SCADA is a system of hardware and software elements that facilitate process control. This central control system consist of communication equipment, network interfaces, input/ output devices and software. It allows organizations to carry out following functions:

- Manage industrial processes remotely or locally.
- Real-time data gathering, monitoring and processing.
- Direct interaction with devices like valves, motors, pumps, valves using Human Machine Interface (HMI) software.
- Create a log file of events.

History of SCADA

Earlier, the controlling of industrial plants and manufacturing floors can be done manually with the help of analog equipment and push-buttons. As the industry's size is growing, so they employed timers and relays to provide supervisory control to a fixed level for minimal automation. So, a fully automated with a more efficient system was necessary for all the industries.

We know that, for industrial control purposes, computers were implemented in the year 1950. After that, the concept of telemetry was implemented for data transmission as well as virtual communication. In the year 1970, the SCADA system was developed along with the microprocessors as well as PLC.
So these concepts were fully helped while developing automation that is operated in industries remotely. The distributed SCADA systems were implemented in the year 2000. After that, new SCADA systems were developed to monitor & control real-time data anyplace in the globe.

Architecture

These SCADA elements are defined as follows:

■■ **Operator**: Human operator who monitors the SCADA system and performs supervisory control functions for the remote plant operations

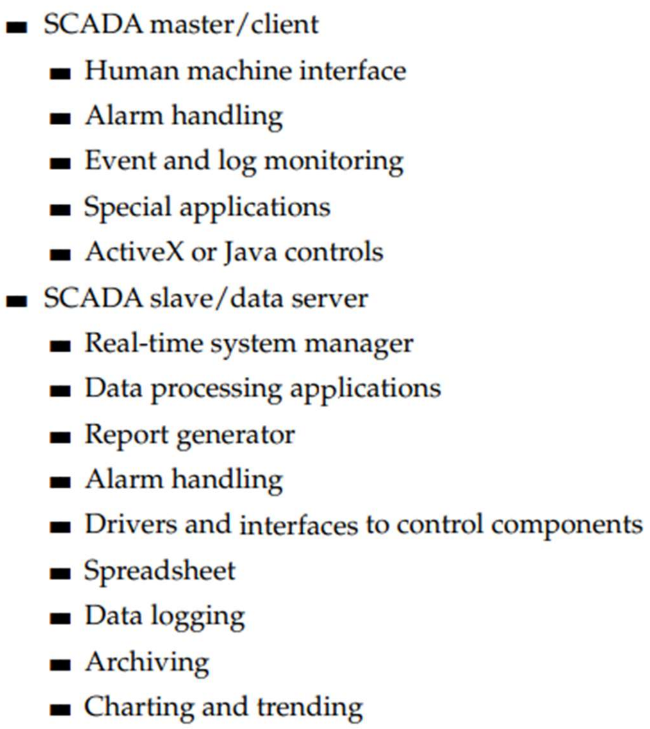
. ■■ **Human machine interface (HMI):** Presents data to the operator and provides for control inputs in a variety of formats, including graphics, schematics, windows, pull-down menus, touch-screens, and so on.

■■ **Master terminal unit (MTU):** Equivalent to a master unit in a master/ slave architecture. The MTU presents data to the operator through the HMI, gathers data from the distant site, and transmits control signals to the remote site. The transmission rate of data between the MTU and the remote site is relatively low and the control method is usually open loop because of possible time delays or data flow interruptions.

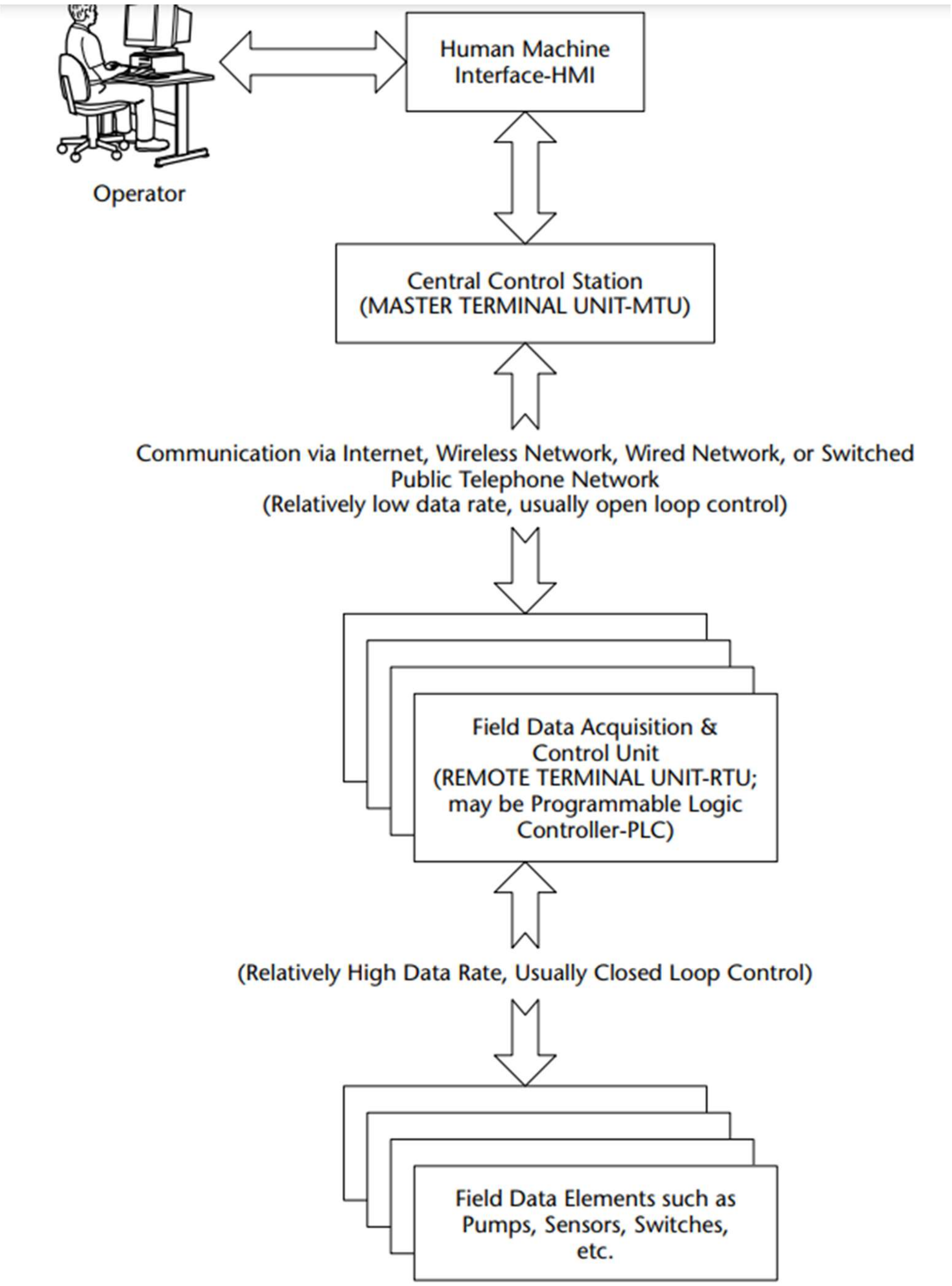
■■ **Communications means:** Communication method between the MTU and remote controllers. Communication can be through the Internet, wireless or wired networks, or the switched public telephone network.

■■ **Remote terminal unit (RTU):** Functions as a slave in the master/slave architecture. Sends control signals to the device under control, acquires data from these devices, and transmits the data to the MTU. An RTU may be a PLC. The data rate between the RTU and controlled device is relatively high and the control method is usually closed loop

In addition to the hardware, the software components of the SCADA architecture are important. Here are some of the typical SCADA software components:



- SCADA master/client
  - Human machine interface
  - Alarm handling
  - Event and log monitoring
  - Special applications
  - ActiveX or Java controls
- SCADA slave/data server
  - Real-time system manager
  - Data processing applications
  - Report generator
  - Alarm handling
  - Drivers and interfaces to control components
  - Spreadsheet
  - Data logging
  - Archiving
  - Charting and trending


Operator
Human Machine Interface-HMI
Central Control Station (MASTER TERMINAL UNIT-MTU)
Communication via Internet, Wireless Network, Wired Network, or Switched Public Telephone Network
(Relatively low data rate, usually open loop control)
Field Data Acquisition & Control Unit (REMOTE TERMINAL UNIT-RTU; may be Programmable Logic Controller-PLC)
(Relatively High Data Rate, Usually Closed Loop Control)
Field Data Elements such as Pumps, Sensors, Switches, etc.

Desirable properties

A good description of the desired properties of a SCADA system is given in the North American Electric Reliability Council (NERC) definition of SCADA reliability objectives

NERC Form 715 defines reliability as:

Adequacy: The capacity to meet system demand within major component ratings in the presence of scheduled and unscheduled outage of generation and transmission components or facilities

Security: A system's capability to withstand system disturbances arising from faults or unauthorized internal or external actions without further loss of facilities, compromise of human safety, and loss of production

Features of SCADA

The important features of SCADA are the following :

1. Alarm Handling
2. Trend Curves Patterns
3. Data Access and Retrieval
4. Computer Networking and Processing

Alarms Handling

Alarm handling consists essentially of time stamped alarms to 1 millisecond precision. Single network acknowledgment and control of alarms with Sharing and Displaying of Alarms to all clients in chronological order.

It performs Dynamic allocation of alarm pages and keeps track of deviation and rate of change monitoring for analog alarms. It has the option of Historical alarm and event logging. It is capable of performing On-line alarm disable and threshold modification with the option of preparing Event-triggered alarms and Alarm-triggered reports

Trends

Trend curves and patterns consists of Trend zooming and display of data. It performs Export and Archiving of historical trend data with Event based trends for Short and long term trend display. It has the option of On-line change of time-base and retrieval of archived historical trend data.

Real Time access and archiving and database Management.

Real time access and data retrieval consists of Direct, real-time access to data by any network user as well as Third-party access to real-time data. It has Network compatibility for read, write and exec to all I/O device points. Support for Direct SQL commands or high level reporting

Computer Networking and processing

Computer Networking and processing aspect of supports all compatible networks and protocols. It has Centralized alarm, trend and report processing – data available from anywhere in the network and Dual networks for full LAN redundancy. Open architecture design with Real-time multitasking are important features with Client/server fully supported with Distributed project updates and Concurrent support of multiple display nodes.

Types of SCADA System

There are Three different types of SCADA systems from four generations. They are:

1. Early or Monolithic SCADA Systems (First Generation)
2. Distributed SCADA Systems (Second Generation)
3. Networked SCADA Systems (Third Generation)

1. Early or Monolithic SCADA Systems (First Generation)

Minicomputers were used in the earlier Supervisory Control and Data Acquisition systems. Monolithic systems were developed during times when ordinary network services were unavailable. These were designed to be independent systems without any connection to other systems.

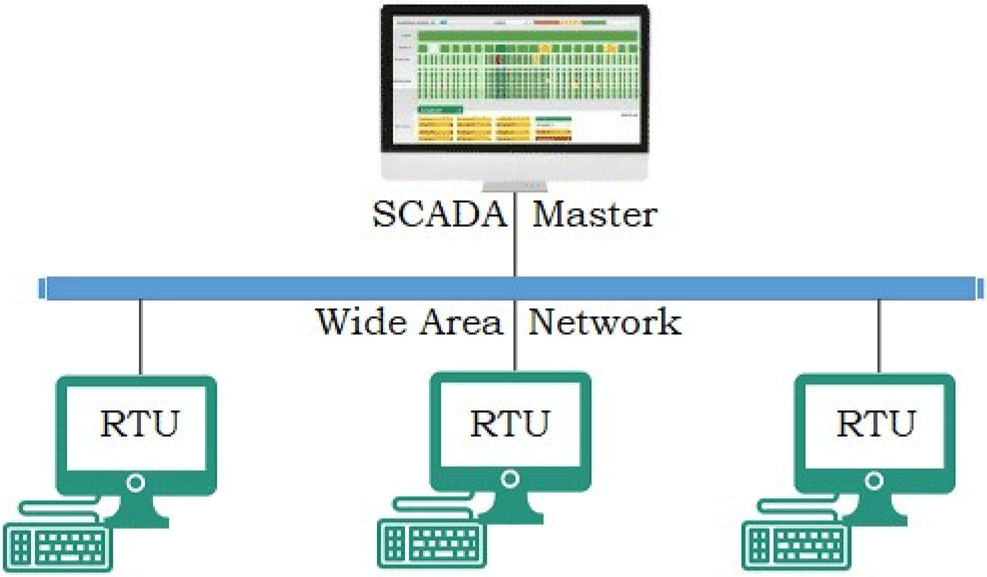


Fig. 6 – Monolithic SCADA System

All the remote terminal unit sites would connect to a back-up mainframe system for achieving the first generation SCADA system redundancy, which was used in case of failure of the primary mainframe system. The functions of the monolithic SCADA systems in the early first generation were limited to monitoring sensors in the system and flagging any operations in case of surpassing programmed alarm levels.

2. Distributed SCADA Systems (Second Generation)

In the second generation, the sharing of control functions is distributed across the multiple systems connected to each other using Local Area Network (LAN). Hence, these were termed as distributed SCADA systems. These individual stations were used to share real-time information and command processing for performing control tasks to trip the alarm levels of possible problems.

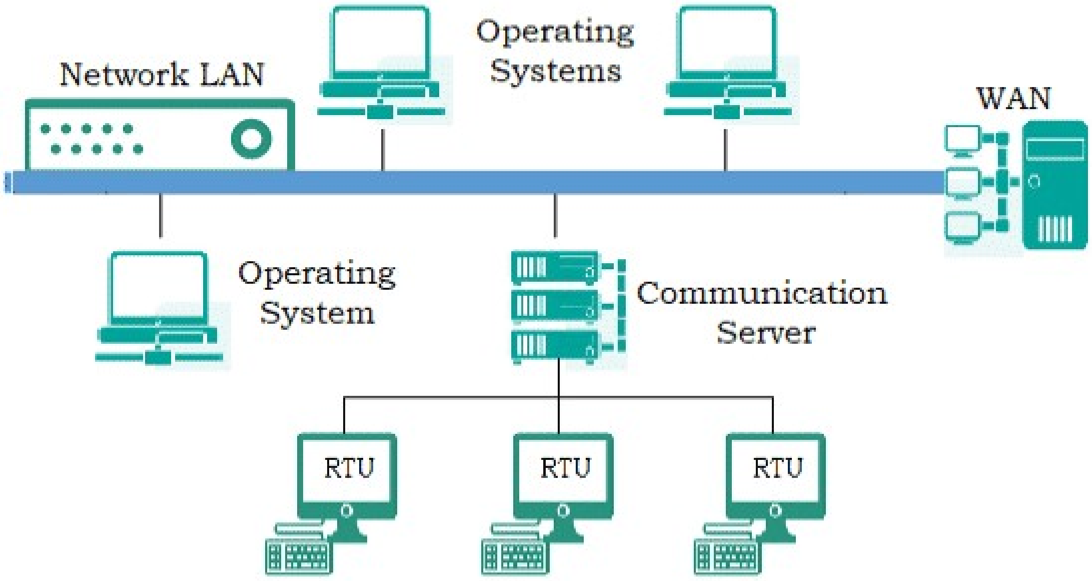


Fig. 7 – Distributed SCADA Systems

The second generation resulted in the reduction of size and cost of each station but there were no standardized network protocols. Since the protocols were proprietary, very few people understood the security of Supervisory Control and Data Acquisition system installation and this factor was largely ignored.

3. Networked SCADA Systems (Third Generation)

Present Supervisory Control and Data Acquisition systems are networked and communicate over WAN system through phone or data lines. Fiber optic connections or Ethernet is used for data transmission between the nodes.

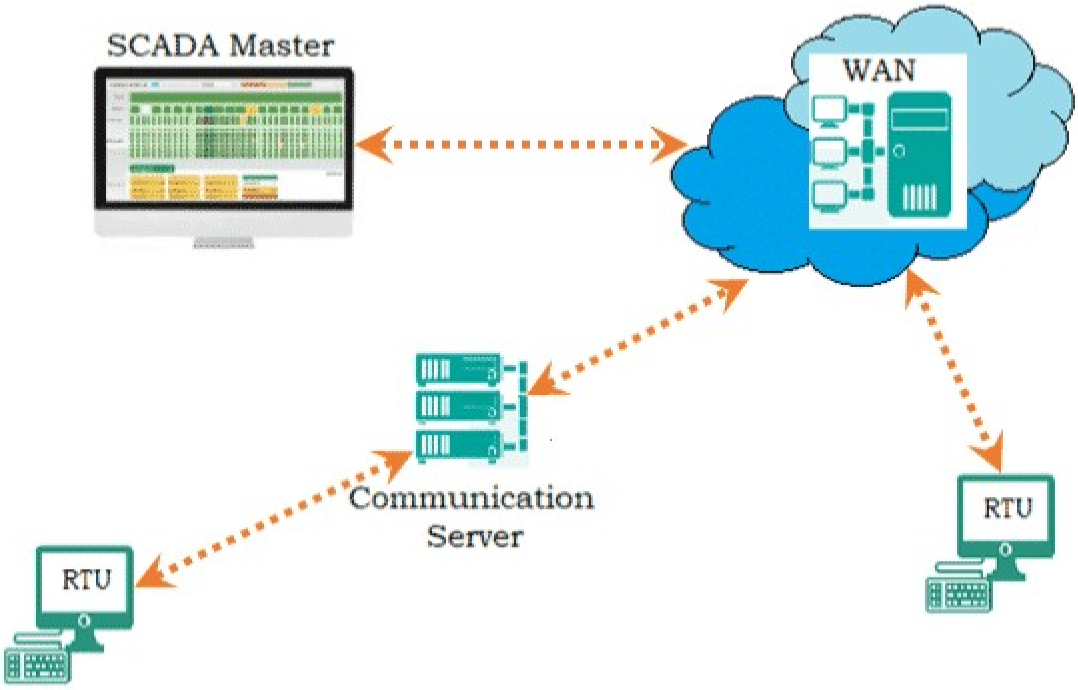


Fig. 8 – Network SCADA System

These systems use PLC for adjusting and monitoring the flagging operations only when there is a requirement for major decisions.

The first and second generation SCADA systems are limited to single site networks or single building called as sealed systems. In these systems, we can not have any risk compared to the third generation SCADA system which are connected to the internet causing the security risks. There will be several parallel working distributed SCADA systems under a single supervisor in network architecture.

Difference between PLC and SCADA

The difference between PLC and SCADA include the following.

PLC	SCADA
The term PLC stands for programmable logic control	The term SCADA stands for Supervisory Control and Data Acquisition
PLC is hardware-based	SCADA is software-based

PLCs are mainly used to control the process of complex industries like motors and running machines.	SCADA is used to observe & run the processes of the plant.
The PLC includes Processor, I/O Modules, a Programming Device & Power Supply	The SCADA system includes three essential components like MTU, RTU, and HMI
There are different types of PLC like fixed or compact & modular.	The different types of a SCADA system are monolithic, distributed, networked & IoT
The i/p & o/ps are signified in NO (normal open), NC (normal close) & coil contacts.	The input & outputs of SCADA are represented through images.
In PLC, every component can be defined through an address.	In SCADA, each component can be defined through the name.

Advantages

The advantages of the SCADA system include the following.

- The quality of service can be improved
- Reliability can be improved
- Maintenance cost is less
- The operation can be reduced
- Large system parameters can be monitored
- Manpower can be reduced
- Repair time can be reduced
- Fault detection & fault localization
- It stores a large amount of data
- As per the user requirement, it displays the data in various formats.
- Thousands of sensors can be interfaced with SCADA for controlling and monitoring
- Real data simulations can be obtained by operators
- Gives fast response
- It is flexible as well as scalable while adding extra resources.
- The SCADA system provides onboard mechanical and graphical information
- The SCADA system is easily expandable. We can add a set of control units and sensors according to the requirement.
- The SCADA system is able to operate in critical situations.

Disadvantages

The disadvantages of the SCADA system include the following.

- It is complex in terms of dependent modules & hardware units.
- It needs analysts, programmers & skilled operators to maintain
- High installation cost
- Unemployment rates can be increased
- This system supports hardware devices and restricted software's

Applications of SCADA System

Supervisory Control and Data Acquisition systems are mainly used to monitor a wide data variety like currents, voltages, temperature, pressure, water levels etc. in several industries. If any abnormal conditions are detected, alarms at remote or central sites are triggered for operator alert. The various applications of SCADA Systems include:

1. **Power Generation & Distribution**: Used to monitor current flow, voltage, circuit breaker functions. Also used in remotely switching on/ off of power grids.
2. **Water & Sewage System**: Used by municipal corporations for regulating and monitoring water flow, reservoir status, pressure in distribution pipes, etc.
3. **Industries and Buildings**: Used to control HVAC, central air conditioning, lighting, entry/ exit gates, etc.
4. **Oil and Gas Industries**: Used for regulating and monitoring flow, reservoir status, pressure in distribution pipes, etc.
5. **Communication Networks**: Used for monitoring and controlling servers, networks and nodes.
6. **Manufacturing**: Used for managing inventories for controlling over manufacturing/ stocking. Also used for monitoring and regulating instrumentation, process and product quality.
7. **Public Transport**: Used for regulating subway electricity, automating traffic signals/ railway crossing and live tracking of flights/ trains/ buses
8. Generators and turbines
9. Traffic light control system

Petroleum Refining

- Petroleum refineries are extremely important elements in a nation's critical infrastructure.
- Goods and services depend on transportation by planes, trucks, cars, trains, and boats and on the myriad of engines running on petroleum based
- fuels.
- The principal function of a refinery is to distill and perform various chemical reactions on the crude oil input.
- These operations require temperatures on the order of 500 to 1,000 degrees Fahrenheit
- Pressures ranging from 150 pounds per square inch (psi) to 3,500 psi.
- In addition to the general fuel products, hydrogen (H) is used and generated and the toxic compounds hydrogen sulfide (H2S) and ammonia (NH3) are generated.
- In a refinery distillation column the component hydrocarbons can be separated because they have diferent boiling points that reach from approximately 50 degree Farhenheit to 1400 degree farhenheit
- The sulfur is removed through *hydrotreating*
- This operation is known as *hydrodesulfurization or (HDS)*

- A product of this reaction is the toxic gas hydrogen sulphide (H2S), which results from hydrogen atoms combing with sulfur atoms.
- It is clear that petroleum refinieries must be kept under strict control in all phases of hydrocarbon processing or serious damage to human life property and eventually the economy will result
- Result of successful SCADA system attacks might include exceeding temperature and floor escape of toxic liquids and vapors and contamination of catalysis
-

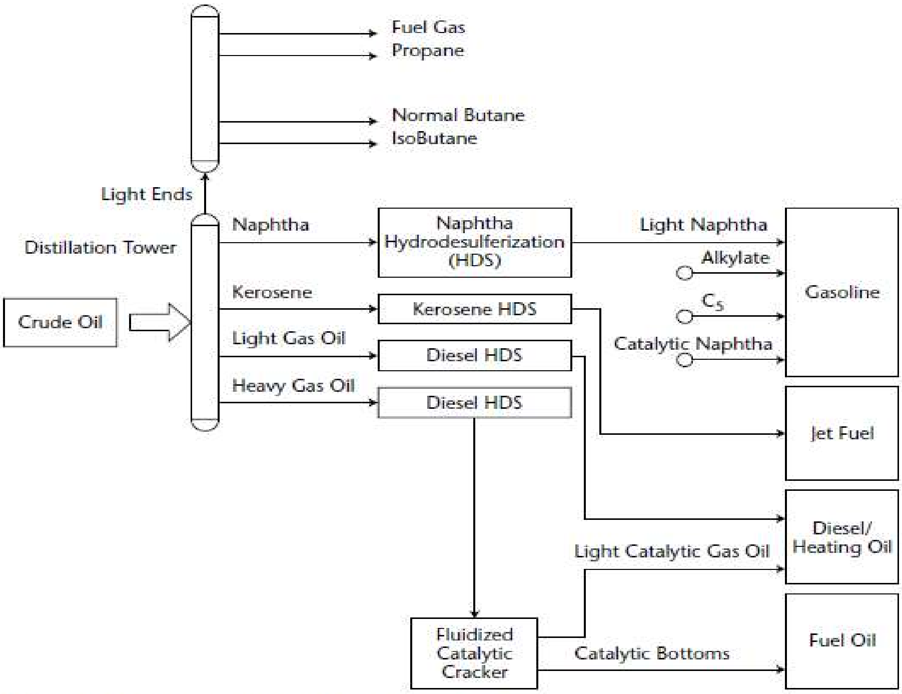


Figure 2-1 The petroleum refining process

Conventional Electric Power Generation

- Conventional electric power generating facility produces electricity by harnessing the energy of falling water or by generating heat through the burning of fossil fuels.
- As in nuclear power plants, the heat is applied to water, steam is generated, and the steam is used to power turbines that turn electricity generators.
- The electrical energy is then transmitted and distributed at different voltages to power substations.
- Figure 2-4 provides a geographic overview of a fossil fuel electric plant and
- Also the subsequent path of the generated electricity to an end user.

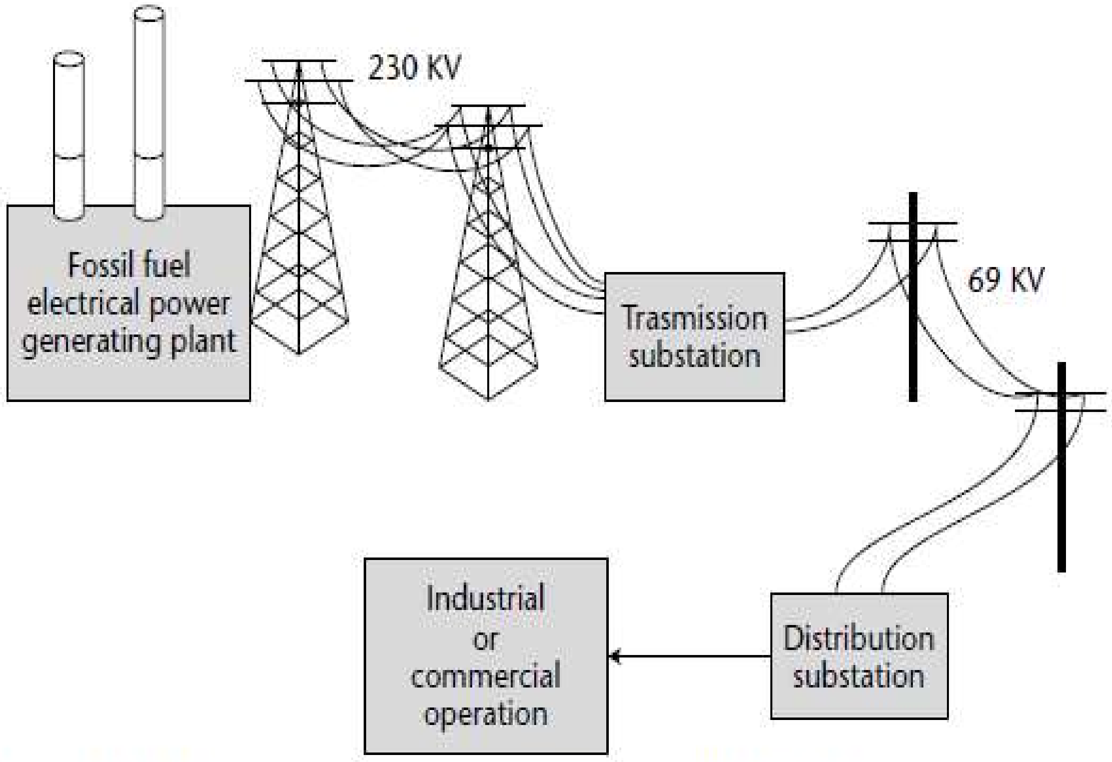

Fossil fuel electrical power generating plant
230 KV
Trasmission substation
69 KV
Distribution substation
Industrial or commercial operation

Figure 2-4 Electrical power generation and geographic distribution overview

Water Purification System

- In a typical water purification operation, water is pumped from a reservoir or other water source to a water purification plant.
- After purification, the water is pumped through a transmission system to the water consumers.
- In designing a water purification system, the following items are considered:
- Future expandability
- Terrain traversed by the water pipelines
- Control of system functions and performance
- Maintenance of water quality

For this type of operation a SCADA system is applied to control and monitor the water purification process, pumping system and pipeline pressures.

Because of the distance involved in same installation, radio models are used to communicate between the central supervisory stations and the remote locations

Possible attack scenarios on a water purification and transmission system include jamming or interference with radio communication links, disabling or interrupting the water purification process, inserting false pressure and pump data to disrupt transmission operation and modifying water reservoir information

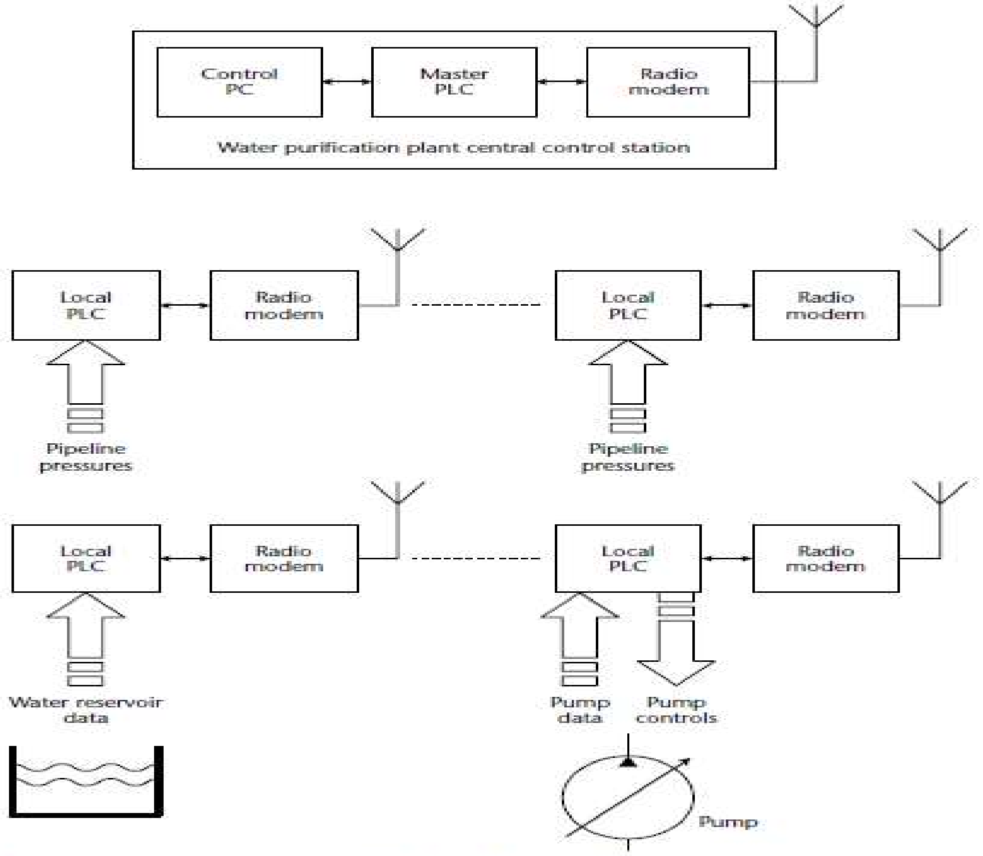
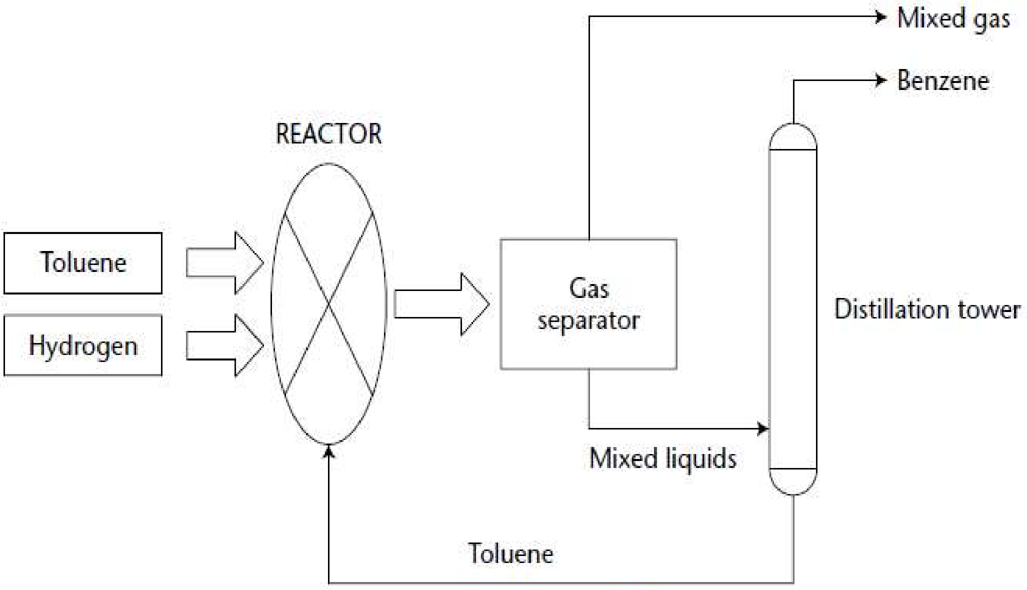


Figure 2-8 Water purification and transmission system

Chemical Plant

- These plants or storage facilities manufacture or hold highly toxic chemicals such as chlorine gas, benzene, anhydrous ammonia, and boron trifluoride.
- The latter is colorless gas that can kill by attacking a person’s mucous membranes
- **Benzene Production:**
- Benzene is produced by three different methods. These methods are steam cracking, catalytic reforming, and toluene hydrodealkylation.
- This example features toluene hydrodealkylation.
- In the toluene hydrodealkylation process, hydrogen reacts with toluene over a catalyst bed with temperatures between 500 and 600 degrees Celsius and 40 to 60 atmospheres of pressure.
- Here is the chemical reaction:
- Figure 2-11 is a process flow diagram for benzene production.



$C_7H_8 + H_2 \longrightarrow C_6H_6 + CH_4$

Figure 2-11 General diagram of benzene production plant