Lect – 2: Supervisory Control And Data Acquisition (SCADA)-SCADA Systems Hardware, Firmware, Software & Protocols, Landlines, LAN systems,Modems

NETWORK

A network is a collection of two or more computers, which are connected together to share data and resources. A centralized network is a network having a central computer called a Server and other computers are called Nodes.

Uses of Network

Networks are mainly used to Sharing Files, Sharing Resources, Saving money and Communication medium

- **Sharing Files/data** :
  Network enable the users to share information with other computers on the network.
- **Sharing Resources**:
  You can set up computer resources, such as a hard disk or a printer or scanner or DVD or CD writer in Network, so that all the computers on the network can access them, that is any one on the network can use it
- **High reliability:**
  All files could be replicated on two or three machines, so if one of them is unavailable (due to a hardware failure, ex: CPU etc), the other copies could be used.
- **Saving Money:**
  Small computers have a much better price than large computer (Ex: Mainframes, Supper computers). Large computers are very faster than small computers but they cost is high. This imbalance has caused many companies (Software or EDP dept. of all companies) to build systems (network) consisting of no of PC (Personal computers) (one per user) with one Large computer to kept on large data.
- **Communication Medium:**
  Using a network, it is easy for two or more people who live far apart to write a report together. When one author makes a change to the documents, which is kept online, the others can see the change immediately.

Network Operating System (NOS):

NOS is an interconnected system of computing devices that provide shared and economical access to computer services. Thus, NOS coordinate the activities of multiple computers across a network.

NOS are divided into two types namely

1. Client / Server network
2. Peer - to – peer network

Client / Server network:

A centralized network is a network having a central computer called a Server and other computers are called Nodes.

A simple definition of CS is " server software accepts requests for data from client software and returns the results to the client".

Resources are controlled by the file server in a Client / Server network

Themain emphasis of Client-Server Architecture is to allow large application to besplit into smaller tasks and to perform the tasks among host (server machine)and desktops (client machine) in the network.

FUNCTIONS OF CLIENT

The client's responsibility is usually to:

- Handle the user interface.
- Translate the user's request into the desired protocol.
- Send the request to the server.
- Wait for the server's response.
- Translate the response into "human-readable" results.
- Present the results to the user.

FUNCTIONS OF SERVER

The server's functions include:

- Listen for a client's query.
- Process that query.
- Return the results back to the client

Peer – to – Peer Network (P2P):

- It does not rely on dedicated servers for communication instead it uses direct connections between clients (Peers).
- Every nodes is able to initiate or complete any supported transaction (file transfer) with the other connected node.
- Resources are shared among equals in a peer – to – peer network

Difference between Peer – to – Peer Network and Client / Server Network

Basis	Peer – to – Peer Network	Client / Server Network
Centralised	No central repository for files and application	Resources and data security are controlled through the server
Maintenance	Low maintenance cost file	Requires extra staff to ensure efficient operation
Installation	Can be easily installed	Requires experts for proper installation
Expensive	No need for a dedicated server	Expensive, as it requires a dedicated server
Security	Lack of proper security	Provides high level of security
Dependence	All nodes are independent of each other.	All clients are dependent on server.

Type of Network

A network can be classified into four primary categories:

1.LAN 2. MAN 3. WAN 4.WLAN

These categories are defined depending upon various factors like the size of the network, the distance it covers, and the type of link used in interconnection.

1. LAN (Local Area Network)

- LAN is a network. It supplies networking capabilities to a group of computers in close proximity to each other such as in an office building, a school.
- On most LANs, cables are used to connect the computers.
- LAN offers a bandwidth of 10 to 100 Mbps.
- A LAN is useful for sharing resources like files, printers, games and other applications.

2. MAN (Metropolitan Area Network)

- MAN is a network of computers spread over a ‘metropolita area such as a city and its suburbs .It covers an entire city. Ex: CATV (Cable television network).

- It may be a means of connecting a number of LANs.
- MAN may be operated by one organization or be shared resources used by several organizations in the same city.

3. WAN (Wide Area Network)

- WAN is a system of interconnecting many computers over a large geographical area such as cities, states, Countries.
- These network use telephone lines, satellite links, and other long-range communications technologies to connect.
- WAN connect multiple smaller networks, such as LANs or MANs.
- The largest WAN in existence is the INTERNET.

4. WLAN

- A Wireless Local Area Network (WLAN) is a wireless communication system that allows computers and workstations to communicate data with each other using radio waves as the transmission medium.
- WLAN is commonly referred to as "Wi-Fi" (wireless fidelity).
- Wireless LANs can be connected to a wired LAN as an extension to the system.
- WLANs can be used in both indoor and outdoor environments.
- Wireless LANs can provide almost all the functionality and high data-trans- mission rates offered by wired LANs
- Data rates for WLAN systems typically vary from 1 Mbps to more than 50 Mbps.

Wifi , lifi

Modem :

- Stands for **mo**dulator – **dem**odulator.
- It is a hardware, which enables a computer to transmit data over telephone lines.
- Modulator – Converts digital signals (data) into analog signals.
- Demodulator – Converts analog signals to digital signals.
- Modem speeds are measured in Kilobits per second (Kbps).
- Modems are of two types, **Internal Modem** and **External Modem**
  Internal Modem : It is a card that is fitted inside the computer with a lead running directly from the computer to the phone socket.
  External Modem : It is a small external box wired between the computer and the phone socket.
- Different modems are capable of different data transfer speeds.
  - Dial-up modems can reach download speeds of 56 kbps.
  - DSL(**Digital Subscriber Line)** modems can download at speeds up to 10 mbps (megabits per second).
  - Cable modems can reach a theoretical download speed of 30 mbps, but the actual speed will almost always be lower because bandwidth is shared by other users.
  - In general, upload speeds are slower than download speeds for all of the above modem types.

Protocol

It is a uniform set of rules that enable the computers to connect and transmit the data to one another

Examples:

IP – Internet Protocol
TCP – Transmission Control Protocol

HTTP (Hyper Text Transfer Protocol) – you are accessing a Web page
FTP (File Transfer Protocol) -- a system for storing and retrieving data files on large computer systems.
NEWS – news server
MAILTO – mail server, used for accessing a E-mail server
TELNET – for accessing remote computers that is a way of connecting directly to computer systems on the Internet.
USENET -- newsgroups, for posting and responding to public "bulletin board" messages.

FTP (File Transfer Protocol)

- It is a system of rules and a software program that enables a user to log on to another computer and transfer information between it and his/her computer.
- It was the first service developed for the Internet. So that government and educational institutions could easily exchange files.
- FTP allows the user to get access to the files stored in the directory of a remote computer that is connected to the Internet.
- Using FTP, one can upload and download files from the remote computer (Knows as FTP servers), if he/she has access permission on the remote machine.
- FTP sites can consists of hundreds to thousands of files with information on books, music, software. Games, images, sounds, multimedia, course work.
- FTP can be done using the command prompt, browsers and GUI based FTP software such as Cuter-FTP and WS_FTP.

Introduction and brief history of SCADA

SCADA is an acronym for Supervisory Control And Data Acquisition, a computer system for gathering and analyzing real time data.

SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.

This manual is designed to provide a thorough understanding of the fundamental concepts and the practical issues of SCADA systems. Particular emphasis has been placed on the practical aspects of SCADA systems with a view to the future. Formulae and details that can be found in specialized manufacturer manuals have been purposely omitted in favor of concepts and definitions. This chapter provides an introduction to the fundamental principles and terminology used in the field of SCADA. It is a summary of the main subjects to be covered throughout the manual. SCADA (supervisory control and data acquisition) has been around as long as there have been control systems. The first 'SCADA' systems utilized data acquisition by means of panels of meters, lights and strip chart recorders. The operator manually operating various control knobs exercised supervisory control. These devices were and still are used to do supervisory control and data acquisition on plants, factories and power generating facilities. The following figure shows a sensor to panel system

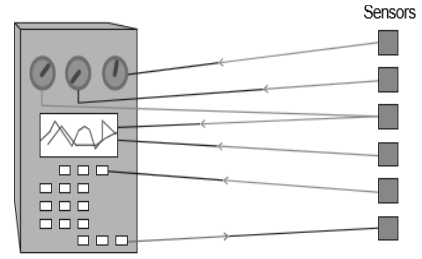


Figure 1.1
Sensors to panel using 4–20 mA or voltage

The sensor to panel type of SCADA system has the following advantages:

- It is simple, no CPUs, RAM, ROM or software programming needed
- The sensors are connected directly to the meters, switches and lights on the panel
- It could be (in most circumstances) easy and cheap to add a simple device like a switch or indicator

The disadvantages of a direct panel to sensor system are:

- The amount of wire becomes unmanageable after the installation of hundreds of sensors
- The quantity and type of data are minimal and rudimentary
- Installation of additional sensors becomes progressively harder as the system grows
- Re-configuration of the system becomes extremely difficult
- Simulation using real data is not possible
- Storage of data is minimal and difficult to manage
- No off site monitoring of data or alarms
- Someone has to watch the dials and meters 24 hours a day

SCADA hardware

A SCADA system consists of a number of remote terminal units (RTUs) collecting field data and sending that data back to a master station, via a communication system. The master station displays the acquired data and allows the operator to perform remote control tasks. The accurate and timely data allows for optimization of the plant operation and process. Other benefits include more efficient, reliable and most importantly, safer operations. This results in a lower cost of operation compared to earlier non-automated systems.

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 sensors situated at each remote site. The communications system provides the pathway for communication between the master station and the remote sites. This communication system can be wire, fiber optic, 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 (or sub-masters) 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, sub-master sites gather information from remote sites and act as a relay back to the control master station.

SCADA software

SCADA software can be divided into two types, proprietary or open. Companies develop proprietary software to communicate to their hardware. These systems are sold as 'turn key' solutions. The main problem with this system is the overwhelming reliance on the supplier of the system. Open software systems have gained popularity because of the interoperability they bring to the system. Interoperability is the ability to mix different manufacturers' equipment on the same system. Citect and WonderWare are just two of the open software packages available in the market for SCADA systems. Some packages are now including asset management integrated within the SCADA system. The typical components of a SCADA system are indicated in the next diagram

Features of SCADA software are:

- User interface
- Graphics displays
- Alarms
- Trends
- RTU (and PLC- Programmable Logic Controller) interface
- Scalability
- Access to data
- Database
- Networking
- Fault tolerance and redundancy
- Client/server distributed processing

Landlines for SCADA

Even with the reduced amount of wire when using a PC to IED system, there is usually a lot of wire in the typical SCADA system. This wire brings its own problems, with the main problem being electrical noise and interference. Interference and noise are important factors to consider when designing and installing a data communication system, with particular considerations required to avoid electrical interference. Noise can be defined as the random generated undesired signal that corrupts (or interferes with) the original (or desired) signal. This noise can get into the cable or wire in many ways. It is up to the designer to develop a system that will have a minimum of noise from the beginning. Because SCADA systems typically use small voltage they are inherently susceptible to noise. The use of twisted pair shielded cat5 wire is a requirement on most systems. Using good wire coupled with correct installation techniques ensures the system will be as noise free as possible. Fiber optic cable is gaining popularity because of its noise immunity. At the moment most installations use glass fibers, but in some industrial areas plastic fibers are increasingly used.

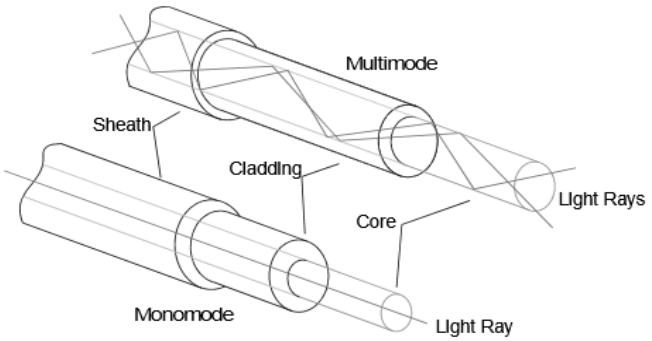


Figure 1.5
Glass fiber optic cables

SCADA and local area networks

Local area networks (LAN) are all about sharing information and resources. To enable all the nodes on the SCADA network to share information, they must be connected by some transmission medium. The method of connection is known as the network topology. Nodes need to share this transmission medium in such a way as to allow all nodes access to the

medium without disrupting an established sender. A LAN is a communication path between computers, file-servers, terminals, workstations, and various other intelligent peripheral equipments, which are generally referred to as devices or hosts. A LAN allows access for devices to be shared by several users, with full connectivity between all stations on the network. A LAN is usually owned and administered by a private owner and is located within a localized group of buildings. Ethernet is the most widely use LAN today because it is cheap and easy to use. Connection of the SCADA network to the LAN allows anyone within the company with the right software and permission, to access the system. Since the data is held in a database, the user can be limited to reading the information. Security issues are obviously a concern, but can be addressed.

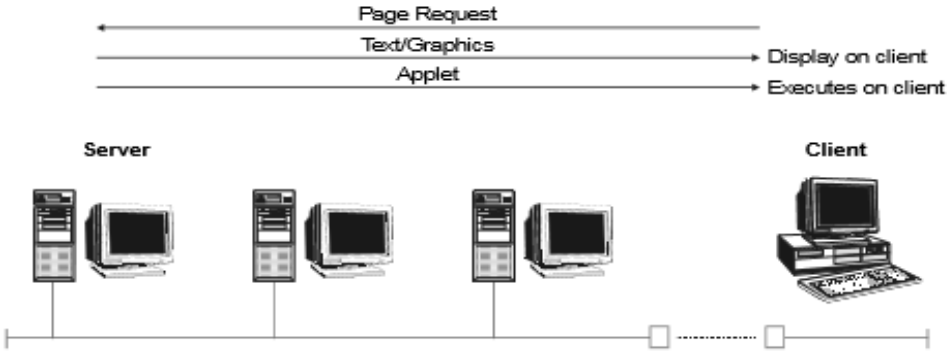


Figure 1.6
Ethernet used to transfer data on a SCADA system

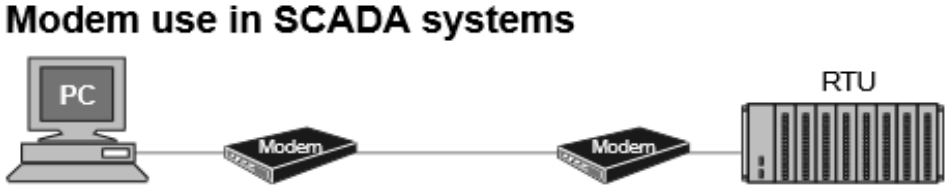


Figure 1.7
PC to RTU using a modem

Often in SCADA systems the RTU (remote terminal unit (PLC, DCS or IED)) is located at a remote location. This distance can vary from tens of meters to thousands of kilometers. One of the most cost-effective ways of communicating with the RTU over long distances can be by dialup telephone connection. With this system the devices needed are a PC, two dialup modems and the RTU (assuming that the RTU has a built in COM port). The modems are put in the auto-answer mode and the RTU can dial into the PC or the PC can dial the RTU. The software to do this is readily available from RTU manufacturers. The modems can be bought off the shelf at the local computer store.

Line modems are used to connect RTUs to a network over a pair of wires. These systems are usually fairly short (up to 1 kilometer) and use FSK (frequency shift keying) to communicate. Line modems are used to communicate to RTUs when RS-232 or RS- 485 communication systems are not practical. The bit rates used in this type of system are usually slow, 1200 to 9600 bp

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 802.5 (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. MAP/PLC type industrial systems)

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.

Token ring LANs

The second type of network is the token ring system, which was developed by IBM in the early eighties. It is common in the office type environment but not as popular for industrial type systems. It uses a token message to pass control from one node to another. When a node receives the token, it has control of the ring network for a short maximum period of time. When this time is up the token must be passed onto the next node. Alternatively, if the node has no messages to transmit, the token is immediately passed onto the next node.

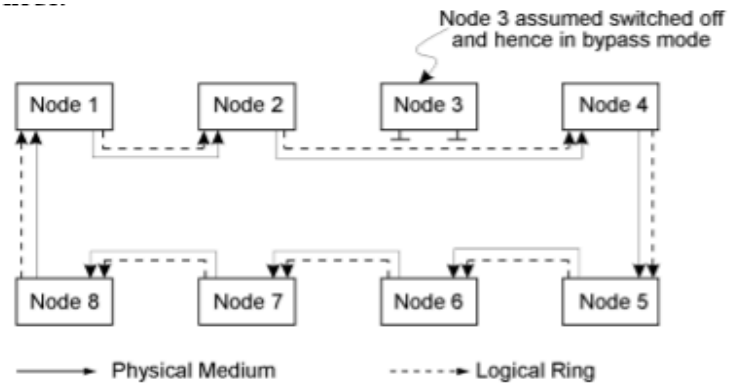
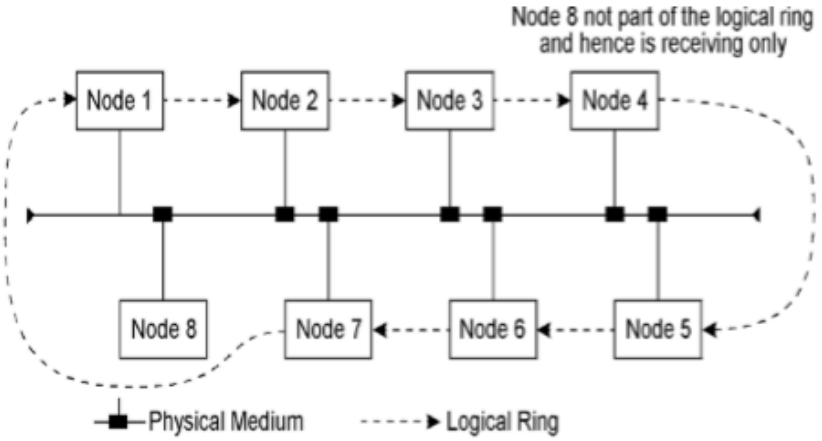


Figure 2.34
Token ring system

Figure 2.34 indicates a typical problem with the ring type network where a node fails (or is switched off) but does not disrupt the operation of the network, due to bypass relays acting to ensure there is a continuous signal path between nodes 2 and 4.

Token bus network

The token bus network is becoming increasingly popular in industrial systems due to its philosophy that all nodes will receive access to a bus with a guaranteed maximum time. The philosophy is similar to that of the token ring network with the use of a token to pass control from node to node.


Node 8 not part of the logical ring
and hence is receiving only
Node 1
Node 2
Node 3
Node 4
Node 8
Node 7
Node 6
Node 5
Physical Medium
Logical Ring