Implementing Modbus along on PIC32MX795F512H for Data monitoring and control of sensor nodes using RS 485

Mr Sameer S Nagtilak[1], Dr S R Chougule[2]
[1]Assistant Professor,KITs COE, Kolhapur
[2]Professor, KITs COE, Kolhapur

Abstract:
In majority of countries industrial automation is growing rapidly. Large no of sensors and actuators are used for data transmission between these nodes. Various protocols are used in automation fields such as Modbus,profibus,canbus etc. In this paper we are going to review about the applications in which Modbus protocol is used efficiently and its security aspects.

1.Introduction

Modbus is a data communication protocol which is invented by Modicon in 1979 mostly having large applications in PLCs, SCADA. Modbus is popular in industrial environments because it is openly published and royalty free. Modbus is basically developed for industrial applications, is relatively has advantage over other protocols. Physical channel used by Modbus is RS 485 or Ethernet. Modbus supports communication to multiple devices connected to the same cable or Ethernet network. Different sensor or actuators used are temperature, humidity etc. It actually connects remote terminal unit(RTU) with the supervisory unit in huge industrial applications.

2. Modbus Protocol Version

- Modbus RTU – In this version data is represented in binary format and mostly used in serial communication. The reliability of data is very important for which CRC checksum is used for error
- checksum mechanism. A Modbus RTU message must be transmitted continuously without inter-character hesitations.
- Modbus ASCII – In this version ASCII characters are used for communication. In ASCII format uses a longitudinal redundancy check checksum. Modbus ASCII messages are framed by leading colon (":") and trailing newline (CR/LF).
- Modbus TCP/IP or Modbus TCP – This version is specifically used for TCP/IP networks with port 502. No checksum mechanism as lower layers already provide checksum protection [1].
- Modbus over TCP/IP or Modbus over TCP or Modbus RTU/IP – The difference between this version and above version is in this checksum is included in the payload as with Modbus RTU.
- Modbus over UDP – In some application at transport layer it has been also used along with UDP, which removes the overheads required for TCP [2].
- Modbus Plus (Modbus+, MB+ or MBP) - Modbus Plus is official used with to Schneider Electric which supports point-point communications between multiple masters. It requires a dedicated co-processor along with a twisted pair at 1 Mbit/s and includes transformer isolation at each node, Some extra hardware is required to connect Modbus Plus to a computer, typically a card made for the ISA, PCI or PCMCIA bus [3].

3. Communication and Devices

In modus network an unique address is allotted to each communicating device. Two types of command are used i.e Request and response. In RTU,ASCII and Plus mode only the node assigned as the Master may initiate a command. All other devices are slaves and respond to requests and commands. However when Modbus is implemented on Ethernet as Modbus TCP then each of the node works as Master and initiate the connection. Number of modems and gateway support Modbus applications.

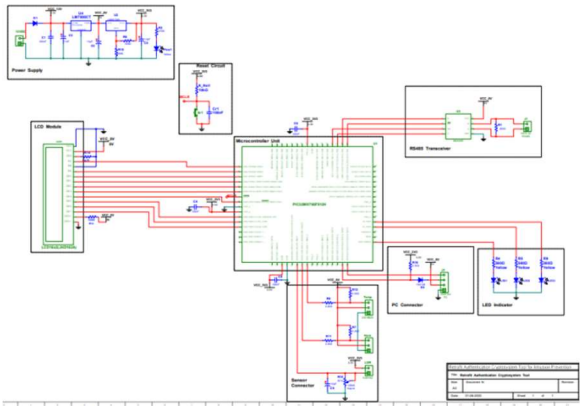
4. Commands and Frame format

Commands used to instruct Modbus devices are:
- Change value in register
- Write into coil/holding register
- Read I/O port
- Read data from Discrete/coil

Modbus devices address the range from 1 to 247. Modbus frame consist of application data unit (ADU) which encapsulates a Protocol Data Unit (PDU).

ADU = Address + PDU + Error check
PDU= Function code + data

5. Circuit layout



Above figure is the circuit layout of the proposed work which consist of 8 modules namely power supply, LCD module, reset circuit, microcontroller unit, RS 485 transceiver, sensor connector, pc connector and LED indicator,

5.1 Power supply

This module consist of LM7805 and LM317AH. LM7805 is 3 pin IC voltage regulator provides 5v output. internal current limiting, thermal shut down and safe operating area protection, making it essentially indestructible[4]. LM317 is adjustable voltage regulator which provides range from 1.25 V to 37 V. It also consist of thermal overload protection. Supply from above modules are provided to microcontroller unit, LCD module, RS 485 transceiver [5].

5.2 Reset Circuit

It takes care that system power supply stabilizes at the appropriate levels based on applications, the clocks are also fixed up at correct level, and that the loading of the internal registers is complete before the device actually starts working or gets powered up.

5.3 LCD Module

5v supply from power supply module is given to LCD module which is JHD162A.The display construction is 16 characters * 2 lines with TN/STN display mode and positive transflective display type. It contains 8 bit parallel data lines. The operating voltage is -.03V to + 7.0 V [6].

5.4 Microcontroller Unit

The LCD module is connected to microcontroller unit which we are using is PIC32MX795F512H. It is 32 bit with upto 512 KB Flash and 128 KB SRAM along with graphics interface. This module is basically used for controlling the function of LCD module, RS 485 module and sending and collecting request and response from sensor nodes. For further application such as to connect above system to internet i.e. Ethernet standard PC connecter is connected to this unit so that it act a bridge between Ethernet and RS 485 standard. Also LED indicators are connected are connected to keep the track of output [7].

5.5 RS 485 Transceiver

MAX485 is low power consumption transceiver used for RS 485 communication which consists of one driver and one receiver. Operating voltage is 5V. Thermal shutdown circuit is used to place the output of driver at high impedance state. It also handles fail safe state along with it provides anti interference performance [8].

5.6 Sensor Connector

To above microcontroller unit three sensor are connected as to implement Modbus protocol along RS 485 namely Temperature, humidity and LDR. The temperature sensor we are using is DS18B20 and LDR is HDR1X2. DS18B20 is 9-bit to 12-bit digital thermometer which measures temperature in celsuis with in built alarm function. It uses only one wire for communication with central controller. It also extract power from data line itself which avoids extra cost and hardware for external power supply [9].

5.7 PC Connector

TX and RX pin of microcontroller is connected to PC connector module having HDR1X4 connector. The GUI to be developed based on VB will be developed on PC through which the patterns will observed which are moving from master to sensor nodes. For this communication we are using Modbus protocol with RS 485 as communication channel. Also this pc wil be acting as the module through which we are going to attack the Modbus network. Intrusion prevention algorithms will be also installed on this pc which will avoid corruption of data and it will be transmitted with security in Modbus network.

5.8 LED Indicator

Three LEDs are used which are connected to microcontroller which can be used ti check various outputs which we are expecting from the above network.

6. Various Applications

As discussed above we are going to develop a network consisting of above 8 modules on which Modbus protocol is implemented with RS 485 as communication model. In number of industrial applications Modbus protocol are used. It can be used in power systems were reliable flow of data is required. Currently large number of applications are present in which single mode of monitoring is required. In such cases Modbus can be combined alone with ARM5708, Linux system, Java Web along with Ethernet standard on which Modbus TCP protocol can be implemented [10].

Also currently rapid development is going on in application of smart home due to rapid development in internet technology. A new smart control applications can be developed if residential application together with motor control and Modbus TCP. For this we can use STM32 series ARM. It can be used to read water, electricity, gas meter but also to monitor gas leakage, fire, door or window magnetic and other security facilities to prevent fire and pilferage [11].

On Ethernet standard Modbus TCP can be also applied on IIoT environment. IIoT environment is built using request – response communication pattern in which polling based mechanism is used. Also in MQTT mobile to mobile

communication is used with asynchronous communication pattern. In this pattern also we can use synchronous request – response communication pattern. Thus Modbus can be used in both synchronous and asynchronous application [12].

Modbus protocol is also used in smart metering applications. Here Modbus RTU is used along with copper fieldbus. In such applications error detection and correction devices are also used for the errors caused due to electromagnetic interferences. It isolates against noisy channel. Here Repeater/error corrector (R/C) devices are introduced between two end devices using parity check method to isolate the effect of electromagnetic interference. Further it was suggested to study the interference by electrical feeders and also to find the suitable Reed–Solomon code for the detection and correction of errors in these systems [13].

Manufacturing industries play very important role in mechanical engineering were data monitoring of running machines has to be monitored at regular interval of time. In some fields it is taken manually but it can cause errors, so automated technology is used based on IoT devices on which Modbus protocol is implemented. In this system Ardino, PLC, GSM is used in cost effective manner [14].

Various software platforms are base of Industrial Internet of Things(IIot) In this auto configuration of the master and client nodes is done along which its Ethernet network with no human man power used. Here OPC UA system is proposed which is used for secure data exchange between control station and client node. During power failure or interruption the system doesn't halt by which operator can modify the faulty nodes in industries and again the data is transferred using Modbus protocol and also Modbus TCP when the same is implemented on Ethernet standards. [15].

7. Conclusion

As seen above we have seen basics of Modbus protocol along with its version and command format. We have also seen the layout of proposed idea which includes eight modules namely power supply, LCD module, reset circuit, microcontroller unit, RS 485 transceiver, sensor connector, pc connector and LED indicator. We have also seen the series of above modules to be used in our proposed work. As per different applications seen above Modbus protocol has wide range of application in smart home application, power station monitoring and various industrial application which can be implemented using microcontroller, Arduino, PLCs chip along different sensor or actuators at end node. Using above layout we are going to monitor and control different sensor nodes by central control station through Modbus protocol and RS 485. Once it is implement we can implement security features on protocol to avoid it from various intrusions.

8. References

[1]Modbus Messaging on TCP/IP Implementation Guide V1.0b (PDF), Modbus Organization, Inc., October 24, 2006, retrieved 2017-01-07

[2]"Java Modbus Library - About". 2010. Retrieved 2017-02-07.

[3] "What is the difference between Modbus and Modbus Plus?".Schneider Electric. Retrieved 2017-02-07.

[4]LM7805 data sheet by Fairchild semiconductor

[5]LM317 data sheet by Texas instrument.

[6]JHD162A data sheet.

[7]PIC 32 MX data sheet by Microchip.

[8]MAX485 data sheet by maxim intergrated.

[9] DS18B20 data sheet by maxim intergrated.

[10] Design and Implementation of Modbus Protocol for Intelligent Building Security by Wenzhu You, Haibo Ge 2019 IEEE 19th International Conference on Communication Technology (ICCT).

[11]Application of Modbus / TCP Protocol in Smart Home Zeyu Xiao Advances in Computer Science Research, volume 70, 2017.

[12]Communication Protocols of an Industrial Internet of Things Environment: A Comparative Study, Samer Jaloudi , MDP, furure internet, 2019.

[13]Enhancing Modbus-RTU Communications for Smart Metering in Building Energy Management Systems, Claudio Urrea and Claudio Morales, security and communication network 2019.

[14] Design Of Industrial Data Monitoring Device Using Iot Through MODBUS Protocol, Mageshkumar G, Kasthuri N, Tamilselvan K S, Suthagar S, Sharmila A., IJSTR, January 2020.

[15] Automatic Configuration of OPC UA for Industrial Internet of Things Environments Jose Miguel Gutierrez-Guerrero, Juan Antonio Holgado-Terriza, MDPI electronics, April 2019.