ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2015; 1(8): 246-253
www.allresearchjournal.com
Received: 02-05-2015
Accepted: 05-06-2015

Ashish S. Bandiwadekar
GSM College of Engineering, Pune.

Prof. Manisha P. Dale
MES College of Engineering, Pune.

Correspondence:
Ashish S. Bandiwadekar
GSM College of Engineering, Pune.

Implementation of Programmable Logic Controller with Wireless Bluetooth Connectivity

Ashish S Bandiwadekar, Prof. Manisha P Dale

Abstract
Programmable Logic Controller is a necessary part of today's industry. The PLC is a microcontroller-based, general-purpose electronic device to control the operation of a machine or process. PLCs are not programmed by the device manufacturer but by the machine builder or the end user[1]. The PLC is a robust industrial computer which accepts both Inputs, digital and analogue data from the switches, sensors etc. and controls the output to drive devices such as motors, pneumatic devices and status indicators. For high speed connectivity with PLC, it has got an Ethernet connectivity module[3]. This paper describes the design methodology of the Programmable Logic Controller with the wireless connectivity over classic Bluetooth media. This technique will allow user to configure, control & monitor the remote near field IO devices on wireless Bluetooth connectivity. The main purpose of using the Bluetooth technology is to replace cable connections with comparable communication speed especially for hazardous industrial sector. This paper presents the methodology which will describe the integral parts & operation of the PLC with wireless Bluetooth connectivity[2,6].

Keywords:PLC (Programmable Logic Controller), BT (Bluetooth Technology), LL (Ladder Logic), SDLC (Software Development Life Cycle), MOV (Metal oxide varistor), ASIC (Application specific integrated circuit), GPIO (General purpose input output), HMI (Human Machine Interface), AFH (Adaptive Frequency Hopping), SDP(Service Discovery Protocol)

1. Introduction
PLC's were developed in the late 1960's to eliminate the large cost involved in changing complicated relay based machine control systems. Most of the PLCs have their Host control PC interface over RS232 interface. Now a day's many PLCs have their connectivity with the PC host on USB media. Screw terminals on the PCB allow for the connection of the input, output and power supply wires. Data monitoring, updating operations through PLC is much slower withacceptable delay. Main base of the PLC is having limited IO channels, but many expansion modules can be connected to increase IO capacity of the PLC[3,4].
Bluetooth provides wireless connectivity between the master & slave, Here PLC is a BT master& remote IO is BT slave. Bluetooth works with the 2.4GHz ISM band. Bluetooth operates at frequencies between 2400 and 2483.5 MHz. Bluetooth uses the radio technology called frequency-hopping spread spectrum (FHSS). Bluetooth divides transmitted data into packets and transmits each packet on one of 79 designated Bluetooth channels; each channel has the bandwidth of 1 MHz, Bluetooth 4.0 uses 2 MHz spacing, which accommodates 40 channels. It usually performs 1600 hops per second with Adaptive Frequency-Hopping (AFH) enabled[2,5].

2. PLC Hardware Design
Main building blocks of the PLC is,
1. Power supply section
2. Processor section
3. Communication section
4. Field input section
5. Field output section
6. Display & control

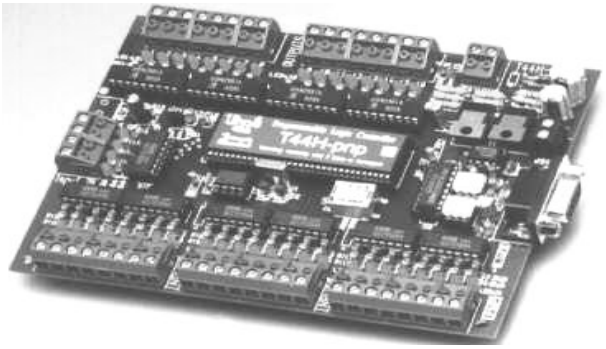


Fig1: A Typical PLC base PCB

Power supply section is the most important section of any industrial product because the noise elimination, generation needs to be handled in this section only. Generally PLC installed to control heavy equipments, machines etc. these industrial equipments are very heavy similarly able to generate very high noise over the supply lines. This high frequency noise generally termaselectricalfasttransientswhichwillresponsibletodisturbth ebehaviorofneighboring equipments. Device power consumption is inversely proportional to the immunity of the device. So the PLC's immunity should be as high as possible because installation of PLC is always in an industrial area where user needs to control high power equipments.

Most of the PLC working on a standard industrial supply voltage which is 24Vdc or 85Vac – 265Vac. Power supply has input resettable fuse which will protect the hardware from over current situation. This fuse has the ratings in several amperes which is much more than the PLC current consumption. It is followed by the surge suppressors (MOV – Metal oxide varistor) which are used as a protection against the high voltage spike like surge. The lower rating of such a MOV should be greater than the maximum possible power supply voltage so that it will provide the high impedance path during normal operation. High frequency & low frequency filter are placed after one another to avoid the external noise injection from supply line into the product. Full bridge rectifier with appropriate value of reservoir capacitor is use to convert AC input into required DC voltage. Appropriate power supply with fly-back or fly forward topology is use to isolate the power supply section from processor & other sections.

Processor section includes the high performance ASIC dedicated for a certain applications like fast ladder execution, Ethernet, USB, LCD controller, High speed dedicated PWM channels etc. this section involves the required reset circuit which provides power on reset to the system, crystal oscillator is used as a clock source. GPIOs are used to input sense & output drive. Different processor peripherals like UART, EMC, SPI is responsible for serial & memory communication respectively. Base timer is the backbone of the PLC firmware where all tasks are scheduled as per timer run. Some critical inputs are treated as interrupt where as the most critical input connected over fast interrupt request to serve on a high priority basis.

The communication section of PLC is having two primary roles one is communication with the host & second is communication with the slaves i.e. IO cards. Generally RS232 communication channel is used between host system & PLC. SPI communication is most widely communicationtypes between base PLC board & slaves (IO cards). RS-232 communication is having standard baud rate between 9600 to 115200 bps, whereas SPI communication works on 1MHz speed. There are some IO cards with wireless connectivity. Generally PLCs are installed in the control room where user can access & control the IOs located away from control room. Such IO card has wired connectivity over RS485 media for longer distance about 500m. Some IO cards are located in hazardous areas like chemical chamber, near reactors etc. so running a long cable near such fields are very dangerous because energy in wired signal may enough to cause explosion. So such remote IO units will equipped with the wireless connectivity like Bluetooth.

In Bluetooth communication PLC is assembled with BT master module, whereas remote IO unit will have BT slave module. Initially, when PLC got powered up the ASIC will configure the Bluetooth master with initial enumeration sequence & push the radio synchronizer inside BT chip at default level where UART set to the default baud rate & initialize the frequency synthesizer for scanning. When remote IO gets power up then its controller will push Bluetooth chip in slave mode for advertising. Master chip always periodically scan for slave & slave will respond with broadcast advertising. Once master finds the slave it will send connection request& in response slave will respond with connection acknowledgement & here link is said to be establish; now master can ask for data towards slave once pairing & bonding is completed. Bluetooth technology is best suited for the point to point communication with the comparable baudrate ascompare to wiredcommunication.

Following sequence is showingthe communicationbetweenmaster& slave.Threechannelsare usedforadvertising& other channels are used for as data communication. The frequency hops follow a pseudo random sequence that meets the power density requirements for the FCC and other regulatory bodies.

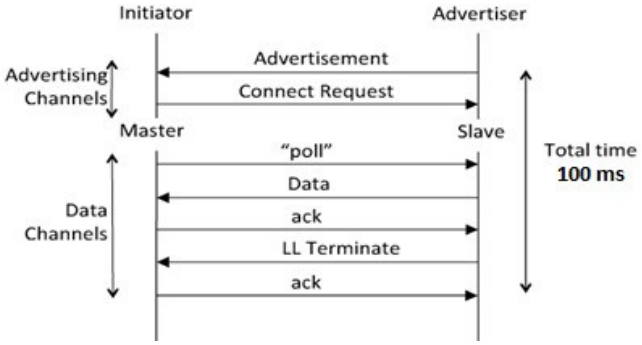


Fig2: Bluetooth Communication sequence between Master & Slave

Field input output section is consist of digital switches & analog sensors. PLC has digital input section to sense any universal voltage value (18Vdc to 100Vdc also 85Vac to 265Vac) & convert it into digital 1 or 0. PLC also has high speed digital input sense circuit also known as a high speed counter. Along with this the digital output section is depends on the type of application used in field like PNP, NPN, Relay type output. This digital outputs are used to actuate the valve, actuator, motor etc. To control the average DC output at the output of PLC they are equipped with the high speed PWM channels. Almost all PLCs are providing the isolation between field ground & internal processor ground to avoid the damage or malfunctioning of PLC in field. Generally

optical isolation is the low cost, safe & good choice to provide isolation between field input & sensing part of controller. For high speed applications such as counter, up down counter, quaderature counter the high speed optocouplers are used. For high speed communication like Ethernet, USB many high speed isolators are available in market. Optical, capacitive & galvanic isolations are the popular isolation techniques used in PLC market.

Some PLCs are coming with the displays on top of it. This shows the input, output status on screen along with the real time clock & menu option. User can configure partial operation of the PLC with the display buttons. Some low cost PLC has rubber made buttons (to avoid electrostatic discharge), some PLC has touch screens & high end PLCs are coming with the HMI (Human Machine Interface) for more precise application control. Display provides continuous update on time, date, IOs, LL execution, Alarm &other functions.

3. Bluetooth Stack and Communication

A Bluetooth device operates at 2.4 GHz in the license-free globally available ISM (Industrial, Scientific and Medical) radio band. A potential disadvantage is that Bluetooth devices must share this band with many other RF emitters. These includes automobile security systems, other wireless communications standards (such as 802.11), and ordinary noise sources (such as microwave ovens)[5]. To overcome this challenge, Bluetooth employs a fast frequency-hopping scheme. Frequency hopping is literally jumping from frequency to frequency within the ISM band. Main advantage of the frequency hopping technique is, it allows Bluetooth devices to use the entire available ISM band which ensures that any interference will be short-lived. Any packet that doesn't arrive safely at its destination can be resent at the next frequency. It provides a base level of security because it's very difficult for an eavesdropping device to predict which frequency the Bluetooth devices will use next[2,6].

The Bluetooth specification ensures this in two ways. First it defines a master-slave relationship between Bluetooth devices. Second it specifies an algorithm that uses device-specific information to calculate frequency-hop sequences. Master sends the clock information to the slave which will decide the frequency hopping sequence. In Bluetooth architecture there are two most important parts the one is Bluetooth specification & Bluetooth profiles. Standard Bluetooth protocol stack is shown below[6],

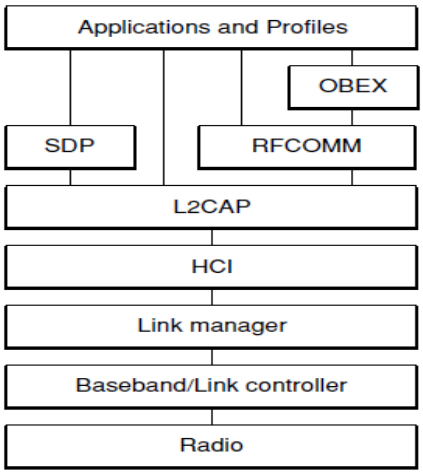


Fig 3: Bluetooth Protocol Stack

The lowest layer is a radio module in a Bluetooth device is responsible for the modulation and demodulation of data into RF signals for transmission & reception. The radio layer describes the physical characteristics like modulation characteristics, radio frequency tolerance & sensitivity. Baseband layer is responsible for proper formatting of the data from & to radio layer, also handles the synchronization of the links. Link controller layer provide the link between link manager & below layer. It will encapsulate the data to be sent. Link manager's job is to translate data frame from HCI interface to Baseband format &vice versa. It is responsible for establishing& configuring links & managing power control configurations.

Bluetooth specifications support two types of links between the devices, One is SCO (Synchronous connection oriented) it is for voice communication like handsets, A SCO link supports regular, periodic exchange of data with no retransmission of SCO packets. Another link is ACL (Asynchronous connectionless) it supports data exchange. ACL link supports the retransmission of data on failure so this link is more robust for the noisy environment[2,6].

HCI (Host controller interface) divides the Bluetooth stack into two parts, layer below HCI is called a Bluetooth module (lower layer) & upper is called Bluetooth host (upper layer). In this system we have on chip complete Bluetooth stack, mean module has both layers. HCI specifications define only when there are two separate processor to control lower & upper layer operation. In upper layer protocol the L2CAP (logical link control & adaption protocol) is the basic & most important layer in upper part of stack, its primary function is,

- Maintaining the connection across existing ACL links & establish new if required
- Multiplexing between higher layer protocol (such as RFCOMM, SDP) & single ACL link

This layer provides a logical channel to multiple data on multiple or single ACL link. The SDP (service discovery protocol) defines actions for both servers and clients of Bluetooth services. Single Bluetooth device can support both, server & client services. An SDP client communicates with an SDP server using a reserved channel on an L2CAP link to find out what services are available. When the client finds the desired service, it requests a separate connection to use that service. The SDP server maintains its own SDP database, which is a set of service records that describe the services that server offers, along with the information describing how a client can connect to the service, the service record contains the service's UUID (universally unique identifier). The RFCOMM protocol emulates the serial cable line settings and status of an RS- 232 serial port. RFCOMM connects to the lower layers of the Bluetooth protocol stack through the L2CAP layer. OBEX (object exchange) is a transfer protocol that defines data objects and a communication protocol, so that two devices can easily exchange those objects. A Bluetooth device wanting to set up an OBEX communication session with another device is considered to be the client device. Following are the steps for connection link on OBEX[6],

Step1: The client first sends SDP requests to make sure the other device can act as a server of OBEX services.

Step2: If yes then server responds with OBEX service records. This record contains the RFCOMM channel number which client should use to establish an RFCOMM channel.

Step3: Convey the communication in packets of request, response & data packets. The format of the packet is defined

by the OBEX session protocol.

The Bluetooth specification defines a wide range of profiles, describing many different types of tasks; every profile depends on the base profile, called the generic access profile. This GAP establish a baseband link between Bluetooth devices. GAP performs the generic procedures for discovering and linking to devices also it provides Basic user-interface terminology

GAP is a basic platform for all profiles so it ensures a high degree of interoperability between applications and devices. Here Bluetooth device uses service discovery application profile, this profile specifies the usage of SDP for service discovery on a remote device before connection. The serial port profile defines RS-232 serial-cable emulation for Bluetooth devices. As such, the profile allows legacy applications to use Bluetooth as if it were a serial-port link, without requiring any modification. The serial port profile uses the RFCOMM protocol to provide the serial-port emulation. In such application class1 device is used whose maximum power is up to 100mW (20dBm), which achieves the range up to 100m.

4. System Integration

Block diagram of PLC with the Bluetooth connectivity is shown below,

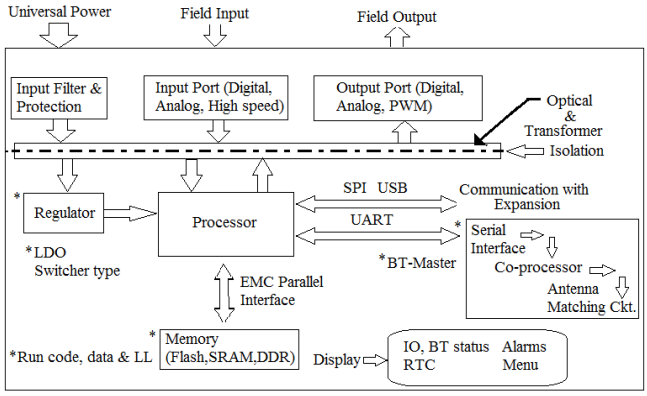


Fig4: PLC block diagram with BT module

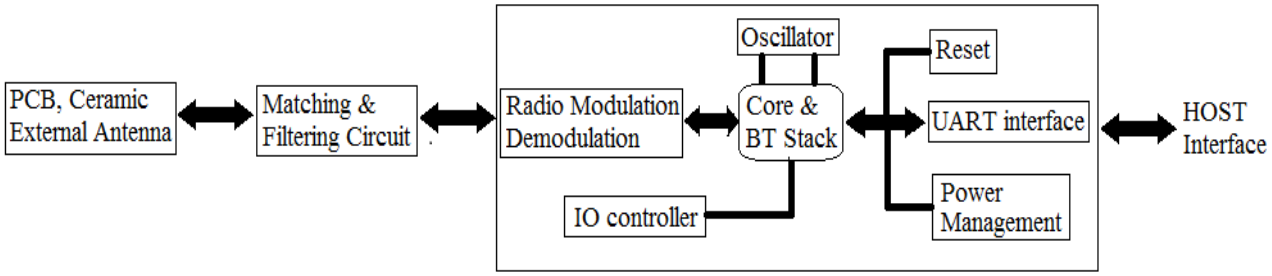
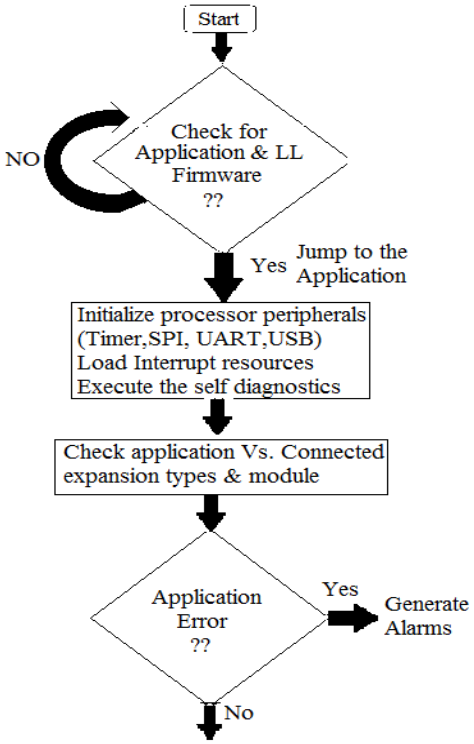


Fig 5: Bluetooth module

5. Firmware Flow

There are two basic firmware flows one is PLC flow with BT as master & other is remote slave flow with BT slave,



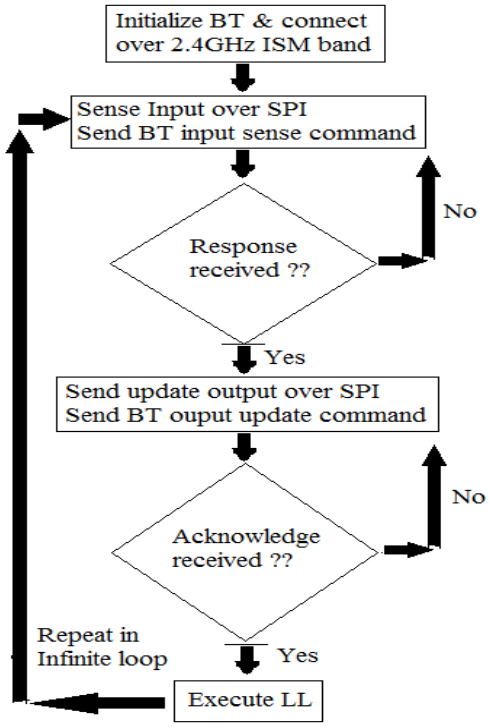


Fig6: Main PLC Base Firmware Flow

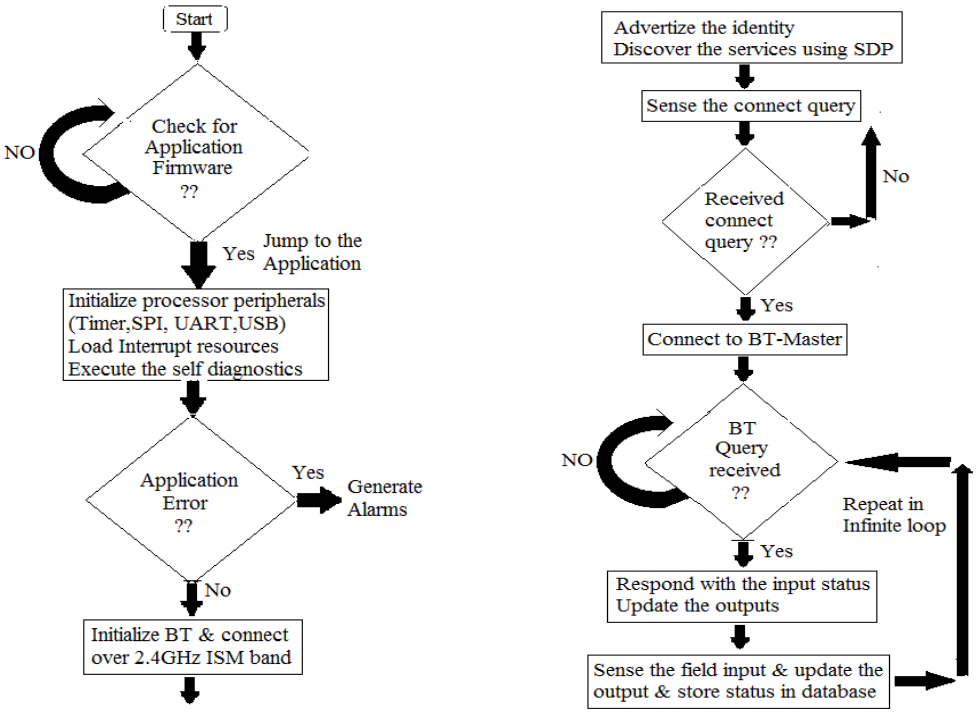


Fig7: Remote expansion Firmware Flow

6. Result and Conclusion

This paper has described the block wise implementation of the PLC with BT master device. Tested maximum range for Bluetooth communication is about 100m based on the antenna used. For the PCB antenna on both side (master & slave) communication range is up to 30m, with chip ceramic antenna it gives a range up to 50m & with external antenna this range can be extend up to 100m. Following are some snapshots showing the system validations,

Fig8: Processor clock validation

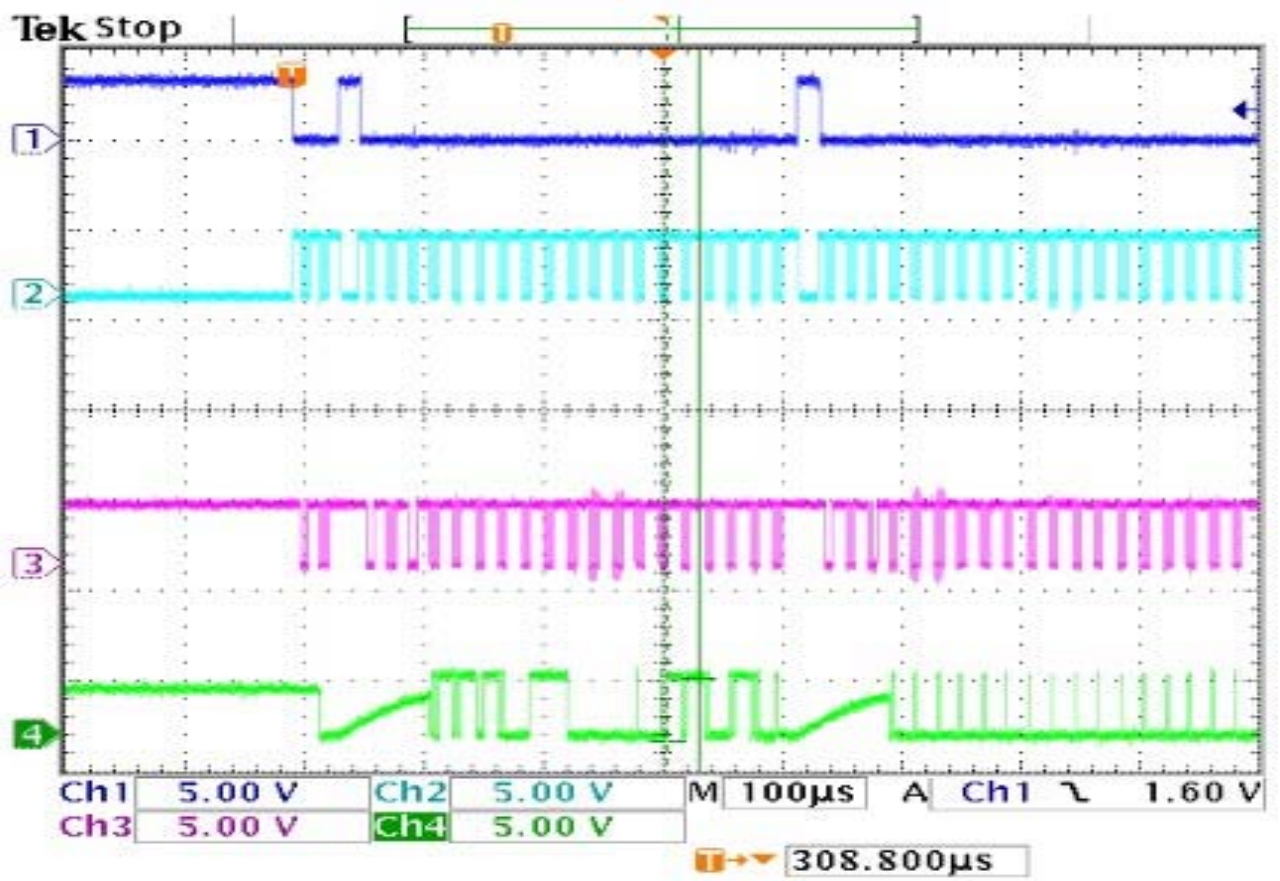


Fig9:SPI signal validation (CS, Clk, MOSI, MISO)

Fig10: Serial BT Frame structure

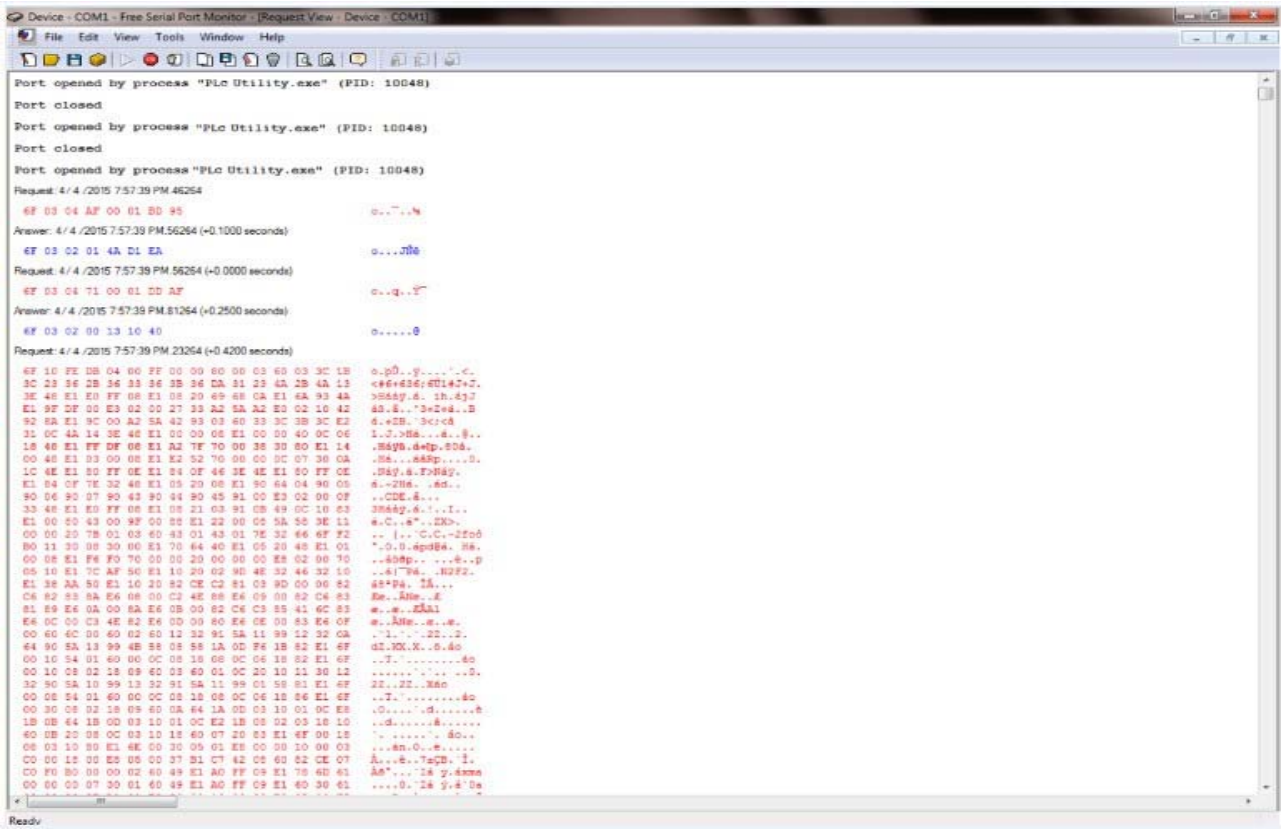


Fig11: Software upgrade session from base to remote IOs

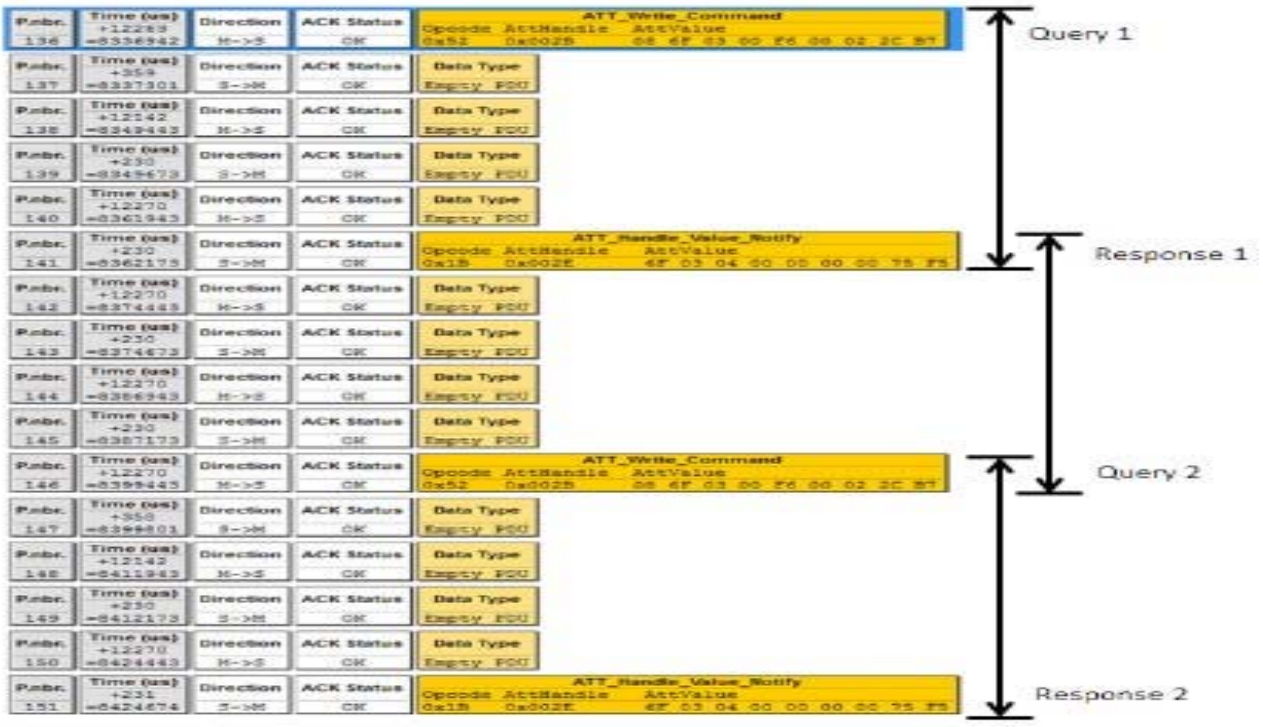


Fig12: Bluetooth packets in the air

From the results it is verified that the proposed methodology of PLC with BT connectivity is low cost & best suited for the hazardous area operation. Future scope is to increase the range & data rate of communication to cover maximum possible industry premises.

7. References

1. Yousif I, Al Mashhadany. Electrical Engineering Department, College of Engineering, University of Anbar, Baghdad, Iraq Design and Implement of a Programmable Logic Controller (PLC) for Classical

Control Laboratory Intelligent Control and Automation, 2012, 3, 44-49, Published Online February 2012 (http://www.SciRP.org/journal/ica) ; Copyright ©, 2012 SciRes.

2. Sairam KVSSSS. University of Madras, Dr. M. G. R. Engineering College; N. Gunasekaran, Anna University; S. Rama Reddy, Jerusalem College of Engineering, Dr. M. G. R. Engineering College, Bluetooth in Wireless Communication IEEE Communications Magazine 0163-6804/02
3. Raja Narayanasamy. Product Apps Manager Sr, Cypress Semiconductor Corp Designing an efficient Programmable Logic Controller using Programmable System On Chip, Published in EE Times Design, January, 2010.
4. Michael Barrett.The Design of A Portable Programmable Logic Controller (PLC) Training System for Use Outside Of the AutomationLaboratory", FAS Training Centre, Athlone, Co.Westmeath, International Symposium for Engineering Education, 2008, Dublin City University, Ireland.
5. Malik ZakaUllah.An Analysis of the Bluetooth Technology, Master Thesis Computer Science, Thesis no: MCS-2009-1, June 2009; School of Computing; Blekinge Institute of Technology Soft Center SE-37225 Ronneby Sweden.
6. Working With Bluetooth Devices, Preliminary 06-29, Apple Computer, Inc. © 2003, 2004 Apple Computer, Inc, 2004.