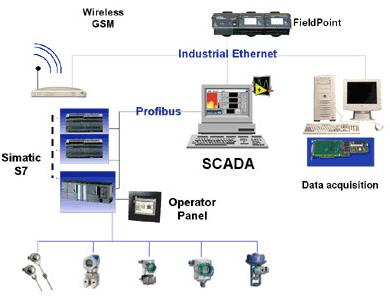
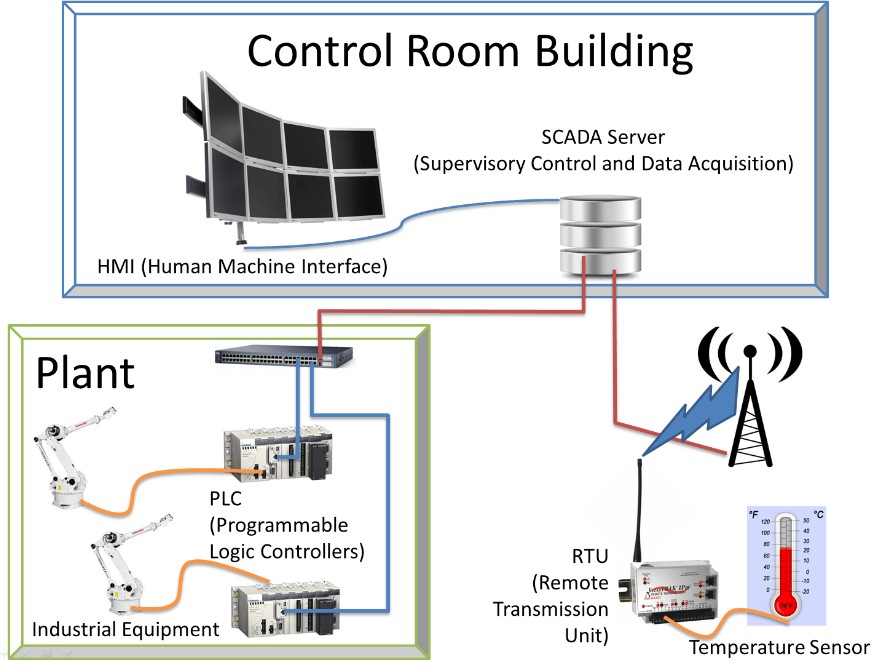
**SCADA Systems Architecture and Types with Applications**

Advancements in Intelligent Instrumentation and Remote Terminal Units (RTUs) / Programmable Logic Controllers (PLCs) have made the process-control solutions in many of the industries to be easily managed and operated by utilizing the benefits of a SCADA system. SCADA is popular in several applications like process industries, oil and gas, electric power generation, distribution and utilities, water and waste control, agriculture/irrigation, manufacturing, transportation systems, and so on. Let us know about the[SCADA system](http://en.wikipedia.org/wiki/SCADA)‘s working principle in brief from this article.

**What is SCADA System?**

SCADA stands for Supervisory Control and Data Acquisition; it is an industrial computer-based control system employed to gather and analyze the real-time data to keep track, monitor and control industrial equipments in different types of industries. Consider the application of SCADA in power systems for operation and control.

SCADA in power system can be defined as the power distribution application which is typically based on the software package. The electrical distribution system consists of several substations; these substations will have multiple numbers of controllers, sensors and operator-interface points.



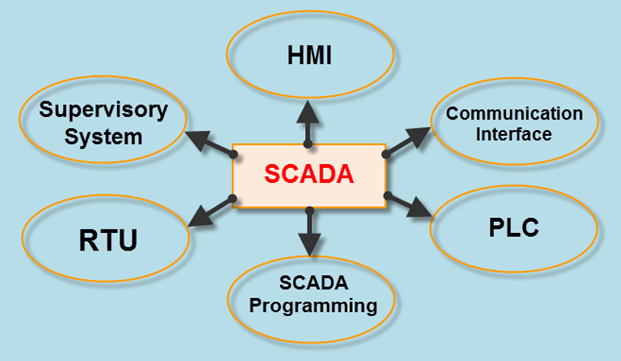
**SCADA System**

In general, for controlling and monitoring a substation in real time Programmable Logic Controllers (PLCs), Circuit breakers and Power monitors are used. Data is transmitted from the PLCs and other devices to a computer-based-SCADA node located at each substation. One or more computers are located at different centralized control and monitoring points.

SCADA system usage have become popular from the 1960s with the increase in need of monitoring and controlling the equipment. Early systems built using mainframe computers were expensive as they were manually operated and monitored. But the recent advancements in technology have made-advanced, automated SCADA systems with maximum efficiency at reduced cost, according to the alarming requirements of the company.

**SCADA Basics**

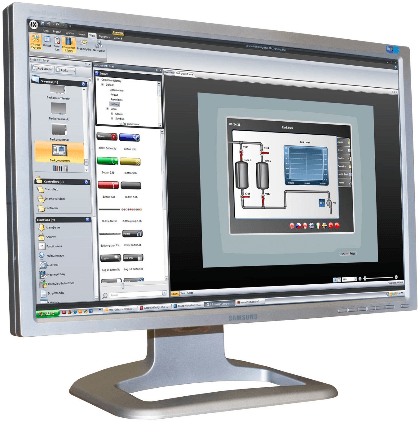
Before discussing about the architecture of SCADA and different types of SCADA systems, primarily we must know a few SCADA basics. Consider the block diagram of SCADA system shown in the figure which consists of different blocks, namely Human-machine Interface (HMI), Supervisory system, Remote terminal units, PLCs, Communication infrastructure and SCADA Programming.



**Basics of SCADA**

**1. Human-machine Interface (HMI)**

It is an input-output device that presents the process data to be controlled by a human operator. It is used by linking to the SCADA system’s software programs and databases for providing the management information, including the scheduled maintenance procedures, detailed schematics, logistic information, trending and diagnostic data for a specific sensor or machine. HMI systems facilitate the operating personnel to see the information graphically.



**Human-Machine Interface**

**2. Supervisory System**

Supervisory system is used as server for communicating between the equipment of the SCADA system such as RTUs, PLCs and sensors, etc., and the HMI software used in the control room workstations. Master station or supervisory station comprises a single PC in smaller SCADA systems and, in case of larger SCADA systems, supervisory system comprises distributed software applications, disaster recovery sites and multiple servers. These multiple servers are configured in a hot-standby formation or dual-redundant, which continuously controls and monitors in case of a server failure for increasing the integrity of the system.

**3. Remote Terminal Units**

Physical objects in the SCADA systems are interfaced with the microprocessor controlled electronic devices called as Remote Terminal Units (RTUs). These units are used to transmit telemetry data to the supervisory system and receive the messages from the master system for controlling the connected objects. Hence, these are also called as Remote Telemetry Units.

**4. Programmable Logic Controllers**

In SCADA systems, PLCs are connected to the sensors for collecting the sensor output signals in order to convert the sensor signals into digital data. [PLCs](https://www.watelectronics.com/how-to-program-the-programmable-logic-controllers/) are used instead of RTUs because of the advantages of PLCs like flexibility, configuration, versatile and affordability compared to RTUs.



**Programmable Logic Controllers**

**5. Communication Infrastructure**

Generally, the combination of radio and direct wired connections is used for SCADA systems, but in case of large systems like power stations and railways SONET/SDH are frequently used. Among the very compact SCADA protocols used in SCADA systems – a few communication protocols, which are standardized and recognized by SCADA vendors – send information only when the supervisory station polls the RTUs.

**6. SCADA Programming**

SCADA programming in a master or HMI is used for creating maps and diagrams which will give an important situational information in case of an event failure or process failure. Standard interfaces are used for programming most commercial SCADA systems. SCADA programming can be done using derived programming language or C language.

**SCADA System Architecture**

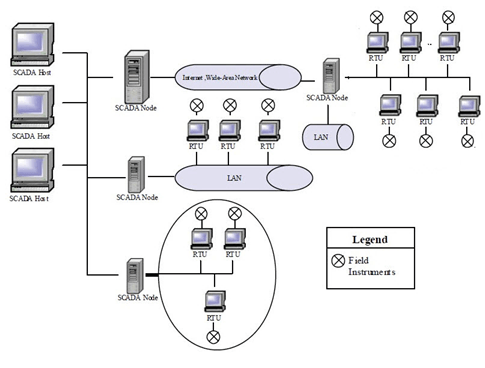
Generally, the SCADA system is a centralized system that monitors and controls the entire area. It is a pure software package that is positioned on top of the hardware. A supervisory system gathers data on the process and sends the commands control to the process. The SCADA is a remote terminal unit which is also known as RTU.

Most control actions are automatically performed by RTUs or PLCs. The RTUs consists of the programmable logic converter which can be set to specific requirement.

For example, in the thermal power plant, the water flow can be set to a specific value or it can be changed according to the requirement. The SCADA system allows operators to change the set point for the flow, and enable alarm conditions in case of loss of flow and high temperature, and the condition is displayed and recorded. The SCADA system monitors the overall performance of the loop.

The SCADA system is a centralized system to communicate with both wired and wireless technology to Clint devices. The SCADA system controls can run completely all kinds of the industrial process.

For example, if too much pressure is building up in a gas pipeline the SCADA system can automatically open a release valve.



**Architecture of SCADA**

The block diagram of SCADA system shown in the figure represents the basic SCADA architecture. The SCADA systems are different from distributed control systems that are commonly found in plant sites. When distributed control systems cover the plant site, SCADA system cover much larger geographic areas.

Above figure depicts an integrated SCADA architecture which supports TCP/IP, UDP and other IP based communication protocols as well as industrial protocols like Modbus TCP, Modbus over TCP, or Modbus over UDP. These all work over cellular, private radio or satellite networks.

In complex SCADA architectures, there are a variety of wired and wireless media & protocols involved in getting data back to the monitoring site. This allows implementation of powerful IP based SCADA networks over landline, mixed cellular and satellite systems. SCADA communications can utilize a diverse range of wired and wireless media.

The choice of the existing communication depends on the characterization of a number of factors. The factors are remoteness, available communications at the remote sites, existing communications infrastructure, polling frequency and data rates. These factors impact the final decision for SCADA architecture. Therefore, a review of SCADA systems evolution allows us to better understand many security concerns.

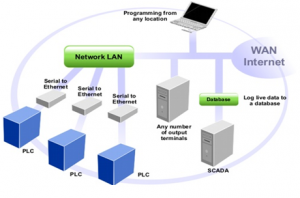
**Hardware Architecture**

The generally SCADA system can be classified into two parts:

* Client layer: The clint layer caters to the man-machine interaction.
* Data server layer: The data server layer handles most of the process of data activities.

The SCADA station refers to the servers and it is composed of a single PC. The data servers communicate with devices in the field through process controllers like PLCs or RTUs. The PLCs are connected to the data servers either directly or via networks or buses. The SCADA system utilizes a WAN and LAN networks, the WAN and LAN consist of internet protocols used for communication between the master station and devices.

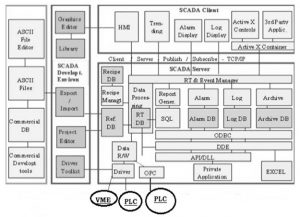
The physical equipment like sensors connected to the PLCs or RTUs. The RTUs convert the sensor signals to digital data and sends digital data to the master. According to the master feedback received by the RTU, it applies the electrical signal to relays. Most of the monitoring and control operations are performed by RTUs or PLCs as we can see in the figure.



SCADA System Hardware Architecture

**Software Architecture**

Most of the servers are used for multitasking and real-time database. The servers are responsible for data gathering and handling. The SCADA system consists of a software program to provide trending, diagnostic data, and manage information such as scheduled maintenance procedures, logistic information, detailed schematics for a particular sensor or machine, and expert-system troubleshooting guides. This means the operator can see a schematic representation of the plant being controlled.



Software Architecture of SCADA

Examples are alarm checking, calculations, logging, and archiving; polling controllers on a set of parameters, those are typically connected to the server.

**SCADA System Working**

The SCADA system performs the following functions

* Data Acquisitions
* Data Communication
* Information/Data presentation
* Monitoring/Control

These functions are performed by sensors, RTUs, controllers, a communication network.  The sensors are used to collect the important information and RTUs are used to send this information to the controller and display the status of the system. According to the status of the system, the user can give the command to other system components. This operation is done by the communication network.

**Data Acquisitions:** The real-time system consists of thousands of components and sensors. It is very important to know the status of particular components and sensors. For example, some sensors measure the water flow from the reservoir to the water tank and some sensors measure the value pressure as the water is released from the reservoir.

**Data Communication:** The SCADA system uses a wired network to communicate between users and devices. Real-time applications use a lot of sensors and components which should be controlled remotely. The SCADA system uses internet communications. All information is transmitted through the internet using specific protocols. Sensors and relays are not able to communicate with the network protocols so RTUs used to communicate sensors and network interfaces.

**Information/Data Presentation:** The normal circuit networks have some indicators which can be visible to control but in the real-time SCADA system, there are thousands of sensors and alarm which are impossible to be handled simultaneously. The SCADA system uses the HMI to provide all the information gathered from the various sensors**.**

**Monitoring/Control:** The SCADA system uses different switches to operate each device and displays the status of the control area. Any part of the process can be turned ON/OFF from the control station using these switches. SCADA system is implemented to work automatically without human intervention but in critical situations, it is handled by manpower.

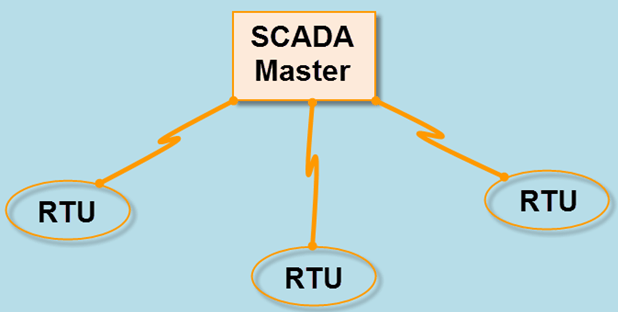
**Types of SCADA systems**

There are different types of SCADA systems that can be considered as SCADA architectures of four different generations:

1. First Generation: Monolithic or Early SCADA systems
2. Second Generation: Distributed SCADA systems
3. Third Generation: Networked SCADA systems and
4. Fourth Generation: Internet of things technology, SCADA systems

**1. Monolithic or Early SCADA Systems**

Minicomputers were used earlier for computing the SCADA systems. In earlier times, during the time of first generation, monolithic SCADA systems were developed wherein the common network services were not available. Hence, these are independent systems without having any connectivity to other systems.

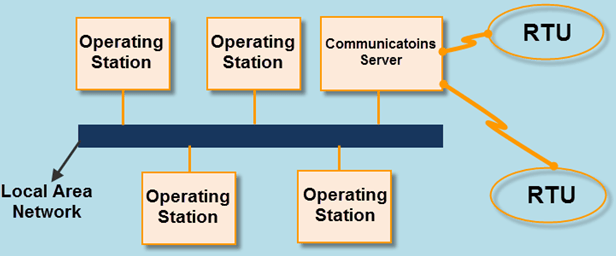


**Monolithic or Early SCADA Systems**

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**

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.

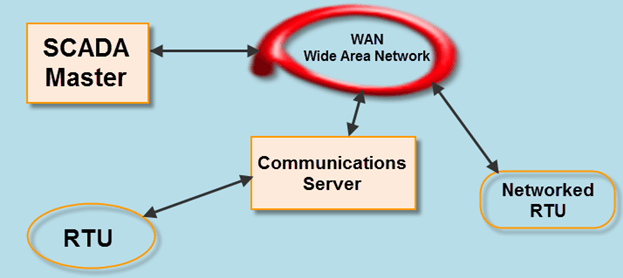


**Distributed SCADA Systems**

The cost and size of the station were reduced compared to the first-generation system, as each system of the second generation was responsible for performing a particular task with reduced size and cost. But even in the second-generation systems also the network protocols were not standardized. The security of the SCADA installation was determined by a very few people beyond the developers, as the protocols were proprietary. But generally, the security of the SCADA installation was ignored.

**3. Networked SCADA Systems**

The current SCADA systems are generally networked and communicate using WANs over data lines or phone. These systems use Ethernet or Fiber Optic Connections for transmitting data between the nodes frequently. These third generation SCADA systems use Programmable Logic Controllers (PLC) for monitoring and adjusting the routine flagging operators only in case of major decisions requirement.

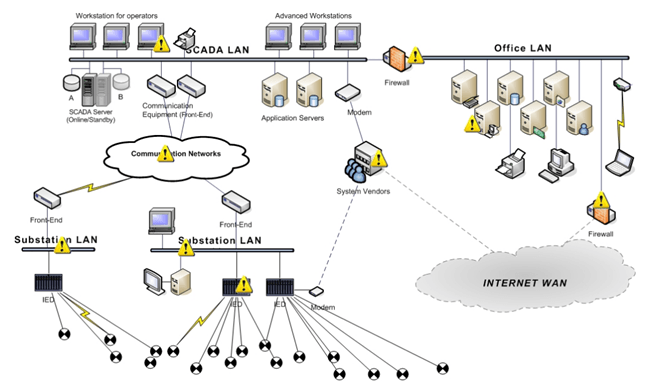


**Networked SCADA Systems**

The first- and second-generation SCADA systems are limited to single site networks or single building called as sealed systems. In these systems, we cannot 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.

**4. Internet of Things**

In fourth generation, the infrastructure cost of the SCADA systems is reduced by adopting the internet of things technology with the commercially available cloud computing. The maintenance and integration are also very easy for the fourth generation compared to the earlier SCADA systems.



**Internet of Things**

These SCADA systems are able to report state in real time by using the horizontal scale from the cloud computing facility; thus, more complex control algorithms can be implemented which are practically sufficient to implement on traditional PLCs.

The security risks in case of decentralized SCADA implementations such as a heterogonous mix of proprietary network protocols can be surpassed using the open network protocols such as TLS inherent in the internet of things which will provide comprehendible and manageable security boundary.

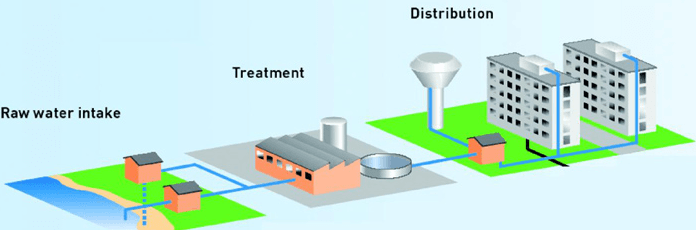
**Applications of SCADA**

SCADA systems are used for monitoring a variety of data like flows, currents, voltages, pressures, temperatures, water levels, and etc., in various industries. If the system detects any abnormal conditions from any monitoring data, then the alarms at the central or remote sites will be triggered for alerting the operators through HMI.

There are numerous applications of SCADA systems, but a few most frequently used SCADA applications are discussed in the following.

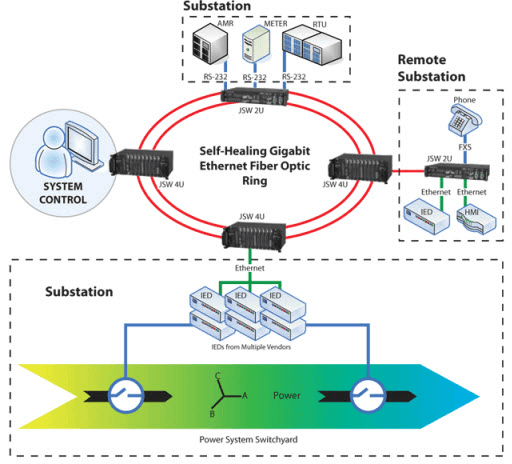
**1. SCADA In Manufacturing Industries:** In manufacturing industries, the regular processes like running the production systems to meet the productivity targets, checking the number of units produced and counting the completed stages of operations along with temperatures at various stages of the manufacturing process, and so on, are taken care by using the SCADA application.

**2. SCADA Application in Wastewater Treatment and Distribution Plants:** Wastewater treatment plants are of different types such as surface-water treatment and a well water treatment system in which many control systems and automation processes are involved in water treatment and distribution systems. SCADA systems are used for controlling the automatic operations of the equipment used like backwashing the filters based on the hours of working or amount of water flow through the filters. In distribution plants the water tank levels, pressure of system, temperature of plant, sedimentation, filtration, chemical treatment and other parameters or processes are controlled using the SCADA applications such as PLCs, PC based workstations which are connected each other using LAN such as Ethernet.



**Waste Water Treatment and Distribution Plants**

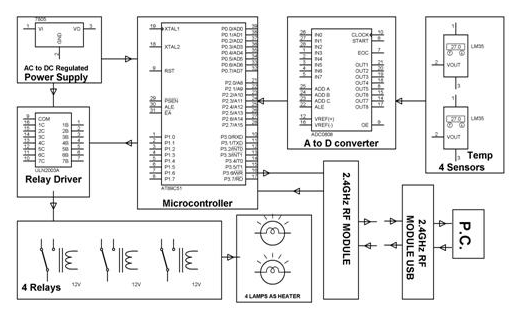
**3. Power Systems:** Power system can be defined as constituent of power generation, transmission, and distribution. All these sectors are needed to be monitored regularly for improving the system efficiency. Thus, the application of SCADA in power system improves the overall efficiency of the system by providing the supervision and control over the generation, transmission and distribution systems. SCADA in the power system network increases the system’s reliability and stability for integrated grid operation.



**SCADA in Power System**

**Wireless SCADA**

In large scale industries like power plants, steel plants and so on, many processes and operations such as movement of conveyer belts for coal or product transport, boiler heat temperature, etc. are to be monitored continuously and there is need to control the factors affecting these parameters. So, application of wireless SCADA will provide better control over the required control systems and operations.



**Wireless SCADA Block Diagram**

In this project 2.4 GHz wireless transmitter and USB receiver are used for sending and receiving the data collected from the temperature sensors which interface with 8051 microcontroller.  If the temperature goes beyond the set limit whether the low limit or high limit, then the microcontroller sends commands to the relays to turn on or off based on the command signal.

Monitoring and controlling of multiple operations in maximum number of industries are being automatically controlled by most advanced SCADA technology implementations. Already we are observing that many industrial operations are automatically controlled using the application of SCADA system technology, but still many researchers are working to develop more efficient SCADA systems for adopting full automatic control of all types of industrial operations. Having any queries and ideas? Post your comments in the comment section below for any technical help for implementing your ideas to develop real time projects.

**SCADA Security**

At present, SCADA networks are used extensively in current industries to check & examine real-time data, industrial processes can be controlled, communicate with devices. So, SCADA systems are essential for industrial organizations because these systems include hardware & software. So, SCADA security is also essential in industries.

The term SCADA security is used to protect the SCADA networks which are fabricated with computer hardware. SCADA networks used by some of the systems are [electricity](https://www.elprocus.com/using-double-fed-induction-generator/), natural gas, etc. The private and government organizations have taken the measures of these networks because of the valuable role to make sure the security of the SCADA systems.

**Examples of SCADA Security**

The threats that occur in SCADA systems include the following.

* Hackers
* Terrorists
* Malware
* Error Inside

The weakness of SCADA security mainly occurs because of the following reasons.

* Poor Training
* Loopholes in Development of App
* Issues while Monitoring
* Less Maintenance

The SCADA system can be protected by mapping all present systems, monitoring, and detecting the institute, and create processes for the security of the network.

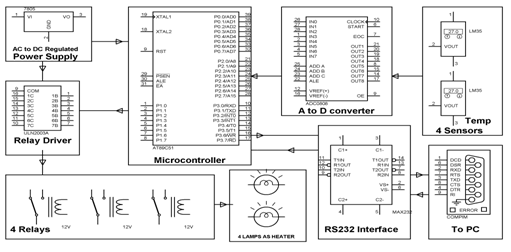
**Difference between PLC and SCADA**

The difference between PLC and SCADA includes 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. |

**SCADA for Remote Industrial Plant**

In large industrial establishments, many processes occur simultaneously and each needs to be monitored, which is a complex task. The SCADA systems are used to monitor and control the equipment in the industrial processes which include water distribution, oil distribution, and power distribution. The main aim of this project is to process the real-time data and control the large scale remote industrial environment. In the real-time scenario, a temperature logging system for a remote plant operation is taken.



Block Diagram of Temperature Control Industrial Plant

The temperature sensors are connected to the microcontroller, which is connected to the PC at the front end, and software is loaded on the computer. The data is collected from the temperature sensors. The temperature sensors continuously send the signal to the microcontroller which accordingly displays these values on its front panel.

One can set the parameters like low limit and high limit on the computer screen. When the temperature of a sensor goes above-set point the microcontroller sends a command to the corresponding relay. The heaters connected through relay contacts are turned OFF and ON.

This is a temperature logging system. Here 8 temperature sensors in multiplexing mode are connected to the microcontroller through ADC 0808. Then the values of all the sensors are sent serially by the microcontroller through Max 32 to the com port of the PC. A Software “DAQ System” loaded on the PC takes these values and show them on its front panel, and also logs them to the database “daq.mdb”.

One can set by the interactive way some parameters like a set point, low limit, and high limit on the computer screen. When the temperature of some sensor increases beyond the setpoint, the microcontroller sends commands to relay driver IC. The heaters connected through relay contacts are (specific for that sensor) turned OFF (or ON in opposite case). High limit and low limits are for alarm. When the temperature goes above the high limit or below the low limit the alarm will be turned on.



SCADA for Remote Industrial Plant