MODBUS To GSM Gateway

Kaustubh V. Samangadkar[1], Sagar D. Rathod[2], Mahesh M. Yenchewad[3], Prof.Kapil B. Kotangale[4]
[1, 2, 3, 4] Dept. of Electronics and Telecommunication
[1, 2, 3, 4] Pimpri Chinchwad College of Engineering, Pune,Maharashtra,India

Abstract*- This paper shows the design of an embedded system for remote accessing of various devices connected to a MODBUS protocol via GSM. This paper brings forward a method for encapsulating a MODBUS message into a short message. It also discusses method for encapsulating AS-CII message for alarm system and instruction message for devices between server and Gateway device.*

Keywords- MODBUS PROTOCOL , GSM,GATEWAY,AS-CII message

I. INTRODUCTION

MODBUS to GSM Gateway is a device use for remote accessing various industrial sensors and devices connected to a Modbus protocol. In the old days for reading the status of various devices in the plant one requires to visit each device. This method is tedious and waste more time and human resources. The MODBUS to GSM Gateway overcome this all disadvantage. It is an intelligent system which reads the data from the devices and sends the user instructions with help of GSM. The gateway is most efficient in the large field plants where remote accessing is very important. Reducing the requirement of repetitive visits to plants user can directly access the various process and status of the plant on a remote server connected to a GSM or a handheld device having GSM protocol to receive messages.

A. Architecture

Figure shows the MODBUS to GSM gateway, as shown the GSM and MODBUS interface is connected to the controller.

The controller is responsible for distinguishing the received data is command or user data. The gateways are connected to the server on which the user access the status and can give instructions to the devices connected to the Modbus interface. When user gives the instruction the server convert this AS-CII message into GSM frame which is sent to the remote gateway. The Gateway function is to convert this GSM frame to MODBUS frame by removing the TPDU. It also convert the MODBUS frames to GSM frames which is short message transmitted on GSM network. When a short message is transmitted into the GSM network, it is first stored in the SMSC (Short Message

Service Center). After verifying the service subscription and making necessary modification to the short message PDU, valid messages will be routed to their destination, whereas the invalid ones are dumped by SMSC, with a send-failure report to their originations. If the destination is out of reach during the process, the message will be temporarily stored in SMSC. Such store-and-forward routine provides reliable transference for short messages, but in the mean time it brings about an inevitable delay for each message. It also gives rise to obsolete messages. These problems are disastrous for monitoring systems. The monitoring systems count on the gateway software to solve them. When a short message is received, it can be restored to its original industrial form by removing the SMS TPDU head. This is also conducted by the gateway of the monitoring system. If needed, the message content can be put into other form and forwarded by the gateway through other industrial network.

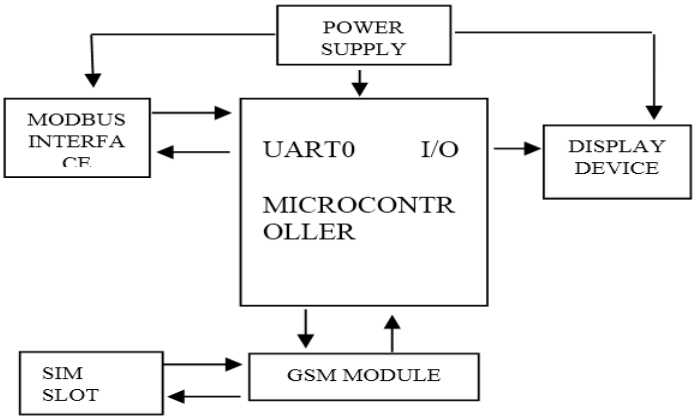

Figure 1. MODBUS To GSM Gateway Architecture

B. Introduction to AT Commands

As shown in figure1 the industrial instructions are transmitted with the help of GSM network. Data for monitoring and commands for the devices are encapsulated in short message. The GSM module connected to the controller as shown in figure communicate with each other with help of AT Commands. AT commands are set of commands which are standardize to communicate with terminal device and GSM modem. Some of AT commands mostly used are:

AT+CMGS: To send a short message
AT+CMGR: To read a short message from the GSM Module.
AT+CMGL: To list SMS short messages stored in the GSM module
AT+GMGD: To delete a short message from the GSMmodule.

As the low-level function interface to the GSM modem, these commands play a fundamental role in the software developing of the gateway program.

II. FORMAT AND ANALYSIS OF MODBUS

A. Introduction to modbus

MODBUS is very widely used application layer protocol in industrial fields. It is most efficient application layer which can be transferred though any network. It is simple and have two modes of coding which is AS-CII and RTU.A-CII is 7bit coding whereas RTU 8bit coding mode. To deliver Modbus messages via SMS, the application data unit (ADU) of Modbus needs to be modified according to the features of SMS, and then merged into the SMS PDU. Below is a basic scheme for the modification:

- The sync word is optional, one can remove or replace it with a password. A short message may not need sync word. However, there may be need of password field there.
- The device address field is required for the identification of the destination device. A device can be identified by SIM card number.

A check field is required as there is no guarantee of wireless transmitted data to be found correct at the destination. The check field is CRC-16.

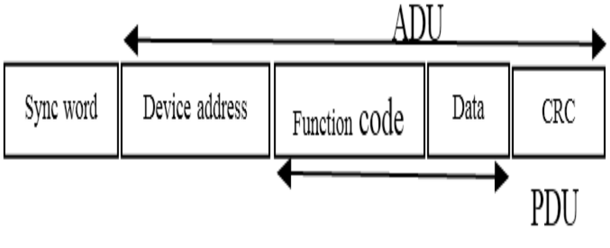

Figure 2. Standard Modbus Frame

As discussed the modified bus is shown in figure3.

Table 1. shows the frame format of MODBUS TCP

Hex code	Description
00	Refference
00	Unit ID
6	Length
1	Function code
24	Standard address
255	Data

III. SOFTWARE DESIGN FOR THE GATEWAY

The software design for the gateway is most crucial and at central position of gateway developing.

The main function of the gateway is two receive the SMS packets from server and convert them to proper MODBUS frame for the devices connected to the MODBUS network.

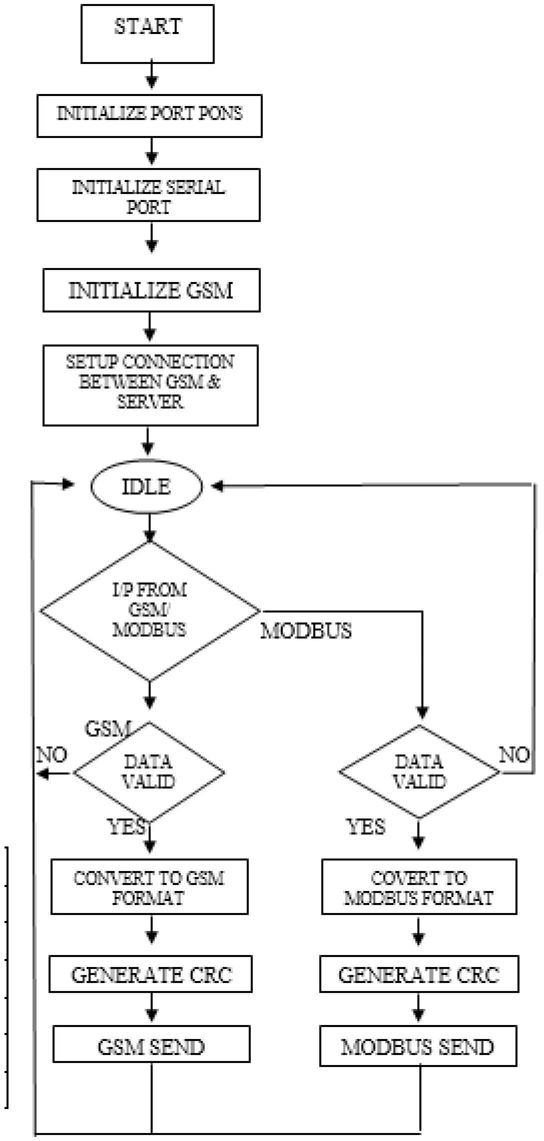

Figure 3. Flowchart for software design

Figure shows the flowchart for the gateway software. It illustrate the key steps for the program.

As shown in figure the gateway program first initializes he controllers all port pins and serial port for receiving and transmission of the data. Next step is to check if there are GSM commands received from the server PC. If yes then the data received are converted to proper MODBUS frames for the devices connected to the MODBUS network. After the conversion the MODBUS frame is transmitted on the MODBUS network.

This are the steps when the gateway receives the data from server PC but when the status of the devices and readings from devices connected to the MODBUS network need to be transmitted the gateway first accept the MODBUS data from the port pins and the it is converted to proper GSM frames which are MODBUS TCP frames. After the conversion of the frames the data is transmitted to the serial port for transmission from the GSM. Besides, the gateway program should provide application interface for the upper layer program, including such functions as sending user data by SMS and notifying the arrival of a short message, etc.

IV. CONCLUSION

This Paper Discusses The Implementation And Design Of A Wireless Remote Sensing Gateway For The Modbus Network With The Help Of Gsm. The Development Of Gateway Programme For The Conversion Of Data Received And To Be Send Toward The Main Pc Is Also Discussed.

REFERENCES

[1] On user Data Protocol Of SMS in Remote Monitoring System, Yu Zhen ; Sun Qiuwei , Environmental Science and Information Application Technology, 2009 ,ESIAT2009. Volume 1

[2] New TECHNOLOGY For Ecosystem-Based Management : Marine Monitoring With the ORCA Kilroy Network, Eric D. Thosteson ; Edith A. Widder ; Chares A.Cimagila ; John W. Taylor; Benjamin C Burns ; Keith J. Paglen OCEANS 2009-EUROPE

[3] Modicon MODBUS Protocol Reference Guide,PI-MBUS-300 Rev.j ,Chapter 1 Page no 2-9 (refference)

[4] Wiley: GSM –Architecture, Protocol and Services,3rd Edition –"Jorg Eberspacher , Hans-Joreg Vorgel, Christian Bettstetter , Christian Hartmann" ISBN:978-0-470-74172-6;Section:-3.2, Page no.33(refference)