

Design and Development of Wireless RTU and Cyber security Framework for SCADA System

Ch. Hemasri

M.Tech Student,

Loyola Institute of Technology and Management.

D.Rakesh

Guide,

Loyola Institute of Technology and Management.

Abstract:

The wave adoption of wireless over wire-line is a global phenomenon and the Oil & Gas industry is no exception. This paper presents a multi-tiered secure hardened Wireless Remote Terminal Unit (WRTU) for SCADA systems. The WRTU is based on ARM7 Processor supported by GSM & Satellite modems, GPS, Wi-Fi and Ethernet. WRTU can be interfaced to an array of standard industrial sensors and actuators. WRTU has data acquisition, monitoring, and control capabilities. WRTU is an inexpensive device, using Commercial off-the-shelf (COTS) modules. WRTU is an easy to deploy (using existing public available infrastructure) device and 'single device that does it all'. WRTU connects to the Control and Monitoring Centre (CMC) via GSM or Satellite modem.

The CMC monitors and controls all peripherals of the WRTU, maintains a log of alerts, sensors information, set critical limits and provides geo-location of all WRTUs via its GIS portal. That we can gather from the sensors security. The CMC has a database to maintain all operational centric data, for report generation, historical analysis and forecasting. Here in this project we are going to interfacing the modules for the communication purpose GSM and GPS for the getting info of the particular place or location. Which the data.

I. INTRODUCTION (HEADING 1):

This template, modified in MS Word 2007 and saved as a "Word 97-2003 Document" for the PC, provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings.

Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

II.EASE OF USE:

An embedded system is a system which is going to do a predefined specified task is the embedded system and is even defined as combination of both software and hardware. A general-purpose definition of embedded systems is that they are devices used to control, monitor or assist the operation of equipment, machinery or plant. "Embedded" reflects the fact that they are an integral part of the system.

At the other extreme a general-purpose computer may be used to control the operation of a large complex processing plant, and its presence will be obvious. All embedded systems are including computers or microprocessors. Some of these computers are however very simple systems as compared with a personal computer. The very simplest embedded systems are capable of performing only a single function or set of functions to meet a single predetermined purpose. In more complex systems an application program that enables the embedded system to be used for a particular purpose in a specific application determines the functioning of the embedded system.

The ability to have programs means that the same embedded system can be used for a variety of different purposes. In some cases a microprocessor may be designed in such a way that application software for a particular purpose can be added to the basic software in a second process, after which it is not possible to make further changes. The applications software on such processors is sometimes referred to as firmware.

ARM PROCESSOR OVERVIEW:

ARM stands for Advanced RISC Machines. It is a 32 bit processor core, used for high end application. It is widely used in Advanced Robotic Applications.



History and Development:

- ARM was developed at Acron Computers Ltd of Cambridge, England between 1983 and 1985.
- RISC concept was introduced in 1980 at Stanford and Berkley. ARM Ltd was found in 1990.
- ARM cores are licensed to partners so as to develop and fabricate new microcontrollers around same processor cores.

Key features:

- 1.16-bit/32-bit ARM7TDMI-S microcontroller in a tiny LQFP64 package.
2. 8 kB to 40 kB of on-chip static RAM and 32 kB to 512 kB of on-chip flash memory.
- 128-bit wide interface/accelerator enables high-speed 60 MHz operation.
3. In-System Programming/In-Application Programming (ISP/IAP) via on-chip boot loader Software. Single flash sector or full chip erase in 400 ms and programming of 256 bytes in 1 m.

Power Supply:

The input to the circuit is applied from the regulated power supply. The ac. input i.e., 230V from the mains supply is step down by the transformer to 12V and is fed to a rectifier. The output obtained from the rectifier is a pulsating dc voltage. So in order to get a pure dc output voltage from the rectifier is fed to a filter to remove any ac components present even after rectification. Now, this voltage is given to a voltage regulator to obtain a pure constant dc voltage. The abbreviation "i.e." means "that is," and the abbreviation "e.g." means "for example."

Since piezoelectric crystals generate a voltage when force is applied to them, the same crystal can be used as an ultrasonic detector. Some systems use separate transmitter and receiver components while others combine both in a single piezoelectric transceiver. Non-piezoelectric principles are also used in construction of ultrasound transmitters. Magnetostrictive materials slightly change size when exposed to a magnetic field; such materials can be used to make transducers. A capacitor microphone uses a thin plate which moves in response to ultrasound waves; changes in the electric field around the plate convert sound signals to electric currents, which can be amplified.

Electric Motors:

Electric motors are used to efficiently convert electrical energy into mechanical energy. Magnetism is the basis of their principles of operation. They use permanent magnets, electromagnets and exploit the magnetic properties of materials in order to create these amazing machines. There are several types of electric motors available today. The following outline gives an overview of several popular ones. There are two main classes of motors: AC and DC. AC motors require an alternating current or voltage source (like the power coming out of the wall outlets in your house) to make them work. DC motors require a direct current or voltage source (like the voltage coming out of batteries) to make them work. Universal motors can work on either type of power. Not only is the construction of the motors different, but the means used to control the speed and torque created by each of these motors also varies, although the principles of power conversion are common to both.

Motors are used just about everywhere. In our house, there is a motor in the furnace for the blower, for the intake air, in the sump well, dehumidifier, in the kitchen in the exhaust hood above the stove, microwave fan, refrigerator compressor and cooling fan, can opener, garbage disposer, dish washer pump, clocks, computer fans, ceiling fans, and many more items. In industry, motors are used to move, lift, rotate, accelerate, brake, lower and spin material in order to coat, paint, punch, plate, make or form steel, film, paper, tissue, aluminum, plastic and other raw materials. They range in power ratings from less than 1/100 hp to over 100,000 hp. They rotate as slowly as 0.001 rpm to over 100,000 rpm. They range in physical size from as small as the head of a pin to the size of a locomotive engine.

3.7.2 Types of Motors: 1. Split Phase:

The split phase motor is mostly used for “medium starting” applications. It has start and run windings, both are energized when the motor is started. When the motor reaches about 75% of its rated full load speed, the starting winding is disconnected by an automatic switch.

Uses: This motor is used where stops and starts are somewhat frequent. Common applications of split phase motors include: fans, blowers, office machines and tools such as small saws or drill presses where the load is applied after the motor has obtained its operating speed.

2. Capacitor Start:

This motor has a capacitor in series with a starting winding and provides more than double the starting torque with one third less starting current than the split phase motor. Because of this improved starting ability, the capacitor start motor is used for loads which are hard to start. It has good efficiency and requires starting currents of approximately five times full load current. The capacitor and starting windings are disconnected from the circuit by an automatic switch when the motor reaches about 75% of its rated full load speed.

Uses: Common uses include: compressors, pumps, machine tools, air conditioners, conveyors, blowers, fans and other hard to start applications.

A.3.8.2 Specifications:

- » Number and type of contacts – normally open, normally closed, (double-throw)
- » Contact sequence – “Make before Break” or “Break before Make”. For example, the old style telephone exchanges required Make-before-break so that the connection didn’t get dropped while dialing the number.
- » Rating of contacts – small relays switch a few amperes, large contactors are rated for up to 3000 amperes, alternating or direct current
- » Voltage rating of contacts – typical control relays rated 300 VAC or 600 VAC, automotive types to 50 VDC, special high-voltage relays to about 15 000 V
- » Coil voltage – machine-tool relays usually 24 VAC, 120 or 250 VAC, relays for switchgear may have 125 V or 250 VDC coils, “sensitive” relays operate on a few milliamperes.

LIQUID CRYSTAL DISPLAY:

LCD stands for Liquid Crystal Display. LCD is finding wide spread use replacing LEDs (seven segment LEDs or other multi segment LEDs) because of the following reasons:

- 1.The declining prices of LCDs.
- 2.The ability to display numbers, characters and graphics. This is in contrast to LEDs, which are limited to numbers and a few characters.
- 3.Incorporation of a refreshing controller into the LCD, thereby relieving the CPU of the task of refreshing the LCD. In contrast, the LED must be refreshed by the CPU to keep displaying the data.
- 4.Ease of programming for characters and graphics.
- 5.These components are “specialized” for being used with the microcontrollers, which means that they cannot be activated by standard IC circuits. They are used for writing different messages on a miniature LCD.



A model described here is for its low price and great possibilities most frequently used in practice. It is based on the HD44780 microcontroller (Hitachi) and can display messages in two lines with 16 characters each. It displays all the alphabets, Greek letters, punctuation marks, mathematical symbols etc. In addition, it is possible to display symbols that user makes up on its own. Automatic shifting message on display (shift left and right), appearance of the pointer, backlight etc. are considered as useful characteristics.

3.4.1 Pins Functions:

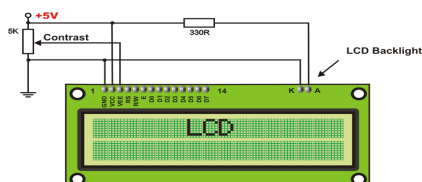
There are pins along one side of the small printed board used for connection to the microcontroller. There are total of 14 pins marked with numbers (16 in case the background light is built in). Their function is described in the table below:

TABLE: 2

Function	Pin Number	Name	Logic State	Description
Ground	1	Vss	-	0V
Power supply	2	Vdd	-	+5V
Contrast	3	Vee	-	0 - Vdd
	4	RS	0 1	D0 - D7 are interpreted as commands D0 - D7 are interpreted as data
Control of operating	5	R/W	0	Write data (from controller to LCD)
			1	Read data (from LCD to controller)
Data commands	6	E	0	Access to LCD disabled
			1	Normal operating
	7-14	D0-D7	From 1 to 0	Data/commands are transferred to LCD
			0/1	Bit 0 LSB
			0/1	Bit 1
			0/1	Bit 2
			0/1	Bit 3
			0/1	Bit 4
0/1	Bit 5			
0/1	Bit 6			
0/1	Bit 7 MSB			

3.4.2 LCD screen:

LCD screen consists of two lines with 16 characters each. Each character consists of 5x7 dot matrix. Contrast on display depends on the power supply voltage and whether messages are displayed in one or two lines. For that reason, variable voltage 0-Vdd is applied on pin marked as Vee. Trimmer potentiometer is usually used for that purpose. Some versions of displays have built in backlight (blue or green diodes). When used during operating, a resistor for current limitation should be used (like with any LE diode).



3.4.3 LCD Basic Commands:

All data transferred to LCD through outputs D0-D7 will be interpreted as commands or as data, which depends on logic state on pin RS: RS = 1 - Bits D0 - D7 are addresses of characters that should be displayed. Built in processor addresses built in "map of characters" and displays corresponding symbols.

Displaying position is determined by DDRAM address. This address is either previously defined or the address of previously transferred character is automatically incremented. To perform time delay functions. Relays can be used to act as a mechanical time delay device by controlling the release time by using the effect of residual magnetism by means of a inserting copper disk between the armature and moving blade assembly.

TEMPERATURE SENSOR

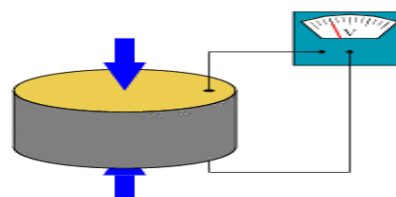
Temperature Sensor which converts temperature value into electrical signals. We used IC called LM 35 as a temperature sensor. LM35 series sensors are precision integrated-circuit temperature sensors whose output voltage is linearly proportional to the Celsius temperature. The LM35 requires no external calibration since it is internally calibrated. . The LM35 does not require any external calibration or trimming to provide typical accuracies of $\pm 1/4^\circ\text{C}$ at room temperature and $\pm 3/4^\circ\text{C}$ over a full -55 to $+150^\circ\text{C}$ temperature range.

The LM35's low output impedance, linear output, and precise inherent calibration make interfacing to readout or control circuitry especially easy. It can be used with single power supplies, or with plus and minus supplies. As it draws only 60 μA from its supply, it has very low self-heating, less than 0.1°C in still air.

2Features

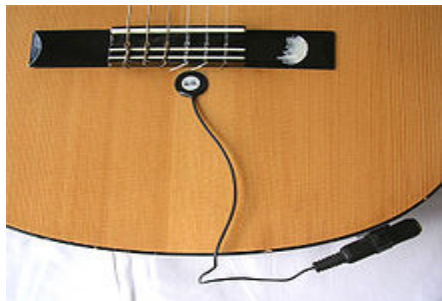
- Calibrated directly in $^\circ\text{Celsius}$ (Centigrade)
- Linear + 10.0 mV/ $^\circ\text{C}$ scale factor
- 0.5 $^\circ\text{C}$ accuracy guaranteed (at +25 $^\circ\text{C}$)
- Rated for full -55 $^\circ\text{C}$ to +150 $^\circ\text{C}$ range
- Suitable for remote applications
- Low cost due to wafer-level trimming.

A piezoelectric sensor is a device that uses the piezoelectric effect to measure pressure, acceleration, strain or force by converting them to an electrical signal.



A piezoelectric disk generates a voltage when deformed

B.Applications:



Piezoelectric disk used as a guitar pickup

» The Piezoelectric sensors have proven to be versatile tools for the measurement of various processes. They are used for quality assurance, process control and for research and development in many different industries.

» In the automotive industry piezoelectric elements are used as the standard devices for engine indicating in developing internal combustion engines. The combustion processes are measured with piezoelectric sensors. The sensors are either directly mounted into additional holes into the cylinder head or the spark/glow plug is equipped with a built in miniature piezoelectric sensor.

» The rise of piezoelectric technology is directly related to a set of inherent advantages. The high modulus of elasticity of many piezoelectric materials is comparable to that of many metals and goes up to 105 N/m². Even though piezoelectric sensors are electromechanical systems that react on compression, the sensing elements show almost zero deflection. This is the reason why piezoelectric sensors are so rugged, have an extremely high natural frequency and an excellent linearity over a wide amplitude range. Additionally, piezoelectric technology is insensitive to electromagnetic fields and radiation, enabling measurements under harsh conditions. Some materials used (especially gallium phosphate or tourmaline) have an extreme stability over temperature enabling sensors to have a working range of up to 1000°C. Tourmaline shows pyroelectricity in addition to the piezoelectric effect; this is the ability to generate an electrical signal when the temperature of the crystal changes. This effect is also common to piezo ceramic materials.

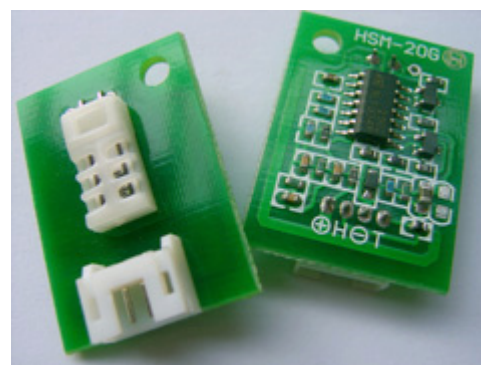
Principle	Strain Sensitivity [V/ μm^2]	Threshold [μm^2]	Span to threshold ratio
Piezoelectric	5.0	0.00001	100,000,000
Piezoresistive	0.0001	0.0001	2,500,000
Inductive	0.001	0.0005	2,000,000
Capacitive	0.005	0.0001	750,000

One disadvantage of piezoelectric sensors is that they cannot be used for true static measurements. A static force will result in a fixed amount of charges on the piezoelectric material. While working with conventional readout electronics, imperfect insulating materials, and reduction in internal sensor resistance will result in a constant loss of electrons, and yield a decreasing signal. Elevated temperatures cause an additional drop in internal resistance and sensitivity. The main effect on the piezoelectric effect is that with increasing pressure loads and temperature the sensitivity is reduced due to twin-formation. While quartz sensors need to be cooled during measurements at temperatures above 300°C special types of crystals like GaPo₄ gallium phosphate do not show any twin formation up to the melting point of the material itself. Anyhow, it would be a misconception that piezoelectric sensors can only be used for very fast processes or at ambient conditions. In fact, there are numerous applications that show quasi-static measurements while there are other applications that go to temperatures far beyond 500°C Piezoelectric sensors are also seen in nature. Dry bone is piezoelectric, and is thought by some to act as a biological force sensor.

C.Principle of operation:

Depending on how a piezoelectric material is cut, three main modes of operation can be distinguished: transverse, longitudinal, and shear.

HUMIDITY SENSORS:

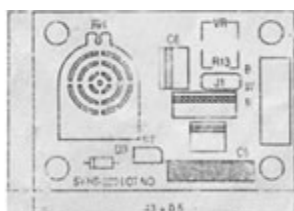
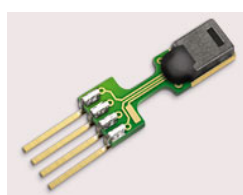


A humidity sensor, also called a hygrometer, measures and regularly reports the relative humidity in the air. They may be used in homes for people with illnesses affected by humidity; as part of home heating, ventilating, and air conditioning (HVAC) systems; and in humidors or wine cellars. Humidity sensors can also be used in cars, office and industrial HVAC systems, and in meteorology stations to report and predict weather.

A humidity sensor senses relative humidity. This means that it measures both air temperature and moisture. Relative humidity, expressed as a percent, is the ratio of actual moisture in the air to the highest amount of moisture air at that temperature can hold. The warmer the air is, the more moisture it can hold, so relative humidity changes with fluctuations in temperature.

The most common type of humidity sensor uses what is called “capacitive measurement.” This system relies on electrical capacitance, or the ability of two nearby electrical conductors to create an electrical field between them. The sensor itself is composed of two metal plates with a non-conductive polymer film between them. The film collects moisture from the air, and the moisture causes minute changes in the voltage between the two plates. The changes in voltage are converted into digital readings showing the amount of moisture in the air.

A person with a respiratory illness or certain allergies might use a home humidity sensor because low humidity can exacerbate breathing problems and cause joint pain, while high humidity encourages bacteria, mold, and fungus growth. Home humidors and wine cellars often have a humidity sensor that helps to maintain a consistent relative humidity optimal to safe long-term storage. Humidity sensors can also be used in homes or museums where valuable antiques or artwork are kept, because these items can be damaged or degraded from constant exposure to too much moisture.



RATED VOLTAGE	DC 5.0V
CURRENT CONSUMPTION	<3.0mA
OPERATING TEMPERATURE RANGE	0-60°C
OPERATING HUMIDITY RANGE	30-90%RH
STORABLE TEMPERATURE RANGE	-

30°C~85°C	
STORABLE HUMIDITY RANGE	within 95%RH
STANDARD OUTPUT RANGE	DC1.980mV (at25°C, 60%RH)
ACCURACY	±5%RH (at 25°C, 60%RH)
REMARKS	PCB unit containing driving circuit

GSM:

GSM (Global System for Mobile communications) is an open, digital cellular technology used for transmitting mobile voice and data services. GSM (Global System for Mobile communication) is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM uses a variation of Time Division Multiple Access (TDMA) and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1,800 MHz frequency band. It supports voice calls and data transfer speeds of up to 9.6 kbit/s, together with the transmission of SMS (Short Message Service).

D.History:

In 1982, the European Conference of Postal and Telecommunications Administrations (CEPT) created the Group Special Mobile (GSM) to develop a standard for a mobile telephone system that could be used across Europe. In 1987, a memorandum of understanding was signed by 13 countries to develop a common cellular telephone system across Europe. Finally the system created by SINTEF lead by Torleiv Maseng was selected. In 1989, GSM responsibility was transferred to the European Telecommunications Standards Institute (ETSI) and phase I of the GSM specifications were published in 1990. The first GSM network was launched in 1991 by in Finland with joint technical infrastructure maintenance from Ericsson. By the end of 1993, over a million subscribers were using GSM phone networks being operated by 70 carriers across 48 countries. As of the end of 1997, GSM service was available in more than 100 countries and has become the de facto standard in Europe and Asia.

E.GSM Frequencies:

GSM networks operate in a number of different frequency ranges (separated into GSM frequency ranges for 2G and UMTS frequency bands for 3G). Most 2G GSM networks operate in the 900 MHz or 1800 MHz bands. Some countries in the Americas (including Canada and the United States) use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated. Most 3G GSM networks in Europe operate in the 2100 MHz frequency band. The rarer 400 and 450 MHz frequency bands are assigned in some countries where these frequencies were previously used for first-generation systems.

GSM-900 uses 890–915 MHz to send information from the mobile station to the base station (uplink) and 935–960 MHz for the other direction (downlink), providing 124 RF channels (channel numbers 1 to 124) spaced at 200 kHz. Duplex spacing of 45 MHz is used. In some countries the GSM-900 band has been extended to cover a larger frequency range. This ‘extended GSM’, E-GSM, uses 880–915 MHz (uplink) and 925–960 MHz (downlink), adding 50 channels (channel numbers 975 to 1023 and 0) to the original GSM-900 band. Time division multiplexing is used to allow eight full-rate or sixteen half-rate speech channels per radio frequency channel. There are eight radio timeslots (giving eight burst periods) grouped into what is called a TDMA frame. Half rate channels use alternate frames in the same timeslot. The channel data rate for all 8 channels is 270.833 Kbit/s, and the frame duration is 4.615 ms.

The transmission power in the handset is limited to a maximum of 2 watts in GSM850/900 and 1 watt in GSM1800/1900. GSM operates in the 900MHz and 1.8GHz bands in Europe and the 1.9GHz and 850MHz bands in the US. The 850MHz band is also used for GSM and 3G in Australia, Canada and many South American countries. By having harmonized spectrum across most of the globe, GSM’s international roaming capability allows users to access the same services when travelling abroad as at home. This gives consumers seamless and same number connectivity in more than 218 countries.

Terrestrial GSM networks now cover more than 80% of the world’s population. GSM satellite roaming has also extended service access to areas where terrestrial coverage is not available.

GLOBAL POSITIONING SYSTEM:

F.Basic concept of GPS:

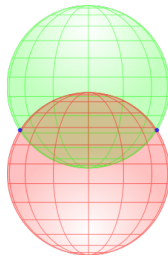
A GPS receiver calculates its position by precisely timing the signals sent by GPS satellites high above the Earth. Each satellite continually transmits messages that include

- the time the message was transmitted
- precise orbital information (the ephemeris)
- The general system health and rough orbits of all GPS satellites (the almanac).

The receiver uses the messages it receives to determine the transit time of each message and computes the distance to each satellite. These distances along with the satellites’ locations are used with the possible aid of trilateration, depending on which algorithm is used, to compute the position of the receiver. This position is then displayed, perhaps with a moving map display or latitude and longitude; elevation information may be included. Many GPS units show derived information such as direction and speed, calculated from position changes.

Three satellites might seem enough to solve for position since space has three dimensions and a position near the Earth’s surface can be assumed. However, even a very small clock error multiplied by the very large speed of light—the speed at which satellite signals propagate—results in a large positional error. Therefore receivers use four or more satellites to solve for the receiver’s location and time. The very accurately computed time is effectively hidden by most GPS applications, which use only the location. A few specialized GPS applications do however use the time; these include time transfer, traffic signal timing, and synchronization of cell phone base stations.

Although four satellites are required for normal operation, fewer apply in special cases. If one variable is already known, a receiver can determine its position using only three satellites. For example, a ship or aircraft may have known elevation. Some GPS receivers may use additional clues or assumptions (such as reusing the last known altitude, dead reckoning, inertial navigation, or including information from the vehicle computer) to give a less accurate (degraded) position when fewer than four satellites are visible.



Position calculation introduction

Surface of sphere intersecting a circle (not a solid disk) at two points

To provide an introductory description of how a GPS receiver works, error effects are deferred to a later section. Using messages received from a minimum of four visible satellites, a GPS receiver is able to determine the times sent and then the satellite positions corresponding to these times sent. The x , y , and z components of position, and the time sent, are designated as $[x_i, y_i, z_i, t_i]$ where the subscript i is the satellite number and has the value 1, 2, 3, or 4. Knowing the indicated time the message was received \bar{t}_r , the GPS receiver could compute the transit time of the message as $(\bar{t}_r - t_i)$, if \bar{t}_r would be equal to correct reception time, t_r .

A pseudo range, $p_i \triangleq (\bar{t}_r - t_i)c$, would be the traveling distance of the message, assuming it traveled at the speed of light, c .

A satellite's position and pseudo range define a sphere, centered on the satellite, with radius equal to the pseudo range. The position of the receiver is somewhere on the surface of this sphere. Thus with four satellites, the indicated position of the GPS receiver is at or near the intersection of the surfaces of four spheres. In the ideal case of no errors, the GPS receiver would be at a precise intersection of the four surfaces.

If the surfaces of two spheres intersect at more than one point, they intersect in a circle. The article trilateration shows this mathematically. A figure, Two Sphere Surfaces Intersecting in a Circle, is shown below. Two points where the surfaces of the spheres intersect are clearly shown in the figure.

The distance between these two points is the diameter of the circle of intersection. The intersection of a third spherical surface with the first two will be its intersection with that circle; in most cases of practical interest, this means they intersect at two points.

ABOUT KEIL SOFTWARE:

It is possible to create the source files in a text editor such as Notepad, run the Compiler on each C source file, specifying a list of controls, run the Assembler on each Assembler source file, specifying another list of controls, run either the Library Manager or Linker (again specifying a list of controls) and finally running the Object-HEX Converter to convert the Linker output file to an Intel Hex File. Once that has been completed the Hex File can be downloaded to the target hardware and debugged. Alternatively KEIL can be used to create source files; automatically compile, link and convert using options set with an easy to use user interface and finally simulate or perform debugging on the hardware with access to C variables and memory. Unless you have to use the tolls on the command line, the choice is clear. KEIL Greatly simplifies the process of creating and testing an embedded application.

4.1.3 Projects:

The user of KEIL centers on "projects". A project is a list of all the source files required to build a single application, all the tool options which specify exactly how to build the application, and – if required – how the application should be simulated. A project contains enough information to take a set of source files and generate exactly the binary code required for the application. Because of the high degree of flexibility required from the tools, there are many options that can be set to configure the tools to operate in a specific manner. It would be tedious to have to set these options up every time the application is being built; therefore they are stored in a project file. Loading the project file into KEIL informs KEIL which source files are required, where they are, and how to configure the tools in the correct way. KEIL can then execute each tool with the correct options. It is also possible to create new projects in KEIL. Source files are added to the project and the tool options are set as required. The project can then be saved to preserve the settings. The project is reloaded and the simulator or debugger started, all the desired windows are opened. KEIL project files have the extension .

4.1.4 Simulator/Debugger:

The simulator/ debugger in KEIL can perform a very detailed simulation of a micro controller along with external signals. It is possible to view the precise execution time of a single assembly instruction, or a single line of C code,

all the way up to the entire application, simply by entering the crystal frequency. A window can be opened for each peripheral on the device, showing the state of the peripheral. This enables quick trouble shooting of miss-configured peripherals. Breakpoints may be set on either assembly instructions or lines of C code, and execution may be stepped through one instruction or C line at a time. The contents of all the memory areas may be viewed along with ability to find specific variables. In addition the registers may be viewed allowing a detailed view of what the microcontroller is doing at any point in time. The Keil Software 8051 development tools listed below are the programs you use to compile your C code, assemble your assembler source files, link your program together, create HEX files, and debug your target program. μ Vision2 for Windows™ Integrated Development Environment: combines Project Management, Source Code Editing, and Program Debugging in one powerful environment.

- » C51 ANSI Optimizing C Cross Compiler: creates relocatable object modules from your C source code,
- » A51 Macro Assembler: creates relocatable object modules from your 8051 assembler source code,
- » BL51 Linker/Locator: combines relocatable object modules created by the compiler and assembler into the final absolute object module,
- » LIB51 Library Manager: combines object modules into a library, which may be used by the linker,
- » OH51 Object-HEX Converter: creates Intel HEX files from absolute object modules.

4.1.5 What's New in μ Vision3?

μ Vision3 add many new features to the Editor like Text Templates, Quick Function Navigation, and Syntax Coloring with brace high lighting Configuration Wizard for dialog based startup and debugger setup. μ Vision3 is fully compatible to μ Vision2 and can be used in parallel with μ Vision2.

CONCLUSION:

The project “Design and Development of Wireless RTU and Cyber security Framework for SCADA System” been successfully designed and tested. Integrating features of all the hardware components used have developed it. Presence of every module has been reasoned out and placed carefully thus contributing to the best working of the unit. Secondly, using highly advanced IC’s and with the help of growing technology the project has been successfully implemented.

Reference:

- [1] A. El-Sawah, N. Georganas, and E. Petriu, “A prototype for 3-D handtracking and gesture estimation,” *IEEE Trans. Instrum. Meas.*, vol. 57, no. 8, pp. 1627–1636, Aug. 2008.
- [2] D. G. Lowe, “Distinctive image features from scale-invariant keypoints,” *Int. J. Comput. Vis.*, vol. 60, no. 2, pp. 91–110, Nov. 2004
- [3] A. Bosch, X. Munoz, and R. Marti, “Which is the best way to organize/ classify images by content?” *Image Vis. Comput.*, vol. 25, no. 6, pp. 778–791, Jun. 2007.
- [4] H. Zhou and T. Huang, “Tracking articulated hand motion with Eigen dynamics analysis,” in *Proc. Int. Conf. Comput. Vis.*, 2003, vol. 2, pp. 1102–1109.
- [5] B. Stenger, “Template based hand pose recognition using multiple cues,” in *Proc. 7th ACCV*, 2006, pp. 551–560.