# Remote Data Acquisition Using Wireless - Scada System

**Dr. Aditya Goel** adityagoel2@rediffmail.com
*Department of Electronics And Communication Engineering M.A.N.I.T.(Deemed University), Bhopal, India – 462051*

**Ravi Shankar Mishra** ravishankarmishra@rediffmail.com
*Department of Electronics And Communication Engineering M.A.N.I.T.(Deemed University), Bhopal, India – 462051*

**ABSTRACT**

In this paper we have developed an integrated wireless SCADA system for monitoring & accessing the performance of remotely situated device parameter such as temperature, pressure, humidity on real time basis. For this we have used the infrastructure of the existing mobile network, which is based on GPRS technique Supervisory Control and Data Acquisition (SCADA) is a field of constant development and research. This project investigates on creating an extremely low cost device which can be adapted to many different SCADA applications via some very basic programming, and plugging in the relevant peripherals. Much of the price in some expensive SCADA applications is a result of using specialized communication infrastructure. The application of infrastructure, in the proposed scheme the cost will come down. Additionally the generic nature of the device will be assured.

Wireless SCADA deals with the creation of an inexpensive, yet adaptable and easy to use SCADA device and infrastructure using the mobile telephone network, in particular, the General Packet Radio Service (GPRS). The hardware components making up the device are relatively unsophisticated, yet the custom written software makes it re-programmable over the air, and able to provide a given SCADA application with the ability to send and receive control and data signals at any non predetermined time.

GPRS is a packet-based radio service that enables “always on” connections, eliminating repetitive and time-consuming dial-up connections. It will also provide real throughput in excess of 40 Kbps, about the same speed as an excellent landline analog modem connection.

From the wireless SCADA system which is proposed in setup the temperature of around 30$^{o}$C could be sufficiently recorded from remote location. In the similar manner reading of electric energy meter could be read 223 Kilo Watt Hour (KWH) or 223 Unit.

The properly designed SCADA system saves time and money by eliminating the need of service personal to visit each site for inspection, data collection /logging or make adjustments.

**Keywords:** Remote monitoring system, SCADA, SMS, GPRS, Sensors, Microcontroller.

# 1. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) is a process control system that enables a site operator to monitor and control processes that are distributed among various remote sites. A properly designed SCADA system saves time and money by eliminating the need for service personnel to visit each site for inspection, data collection/logging or make adjustments.

Supervisory Control and Data Acquisition systems are computers, controllers, instruments; actuators, networks, and interfaces that manage the control of automated industrial processes and allow analysis of those systems through data collection .They are used in all types of industries, from electrical distribution systems, to food processing, to facility security alarms.[7]

Supervisory control and data acquisition is used to describe a system where both data acquisition and supervisory control are performed. Mobile Supervisory Control and Data Acquisition (referred to as Mobile SCADA) is the use of SCADA with the mobile phone network being used as the underlying communication medium. GSM is a wireless communication technology; most popular today for transmitting data anywhere in the world through SMS with the help of mobile phones.[1],[5]
General Packet Radio Service (GPRS) is chosen as the specific mobile communication protocol to use as it provides an always on-line Inter connection without any time based charges. SMS is a globally accepted wireless service that enables the transmission of alphanumeric messages between mobile subscribers and external systems such as electronic mail, paging, and voice-mail systems. It is a store and forward way of transmitting messages to and from mobiles.[16]

SMS benefits includes the delivery of notifications and alerts, guaranteed message delivery, reliable and low-cost communication mechanism for concise information, ability to screen messages and return calls in a selective way and increased subscriber productivity[5].

## 1.1 Components of the SCADA system

SCADA systems typically are made of four components:
**Master Unit -** This is heart of the system and is centrally located under the operator's control.
**Remote Unit -** This unit is installed from where the process is actually monitored. It gathers required data about the process and sends it to the master unit.
**Communication Mode -** This unit transmits signals/data between the master unit and the remote unit. Communication mode can be a cable, wireless media, satellite etc.
**Software -** The software is an interface between the operator and the units. It allows the operator to visualize and control the functions of the process.9

The implementation Scheme is proposed in FIGURE 1, FIGURE 2, and FIGURE 3

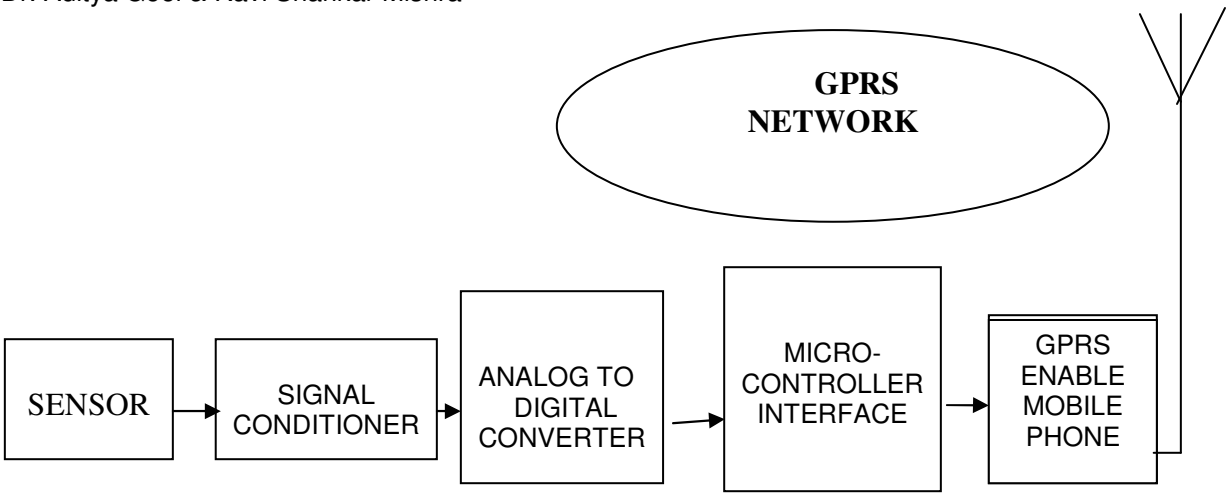



**FIGURE 1:** Block diagram of wireless SCADA

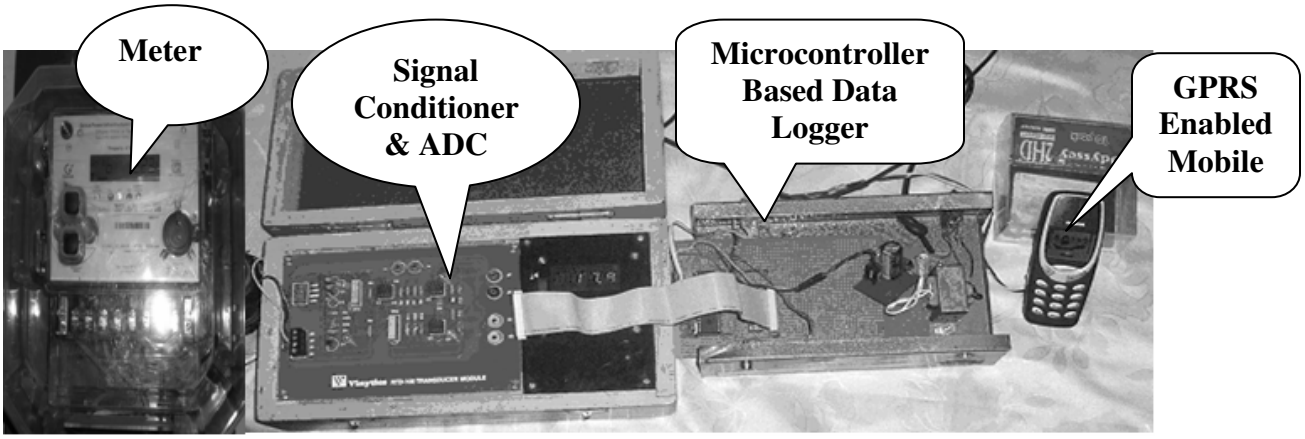



**FIGURE 2:** Complete Setup of Wireless SCADA system for meter reading

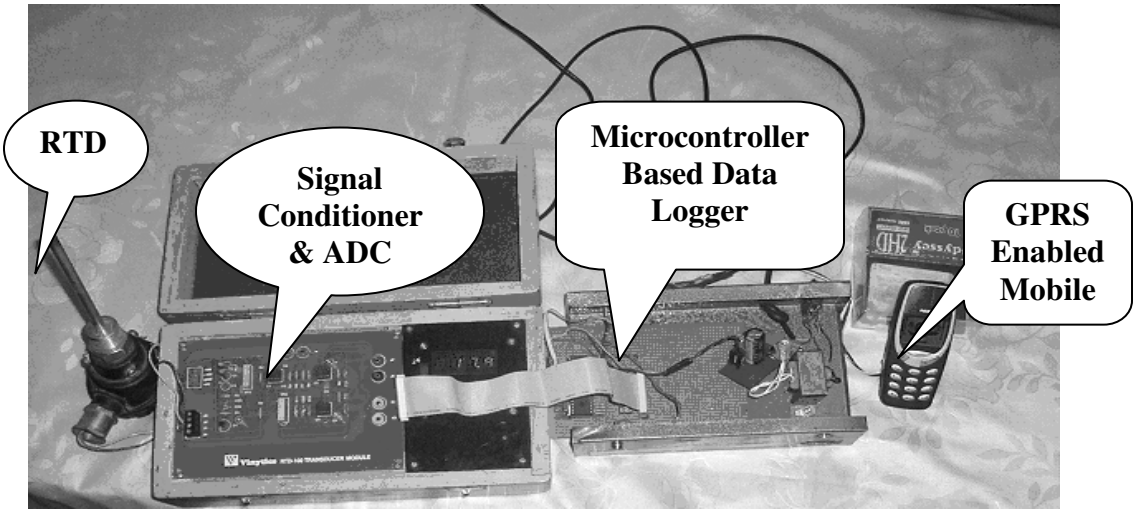



**FIGURE 3:** Complete Setup of Wireless SCADA system for temperature reading

### 1.2 SENSOR: RTD Basics

1. Resistance temperature detectors (RTDs) are made of coils or films of metals (usually platinum). When heated, the resistance of the metal increases; when cooled, the resistance decreases.
3. Resistance varies with Temperature
4. Platinum 100 Ohm at 0°C
5. Very accurate
6. Very stable

#### 1.2.1 Characterstic of RTD

$R = R_0(1+\alpha T_0)$
Where $R_0$ = Resistance at $0^0$
$\alpha$ = Temperature coefficient of resistance
$T_0$ = Temperature in Degree Centigrade

### 1.3 Energy meter Calculation

An electric meter or energy meter is a device that measures the amount of electrical energy supplied to or produced by a residence, business or machine. The most common unit of measurement on the electricity meter is the kilowatt hour, which is equal to the amount of energy used by a load of one kilowatt over a period of one hour, or 3,600,000 joules. general, energy (E) is equivalent to power (P) multiplied by time (t). To determine E in kilowatt-hours, P must be expressed in kilowatts and t must be expressed in hours.[8]

$$E = Pt$$

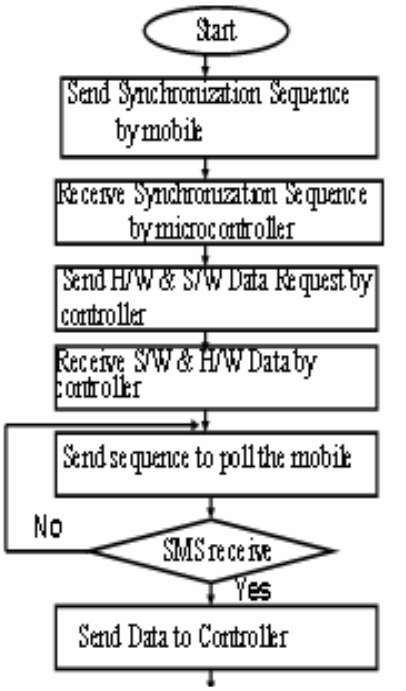
If *P* and *t* are not specified in kilowatts and hours respectively, then they must be converted to those units before determining *E* in kilowatt-hours

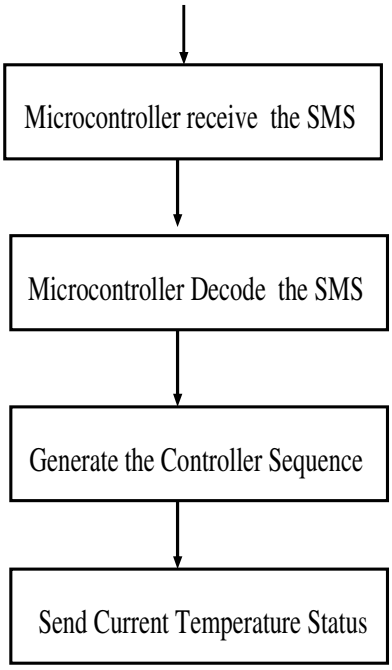
## 2. IMPLEMENTATION

The proposed implementation the system that solves the problem of continuous monitoring of data acquisition system with the help of cheap wireless communication.[12],[14]

The basic components of remote monitoring system designed in this paper include sensors, Signal conditioning device, AT90S8515 microcontroller, and mobile phone. The sensors i.e. RTD is used to measure remote area temperature or energy meter reading. The microcontroller based data logger is fully depends on what is being measured. The AT90S8515 is a low-power, high-performance CMOS 8-bit microcontroller with 8K bytes of in-system programmable Flash memory. The microcontroller is to be programmed using C language.[11]
For Wireless communication. I have used GSM mobile with GPRS services. In this project NOKIA 3310 hand set is used for GSM communication. Most NOKIA phones have F-Bus connection that can be used to connect a phone to microcontroller. This bus will allow us to send and receive SMS messages [4].

### 2.1 Flow chart for wireless SCADA




**2.2 Frame Format**

**Total Frame -98 byte (0-97)**

**F-Bus Frame Header (6 Byte)**

Byte 0: F-Bus Frame ID (0x1E).
Byte 1: Destination address (0x00)
Byte 2: Source addresses (0x0C).
Byte 3: Message Type 0x02 (SMS Handling).
Byte 4 & 5: Message length.

**SMS Frame Header (18 Byte)**

Byte 6 to 8: Start of SMS Frame Header (0x00, 0x01, 0x00)
Byte 9 to 11: Send SMS Message (0x01, 0x02, 0x00)
Byte 12: SMS Centre number length. 0x0a is 10 bytes long.
Byte 13: SMSC number type(0x81-unknown0x91-national
Byte 14 to 23: SMS Centre phone number

**(TPDU) Transfer Protocol Data Unit (5 Byte)**

Byte 24: Message Type (1-sms submit, 0-sms deliver)
Byte 25: Message Reference if SMS Deliver & Validity Indicator used
Byte 26: Protocol ID. (0x00)
Byte 27: Data Coding Scheme.
Byte 28: Message Size is 0x22 in hex or 34 bytes long in decimal.
This is the size of the unpacked message.

**Destination's Phone Number (12 Bytes)**

Byte 29: Destination's number length.
Byte 30: Number type 0x91-international, 0xa1-national
Byte 31 to 40: (Octet format) Destination's Phone Number

**Validity Period (7 Byte)**

Byte 41: Validity-Period Code. (0xFF)
Byte 42 to 47: Service Centre Time Stamp (0x00…. 0x00)

**The SMS Message (SMS-SUBMIT) (45 Byte)**

Byte 48 to 92: SMS message packed into 7 bit characters.
Byte 93: Always 0x00

**The F-Bus Frame ending (4 Byte)**

Byte 94: Packet Sequence Number
Byte 95: Padding Byte - String is old and require to be even
Byte 96 & 97: Odd & even checksum bytes.

## 3. RESULT AND DISCUSSION

| Synchronizing...S==40 CE=21 CO=f4 |
|---|
| S==41 CE=20 CO=f4 |
| S==42 CE=23 CO=f4 |
| S==43 CE=22 CO=f4 |
| S==44 CE=25 CO=f4 |
| S==45 CE=24 CO=f4 |
| S==46 CE=27 CO=f4 |
| S==47 CE=26 CO=f4 |

**TABLE 1:** Synchronization Pattern for temperature

| Printing... |
|---|
| Current temperature status is 20 deg |
| S==46 CE=13 CO=44 |
| S==47 CE=52 CO=d5 |
| Printing... |
| Current temperature status is 30 deg |

**TABLE 2:** Temperatures Status on PC

| Synchronizing...S==40 CE=21 CO=f4 |
|---|
| S==41 CE=20 CO=f4 |
| S==42 CE=23 CO=f4 |
| S==43 CE=22 CO=f4 |
| S==44 CE=25 CO=f4 |
| S==45 CE=24 CO=f4 |
| S==46 CE=27 CO=f4 |
| S==47 CE=26 CO=f4 |

**TABLE 3:** Synchronization Pattern Energy meter

| Printing... |
|---|
| Current meter reading is 223 KWH |
| S==42 CE=13 CO=42 |
| S==43 CE=52 CO=e5 |
| Printing... |
| Current meter reading is 224 KWH |

**TABLE 4:** Energy meter Status on PC

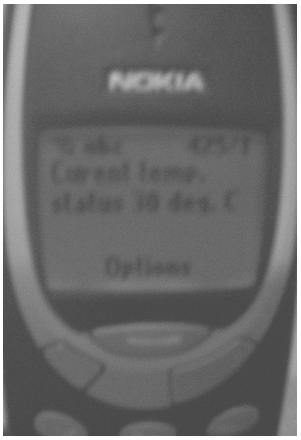



**FIGURE 5:** Temperature Status on Mobile

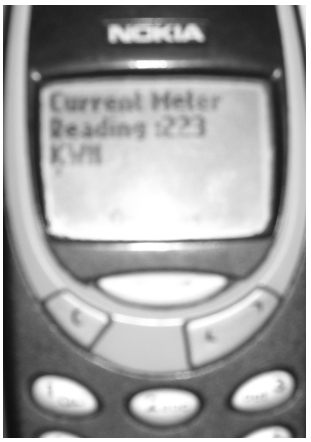



**FIGURE 6:** Energy meter reading on Mobile

The F-Bus cable is High-speed full duplex bus. It uses one pin for transmitting data and one pin for receiving data plus one ground pin. The F-Bus is bidirectional serial type bus running at 115,200bps,8 data bits, no parity and one stop bits. For synchronizing UART in the phone with micro controller, string of 0x55 or 'U' was send 128 times. The NOKIA Protocol has a series of commands that allow the user to make calls, send and get SMS. The NOKIA frame consists information about source address, destination address and message length. In NOKIA Frame format the SMS message packed into 7 bit characters. The last byte in the data segment is sequence number. The last 3 bits of these bytes increments from 0 to 7 for each frame. This part is used as acknowledgement frame.4

The synchronizing frame sent to synchronize the mobile and controller. After sending synchronizing frame that is 128 times "U" or 0x55, PC shows the seven sequence number from S=40 to S= 47 on which message should receive. After receiving the request message, the 58 byte frame format is formed in that format last 3rd and 4th byte is used as CRC check byte .The CE and CO is the even and odd CRC check bits which is decided by length of the message. TABLE 1 and TABLE 3 shows the results of synchronization pattern display on PC with the F-bus cable of temperature monitoring and meter reading. TABLE 2 and TABLE 4 show the temperature and energy status on PC and the FIGURE 5 and FIGURE 6 shows the current temperature and energy status on mobile phone.4

## 4. CONCLUSION AND FUTURE SCOPE

Our objective is to work on the "Remote site Safety & security Application by using Controller" to achieve to produce an input data file for each of the Data Logger, build a Controller Area network ,Collect & manage data in the Control Area Network(CAN) and Send SMS to a monitoring centered .

GSM communication performed almost flawlessly data transfer from sensor at remote area was executed Without incidents. Since all communication between data logger and user are wireless based, this translates into lowest cost compared to all others system. In this project all the database is stored in a central database in the data logger; user has global access to consolidate data from many system or locations.

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.

With the proposed setup in Figure 3 temperature was successfully monitored remote location and it was measured to be around 30$^{o}$C. Similarly energy meter reading from remote location was also successfully implemented using demonstrated hardware setup of wireless SCADA system. The recorded energy meter reading as demonstrated in Figure2 is 223 KWH. Hence the wireless SCADA system is powerful setup for monitoring and controlling the various applications from remotely placed location. It can be further extended for various area of application like health monitoring system, Home security system, Vehicle Security system etc.

## 5. 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. http://www.embedtronics.com. online details of frame format of NOKIA

5. Surve, V, 2006, *"A wireless Communication Device for Short Messages",* Masters Thesis, Available: www.certec.lth.se/doc/awireless.pdf.

6. Das, AN, Lewis, FL, Popa, DO, 2006, *"Data-logging and Supervisory Control in Wireless Sensor Networks,"* Proceeding of the Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, networking, and Parallel/Distributed Computing (SNPD'06), Volume 00, ISBN:0-7695-2611-X, pp 330- 338

7. Hildick-Smith, Andrew, *"Security for Critical Infrastructure SCADA Systems,"* (SANS Reading Room, GSEC Practical Assignment, Version 1.4c, Option 1, February 2005), http://www.sans.org/reading_room/whitepapers/warfare/1644.php

8. Carlson, Rolf E. and Jeffrey E. Dagle, Shabbir A. Shamsuddin, Robert P. Evans, *"A Summary of Control System Security Standards Activities in the Energy Sector,"* Department of Energy Office of Electricity Delivery and Energy Reliability,66 National SCADA Test Bed, October 2005, http://www.sandia.gov/scada/documents/CISSWG_Report_1_Final.pdf

9. Technical Information Bulletin 04-1, Supervisory Control and Data Acquisition (SCADA) Systems, NCS TIB 04-1, Oct. 2004

10. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, *"A Survey on Sensor Networks,"* IEEE

Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002; receives the IEEE Communications Society 2003 Best Tutorial Paper Award, April 2003.

11. Bement, Arden "*Keynote Address at the NSF Workshop on Critical Infrastructure Protection for SCADA & IT,"* October 20, 2003, http://www.nist.gov/speeches/bement_102003.htm .

12. 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

13. 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

14. 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

15. Stephen Beasley, Mr Choon Ng Dr Dario Toncich and Dr Andrew Dennison *"Remote Diagnostics for Data Acquisition Systems"* white paper by Industrial Research Institute Swinburne Available online at www.swinburne.edu.au/feis/iris/pdf/profiles/**StephenBeasley**.pdf

16. Taylor, K; *"Mobile Monitoring and Control Infrastructure",* CSIRO Available online at http://mobile.act.cmis.csiro.au