# Study of Wireless Sensor Network in SCADA System for Power Plant

**U. S. Patil**

Electrical Engineering Dept., Govt. College of Engineering, Karad, Maharashtra, India
E-mail : umapatil15@gmail.com

***Abstract*** **-** In this paper, study of wireless SCADA system which is powerful setup for monitoring and controlling the various applications from remotely placed is presented. All communication between GSM modem and user are wireless based, this translates into lowest cost compared to all other systems. Wireless based solutions have universally accepted, familiar and user friendly system. Real-time logging would allow warnings to be flagged to the relevant personnel (e.g. an SMS warning message to the supervisors) and allow corrective action to be taken before the quality and value of the catch is degraded.

***Keywords*** **-** *SCADA system, GSM modem, Protection and automation.*

## I. INTRODUCTION

SCADA stands for supervisory control and data acquisition. It generally refers to an industrial control system: a computer system monitoring and controlling a process. The process can be industrial, infrastructure or facility-based as described below:

- Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defense siren systems, and large communication systems.
- Facility processes occur both in public facilities and private ones.

### *A. Common system components*

A SCADA System usually consists of the following subsystems:

- A Human-Machine Interface or HMI is the apparatus which presents process data to a human operator, and through this, the human operator monitors and controls the process.
- A supervisory (computer) system, gathering (acquiring) data on the process and sending commands (control) to the process. Remote Terminal Units (RTUs) connecting to sensors in the process, converting sensor signals to digital data and sending digital data to the supervisory system.
- Programmable Logic Controller (PLCs) used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.
- Communication infrastructure connecting the supervisory system to the Remote Terminal Units.

## II. SYSTEM CONCEPT

The term SCADA usually refers to centralized systems which monitors and controls entire sites, or complexes of systems spread out over large areas (anything between an industrial plant and a country). Most control actions are performed automatically by Remote Terminal Units (RTUs) or by Programmable Logic Controllers (PLCs). Host control functions are usually restricted to basic overriding or supervisory level intervention. For example, a PLC may control the flow of cooling water through part of an industrial process, but the SCADA system may allow operators to change the set points for the flow, and enable alarm conditions, such as loss of flow and high temperature, to be displayed and recorded. The feedback control loop

passes through the RTU or PLC, while the SCADA system monitors the overall performance of the loop [1].

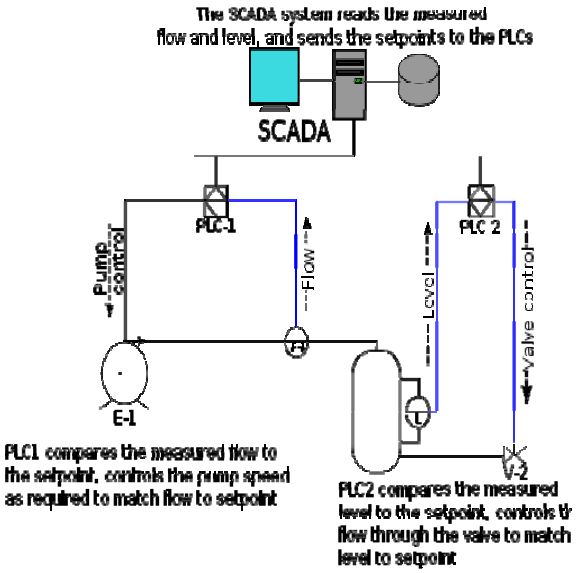


Fig. 1 : Representation of SCADA system

Data acquisition begins at the RTU or PLC level and includes meter readings and equipment status reports that are communicated to SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the HMI can make supervisory decisions to adjust or override normal RTU (PLC) controls. Data may also be fed to a Historian, often built on a commodity Database Management System, to allow trending and other analytical auditing.

SCADA systems typically implement a distributed database, commonly referred to as a tag database, which contains data elements called tags or points. A point represents a single input or output value monitored or controlled by the system. Points can be either 'hard' or 'soft'. A hard point represents an actual input or output within the system, while a soft point results from logic and math operations applied to other points. (Most implementations conceptually remove the distinction by making every property a 'soft' point expression, which may, in the simplest case, equal a single hard point.) Points are normally stored as value-timestamp pairs: a value, and the timestamp when it was recorded or calculated. A series of value-time stamp pairs gives the history of that point. It's also common to store additional metadata with tags, such as the path to a field device or PLC register, design time comments, and alarm information [2].

*A. GSM modem*

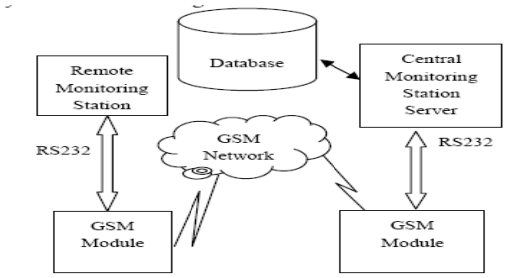


Fig. 2 : Block diagram of GSM Network.

GSM is a digital mobile communication network which develops rapidly in recent years. Short message service of GSM is a value-added service based on data packet switching provided by mobile communication company using GSM network besides of all sorts of telecommunication services and bearer services based on the circuit-switched [2]. Because the GSM network can be interconnected and roamed all over the country, it has strong network ability, the users has no need to organize another network. The coverage of the network is improved and the expensive network building and maintenance cost can be saved for users [3]. At the same time, the number of its users is not limited. Wireless communication of using GSM has some features such as two-way data transmission function, stable performance and so on. GSM network provides a strong platform for remote data transmission and monitoring the communication of equipment, ant it is an important method of wireless remote monitoring system.

The paper uses SMS as a method of information transmission, the collected data of the remote monitoring station is transmitted to the central monitoring station by means of the SMS through the GSM network. The central station analyzes the data and sends the controlling orders to the remote stations in the same way. Thus the remote monitoring function between the monitoring central station and the remote monitoring station is realized.

*B. Working of the model*

The main object of our project is to monitor and control the parameters such as voltage, current, temperature, power factor, frequency. By using SCADA system we supervise the data and then by processing on it we can control the parameters as shown in Fig.3.

The whole assembly is differentiated in

1. Power supply circuit
2. C.T. and P.T and temperature sensors
3. ADC

4. Microcontroller
5. GSM modem
6. Relay

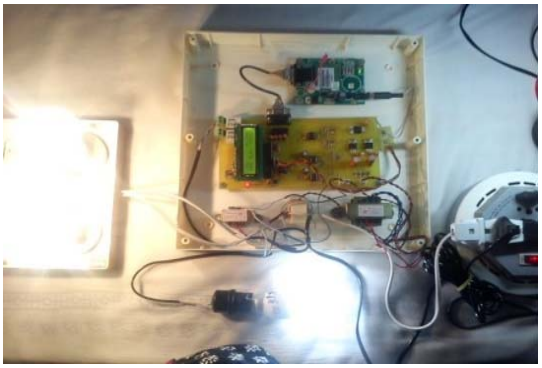

Fig. 3 : Representation of SCADA system

1. Power Supply Circuit:

It mainly consists of step down transformer 100:1 with bridge rectifier, voltage regulator, and filter.

Voltage regulator-

- 7805 for 5V
- 7812 for 12V
- 7912 for -12V

Regulated 5V supply is given to various parts of circuit like ZCD, ADC, MAX232, µC 8052, LCD. Regulated 12V supply is given to LM358, ULN Driver 2803.

The 230V supply is stepped down to 23V by 100:1 transformer. Then it is rectified by the bridge rectifier circuit and regulated to 5V, +12V and -12V by the voltage regulators. It is then filtered by capacitor filter.

2. C.T. and P.T.:

These are used for acquisition of current and voltage. The conversion ratio is 100:1. The LM358 is used as sensors. Two resistive loads of 100W are used. PT is connected across the load in parallel. CT is connected in series with load. Current and voltage values which are to be processed are stepped down and sensed using LM358 and given to ADC.

3. Zero Crossing Detectors (ZCD):

To measure frequency and power factor ZCD circuit is used. It consists of LM358. CT, PT connections are connected to ZCD circuit. The no of zero crossings of current wave in 1 second is known as frequency. The power factor is calculated by the delay angle between voltage and current waves.ZCD circuit needs +5V supply. For continuous supply of current wave resistive load of 100W is used. So that we can get power factor at no load.

4. TCN75

TCN75 is two wire temperature sensors. It has inbuilt transducer and ADC. Hence directly connected to microcontroller. It sense ambient temperature of surrounding and feeds to microcontroller.

5. ADC

MCP 3202 is used as analog to digital convertor. It requires regulated 5V supply. Its output code is

O/P Code=4096 $V_{in}/V_{DD}$

Where $V_{DD}$ =5V and $V_{in}$=I/P voltage

It converts the analog voltage and analog current values into digital. Sampling period is 1.5 clock cycles. Microcontroller senses only digital signal. Hence all analog values are converted into digital values.

ADC is interfaced to microcontroller using CS, CLK, $D_{out}$, $D_{in}$ pins. Digital data is serially transmitted to microcontroller.

6. Micro Controller (89C52):

ADC is interfaced to pin4, pin5, pin7. Two interrupts are used. INT0 is used for voltage zero during zero crossing to pin12. INT1 is used for current zero during zero crossing to pin13. +5V supply is given to pin40.Crystal oscillator is connected to pin18, pin19. Pin20 is grounded. Pin22 and pin 23 are connected to relay. Pins 26, 27, 28 and pins 31 to 39 are used to interface with LCD.

7. Relay

We used two relays overvoltage and over current relays. Microcontroller gives trip signal through pin22. LED's are connected across each relay to indicate which relay has been tripped. We used SPDT relay of 12V. Over current relay will trip at 0.66 ampere. Relays are not connected directly to microcontroller but through ULN Driver 2803 to boost the voltage level.

One link is provided from relay to phase wire of current coil in series. When relay will trip it interrupts circuit through disconnecting the current transformer.

8. ULN Driver:

The eight NPN Darlington connected transistors in this family of arrays are ideally suited for interfacing between low logic level digital circuitry (such as TTL, CMOS or PMOS/NMOS) and the higher current/voltage requirements of lamps, relays, printer hammers or other similar loads for a broad range of computer, industrial, and consumer applications. All devices feature are open–

collector outputs and free wheeling clamp diodes for transient suppression.

9. GSM Modem:

Frequency band of GSM Modem is 900-1800MHz. I2C protocol. TTL is interface to RS232 by MAX232 dual driver and receiver. When trip signal is given to relay by microcontroller it will send the sms on entered destination no. and disconnect the load from the mains.

10. LCD:

16x2 LCD Display is used. All parameters are being continuously monitored and displayed on LCD screen. When fault is detected respective parameters are displayed with '*' and trip signal is sent to relay.

## III. CONCLUSION AND FUTURE SCOPE

Our objective to work on the "wireless sensor network in SCADA system for power plant" to achieve this real-time logging would allow warnings to be flagged to the relevant personnel (e.g. an SMS warning message to the supervisors) and allow corrective action to be taken before the quality and value of the catch is degraded. With the proposed setup Voltage, Current, temperature, Frequency, Power factor was successfully monitored remote location and it was measured to be around 230V,0.66A,30$^{o}$C,50Hz,unity Hence the wireless SCADA system is powerful setup for monitoring and controlling the various applications from remotely placed location.

All communication between GSM modem and user are wireless based, this translates into lowest cost compared to all others system. In this project all the database is stored in controller; user has global access to consolidate data from many system or locations.

There is a trend for PLC and HMI/SCADA software to be more 'mix-and-match'. In the mid 1990s, the typical DAQ I/O manufacturer supplied equipment that communicated using proprietary protocols over a suitable-distance carrier like RS-485.Open architecture SCADA systems enabled users to mix-and-match products from different vendors to develop solutions that were better than those that could be achieved when restricted to a single vendor's product offering.

SCADA systems provide this sequence of events recorder function, using Radio clocks to synchronize the RTU or distributed RTU clocks.

SCADA systems are coming in line with standard networking technologies. Ethernet and TCP/IP based protocols are replacing the older proprietary standards. Ethernet in a few specialized applications, the vast majority of markets have accepted Ethernet networks for HMI/SCADA.

With the emergence of software as a service in the broader software industry, a few vendors have begun offering application specific SCADA systems hosted on remote platforms over the Internet. SCADA systems are becoming increasingly ubiquitous. Thin clients, web portals, and web based products are gaining popularity with most major vendors. SCADA systems have understood the changes in accessibility and threat scope implicit in connecting a system to the Internet.

## IV. ACKNOWLEDGMENT

I wish to thank Electrical Engg.Dept.Govt.College Of Engg.Karad and Pawar S.L., Choudhari V.K., Bhosale V.K., Bansode S.G. and Pimpalgaonkar P.B.

## REFERENCES

[1] Sungmo Jung, Jae-gu Song, Seoksoo Kim, "Design on SCADA Test-bed and Security Device," International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 4, October, 2008.

[2] Sandip C.Patel, Pritimoy Sanyal " Securing SCADA System" Information Management & Computer Security Journal Volume: 16 Issue: 4 Page: 398 – 414 Year: 2008.

[3] Gumbo, S, Muyingi, H, "Development of a web based interface for remote monitoring of a Long-distance power transmission overhead line", SATNAC 2007, Sugar Beach Resort, Mauritius, ISBN 978 0 620 39351 5.

[4] McClanahan, R.H.," The Benefits of Networked SCADA Systems Utilizing IP Enabled Networks", Proc. Of IEEE Rural Electric Power Conference 5-7 May 2002 Pages: C5 - C5_7.

[5] Dagle, J.E.; Widergren, S.E.; Johnson, J.M." Enhancing the security of supervisory control and data acquisition (SCADA) systems: the lifeblood of modern energy infrastructures" Power Engineering Society Winter Meeting, 2002. IEEE Volume 1, Issue , 2002 Page(s): 635 vol.1.

[6] J.E. Dagle (SM), S.E. Widergren (SM), and J.M. Johnson (M)" Enhancing the Security of Supervisory Control and Data Acquisition (SCADA) Systems: The Lifeblood of Modern Energy Infrastructures" Power Engineering Society Winter Meeting, 2002. IEEE Volume 1, Issue, 2002 Page(s): 635 vol.1.

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Dr. Aditya Goel & Ravi Shankar Mishra International Journal of Engineering (IJE), Volume (3) : Issue (1) 65 Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002; receives the IEEE Communications Society 2003 Best Tutorial Paper Award, April 2003.