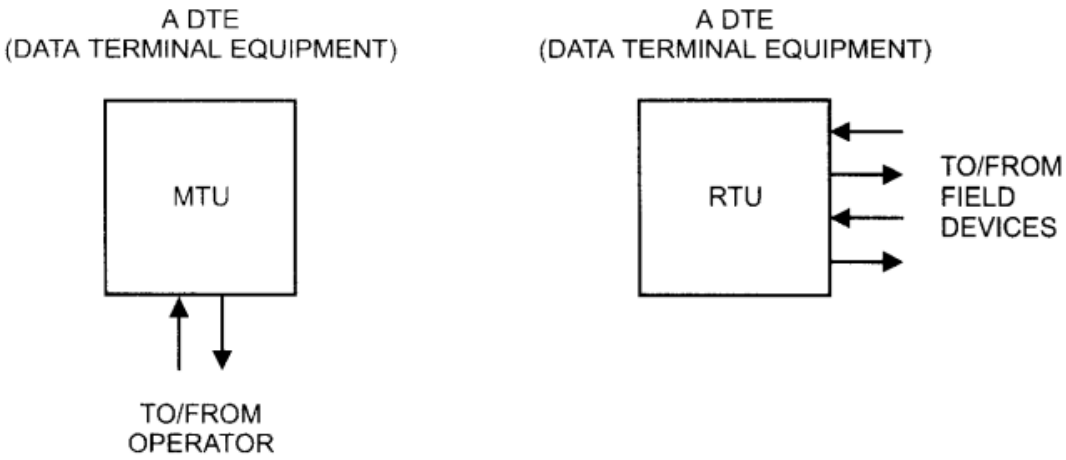
The repeater receives on one frequency and retransmits on another frequency simultaneously.

There is still a **slight time delay** in transmission of data with a repeater.

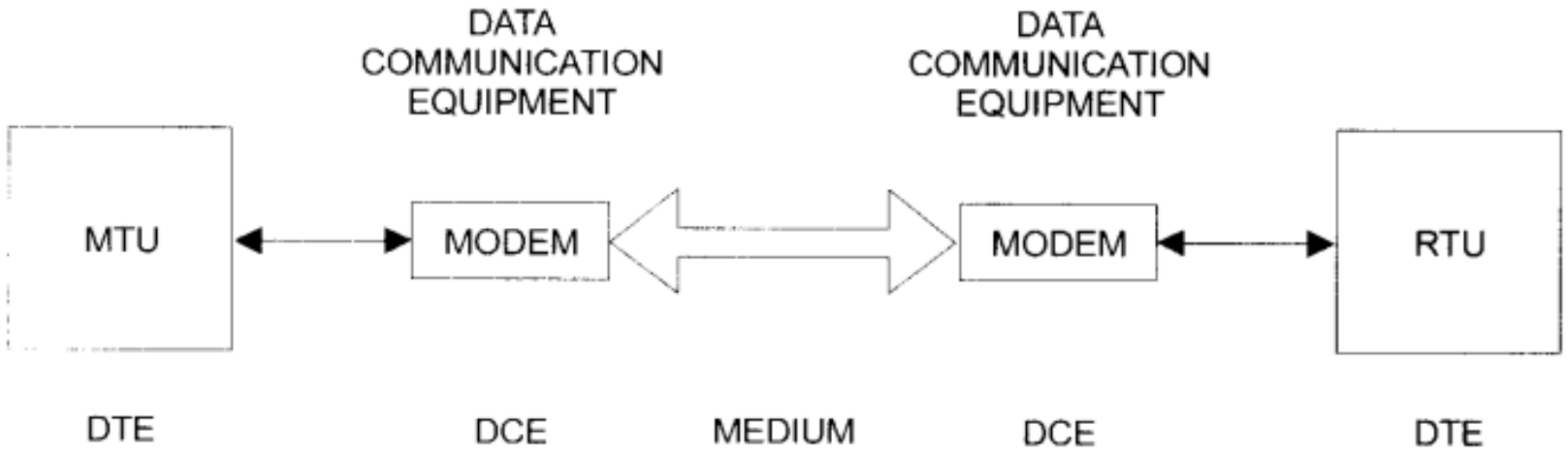
Talk through repeaters



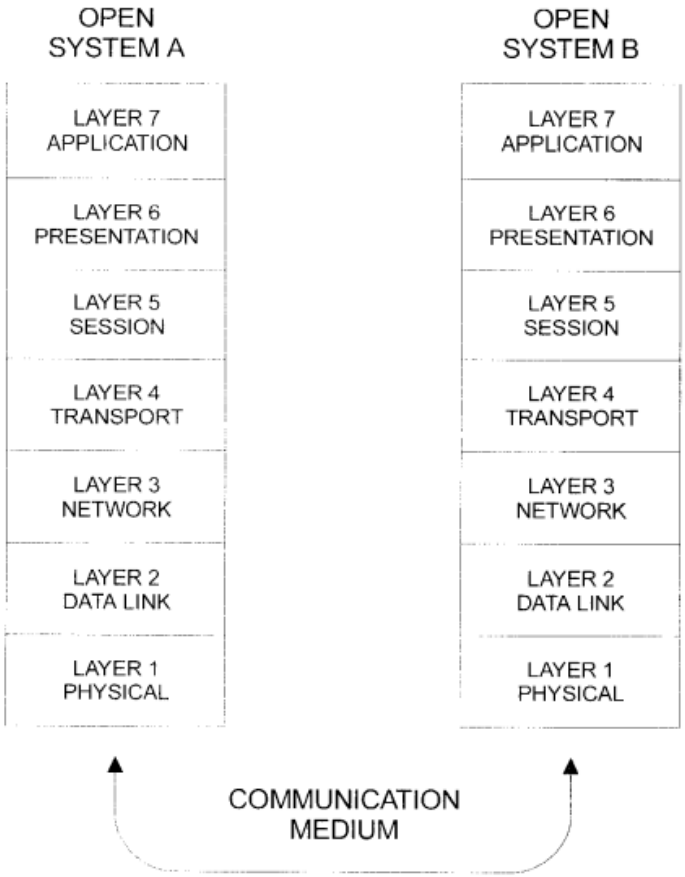
Communication system components



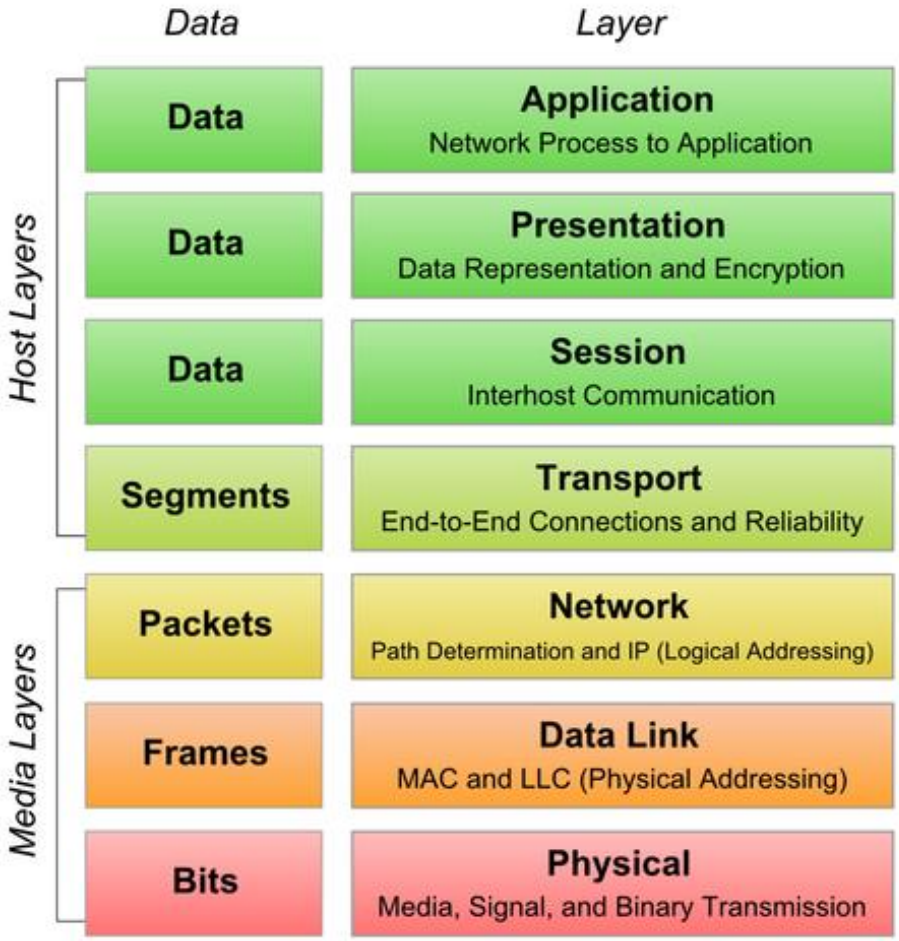
Communication system components



Structure of a SCADA Communications Protocol



OSI Model


Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical Addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Layer 7 – Application

The Application layer is the highest layer of the OSI model, and it provides the interface between the network protocol and the software running on the computer. The Application layer provides the necessary services that support applications. It provides the interface for e-mail, Telnet and File Transfer Protocol applications

Layer 6 – Presentation

The Presentation Layer's primary responsibility is to define the syntax that network hosts use to communicate.

The functions performed at the Presentation layer of the OSI are:

- Protocol conversion
- Data translation.
- Data encryption and decryption
- Data compression
- Character set conversion
- Interpretation of graphics commands

Layer 5 – Session

The Session Layer establishes process to process communications between two or more networked hosts
Establishes, terminates, and monitors communication sessions between applications
Name lookup and security functions.
Placement the header information in a packet which determines the point where a message starts and the point where a message ends.
Data synchronization.
The layer performs synchronization between the Session layer of the data sender and the Session layer of the receiver of the data.
Controls whether the communication or messages being exchanged in a session are transmitted as full duplex messages or half duplex messages.

Layer 4 – Transport

The Transport Layer is responsible for the delivery of messages between two or more networked hosts. It handles fragmentation and reassembly of messages and controls the reliability of a given link.

The important functions performed at the Transport layer to enable network communication are listed below:

- Guaranteed data delivery
- Name resolution
- Flow control
- Error detection
- Error recover

Layer 3 – Network

The Network Layer is primarily responsible for establishing the paths used for transfer of data packets between devices on the network.
Network routers operate at this layer which can commonly be divided into three sub-layers: Sub network access, Sub network-dependent convergence, and Sub network-independent convergence.
The functions performed at the Network layer of the OSI model are listed below:

- Traffic direction to the end destination
- Addressing; logical network addresses and services addresses
- Routing functions; route discovery and route selection
- Packet switching
- Packet sequence control
- End-to-end error detection, from the data sender to the receiver of data.
- Congestion control
- Network layer flow control and Network layer error control
- Gateway services

Layer 2 – Data Link

The Data Link Layer is primarily responsible for communications between adjacent network nodes.
Network switches and hubs operate at this layer which may also correct errors generated in the Physical Layer.

The responsibilities of the Data-link layer include:

- Packet addressing
- Media access control
- Format the frame used to encapsulate data
- Error notification on the Physical layer
- Managing of error messaging specific to the delivery of packets.

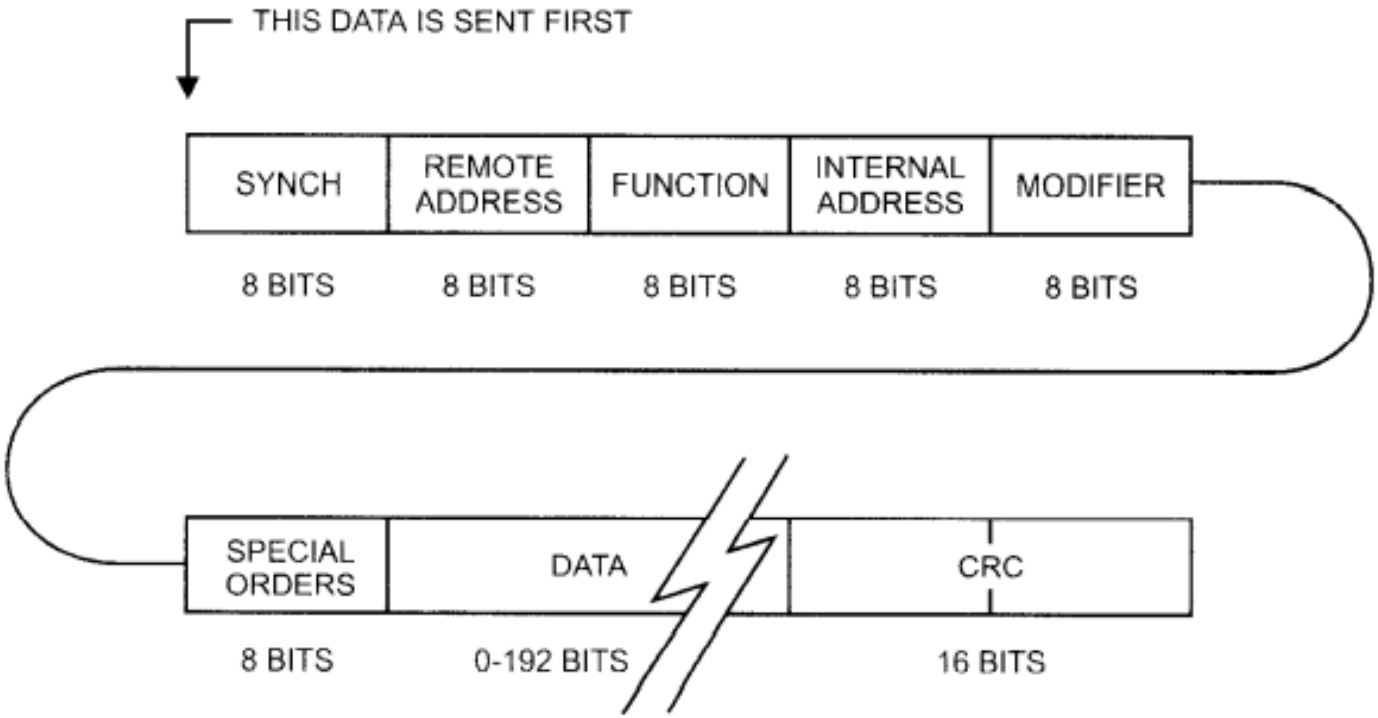
Layer 1 – Physical

The Physical Layer handles the bit level transmission between two or more network nodes.

The specifications of the Physical layer include:

- Physical layout of the network
- Voltage changes and the timing of voltage changes.
- Data rates
- Maximum transmission distances
- Physical connectors to transmission mediums

Message Layout based on IEEE C37.10 protocol



Cyclic codes including CRC can detect many combinations of likely errors

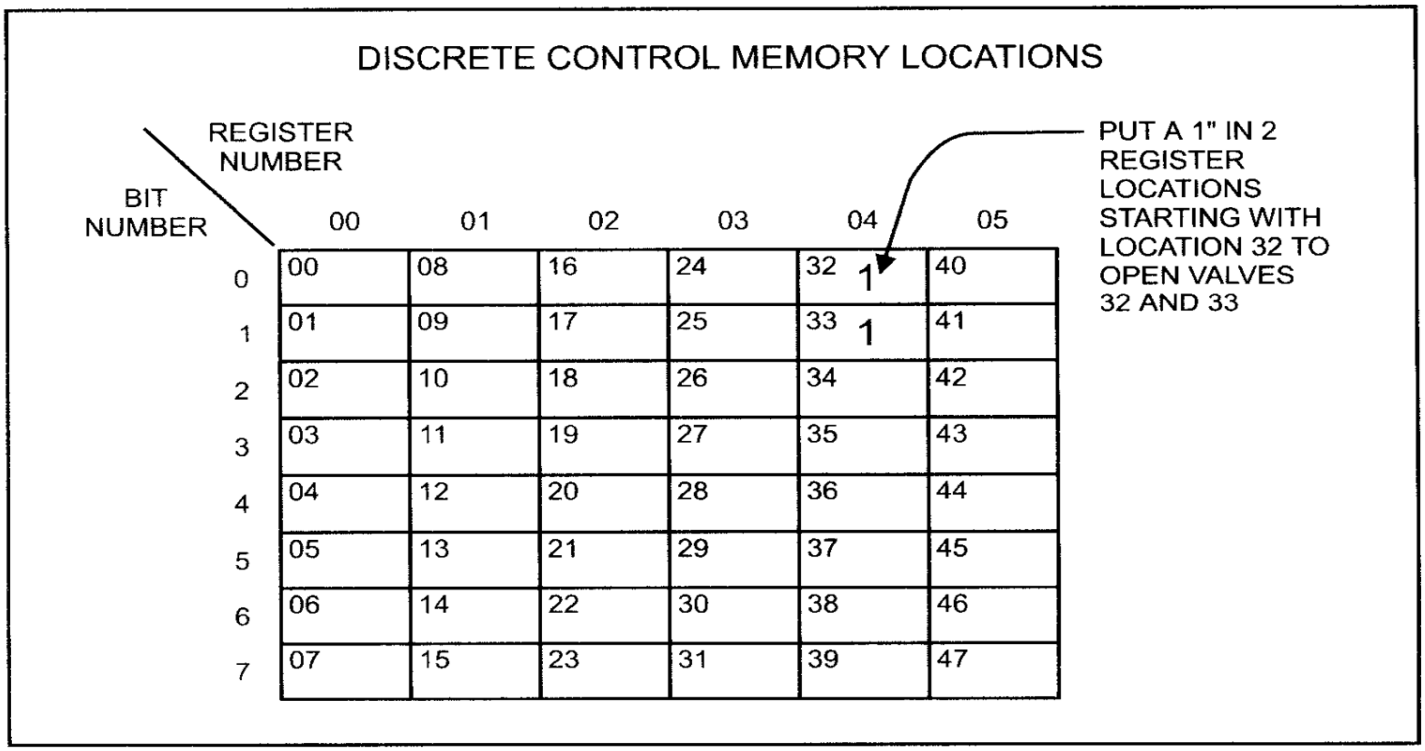
- Single bit errors
- Errors in two consecutive bits
- Any odd number of single bit errors
- Burst errors (a sequence of bits some of which are in error)

Telephone Cable or Radio?

In the past, the choice of communications media was determined by two things: data rate and cost. More and more now, consideration is being given to a third, and that is: security of data.

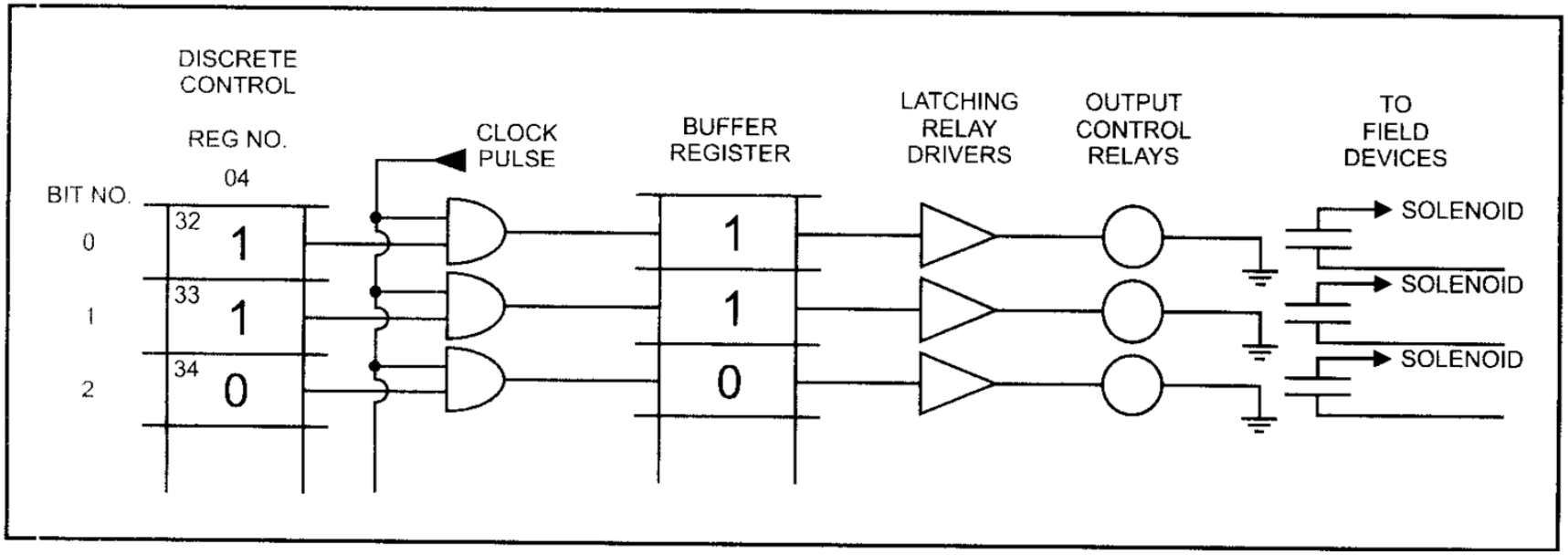
SCADA purposes, it is not feasible to get a short enough scan interval unless the data rate is pushed very high, that is, over 5000 bps. When this situation exists, a communications medium with a bandwidth greater than a voice-grade line will be required, such as optical fiber cable, microwave radio, or one of the more sophisticated UHF systems. Lines leased from

Discrete control



Message to RTU Calling for It to Open a Two-position Valve

Each register can control eight discrete devices.
Valve close – 0
Valve open - 1



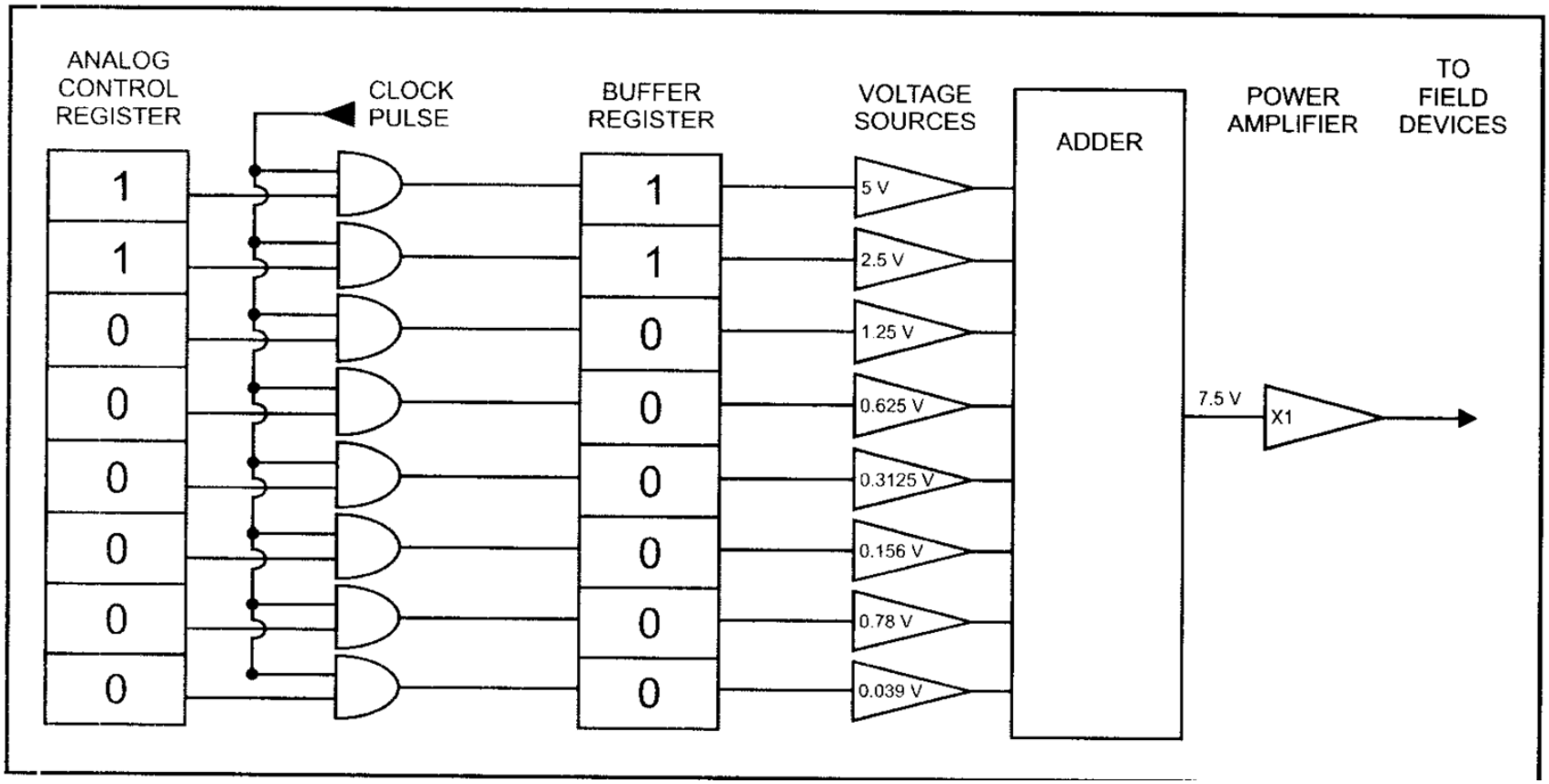
Routine Reading of First Specified Register Position

Analog Control

	CONTROL REGISTER NUMBER 22	BIT VALUE	
BIT 0	1	50%	128/256
BIT 1	1	25%	64/256
BIT 2	0	12.5%	32/256
BIT 3	0	6.25%	16/256
BIT 4	0	3.125%	8/256
BIT 5	0	1.5625%	4/256
BIT 6	0	0.78125%	2/256
BIT 7	0	0.390625%	1/256

MTU Message Calls for Analog Output, Register 22

- Register has been set 11000000 – 75%
- 50% open – 10000000
- 100% open – 11111111
- 60% - 11011001



Analog Output Card