Development of A web and GSM Based Monitoring and Controlling System for PLC Based Application

A.S. Gundale[1] K.M. Vakani[2] P.D.R. Patnaik[3]
[1, 2, 3] Department of Electronics Engineering, WIT Solapur, Maharashtra (INDIA).

Abstract-- In this paper we have developed a platform to remotely monitor and control PLC-based processes over web and GSM network. It will be great benefit if we control the process plant through remote monitoring and controlling. In recent years the development of industrial automation through remote monitoring and controlling has been increased. The proposed system is made possible by the use of PLC, Microcontroller, GSM modem, Ethernet Module, and other elements. The main aim of the remote monitoring and controlling is when a critical failure occurs notifications are generated and send to the expert via SMS and internet message with the help of GSM modem and through internet. The remote controlling of process is now much required control to use expert man power. The challenge here is to establish a proper serial and Ethernet communication between PLC and Microcontroller via appropriate protocol and also to integrate conventional process with recent communication technologies along with advancements in wireless and internet technology.
Keywords: PLC, Microcontroller, Real time control, remote controlling

I. INTRODUCTION

A Programmable Logic Controller is programmed to control the operation of the plant and a SCADA system implemented to monitor and control the process [1].A control program stored in the PLC memory determines the relationship between the inputs and outputs of the PLC.PLCs are intelligent automation stations that possess highly useful and desirable features such as Robustness, High degree of scalability, Powerful development Environment, sophisticated Communication capabilities, Extensibility etc[2].
Industrial monitoring involves monitoring and controlling of different plant's factory or manufacturing conditions while logging data to enterprise systems[3]. The system which we have proposed is likely to offer economical solution for various users in a lab based environment [4].

II. PRESENT TRENDS OF CONTROLLING OF PLC PLANT

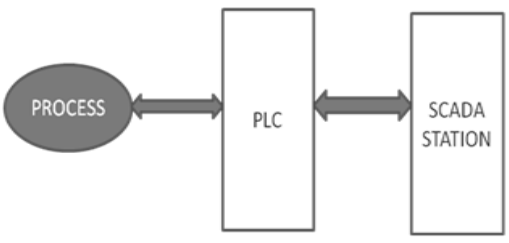

Fig. 1: System overview of controlling a PLC plant

Figure 1 shows basic overview of a present system which is normally implemented in process control plant, The system compromise of a PLC which is used to control the process and a PC which is used for graphically view of the PLANT and as a SCADA station through which we can control the process as well as have the status of alarms, history trends and real trends etc.

III. REMOTE CONTROLLING SYSTEM OVERVIEW AND DESIGN

The system overview of Development of a Web and GSM based system is shown in fig-1.This system can be controlled by either through mobile or through internet Monitoring and controlling system for PLC based application

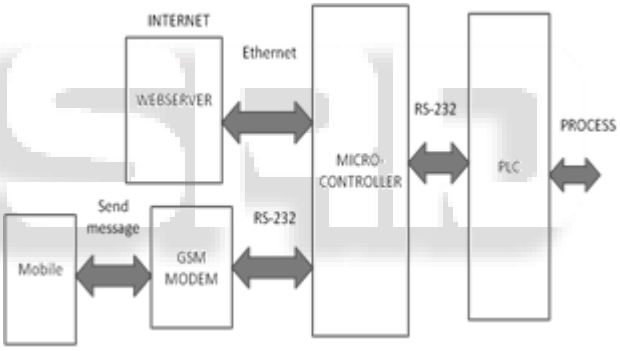

Fig. 2: System overview of Development of a Web/GSM based

IV. MODBUS PROTOCOL ARCHITECTURE

Modbus is a Master-Slave Serial Line protocol. This protocol takes place at layer 2 of the OSI model. A Master-slave type system has the master node and slave node. The master node will issue explicit commands to one of the slave nodes and Processes responses. The client that initiates a Modbus transaction builds the Modbus PDU, and then adds fields in order to build the appropriate communication PDU which is shown in fig 3.

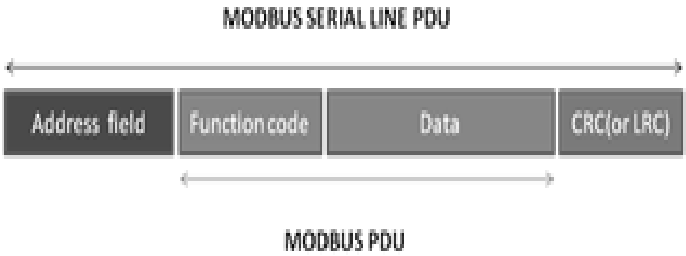

Fig. 3: Modbus mapping.

V. MODBUS MASTER ALGORITHOM

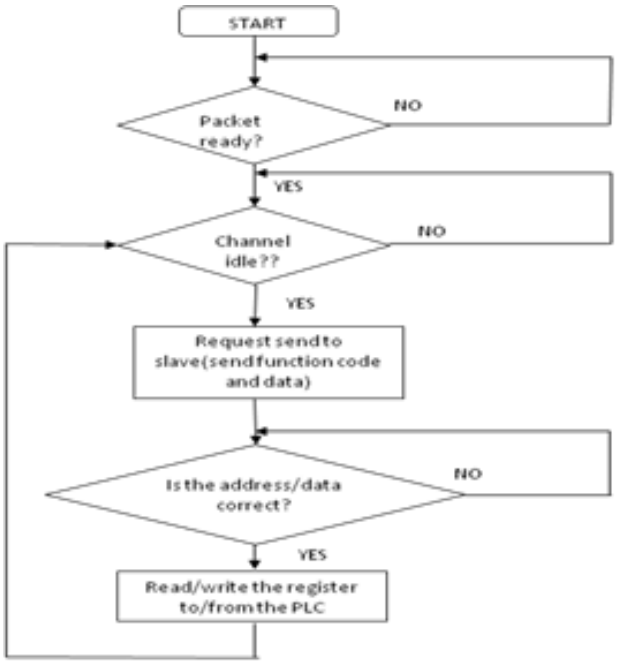

Fig. 4: Modbus master behavior

VI. MODBUS SLAVE ALGORITHOM

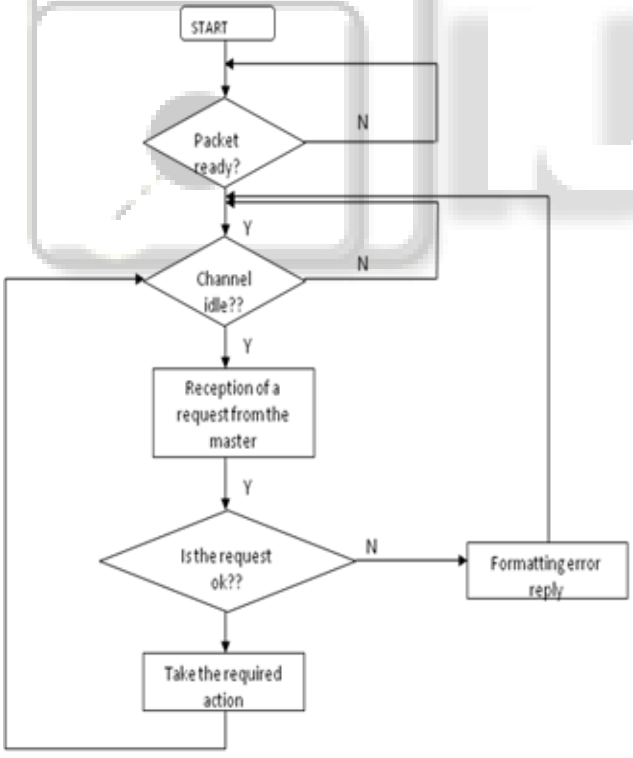

Fig. 5: Modbus slave behavior

Fig.4 and Fig.5 shows the implemented MODBUS protocol which follows a master/slave architecture where a master will request data from the slave. The master can also ask the slave to perform some action. The master initiates a process by sending a function code that represents the type of transaction to perform.

The transaction performed by the MODBUS protocol defines the process a controller uses to request access to another device, how it will respond to requests from other devices, and how errors will be detected and reported and if the address and data format is correct then it will write or read the data from the desired register and will send the status of that coil/register.

In this system the PLC is interfaced with the micro-controller serially using RS-232 serial port. The controller which has serial communication capabilities interfaced with PLC using MODBUS protocol by writing a separate library in microcontroller. We can remotely monitor and control the I/O of PLC by using the WEB as well as MOBILE. So user can choose the appropriate option for the controlling.

VII. GSM INTERFACE

Short Message Service, better known as SMS is a service that enables the sending of text messages over a mobile cellular network

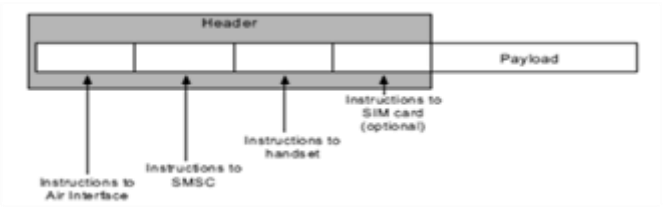

Fig. 6: SMS format

The above figure shows the standard SMS format. It contains a payload and header. The header is used to include the originating address (the phone number of the sender) as well as to route the SMS to the desired user. The payload is used to display the message content.

VIII. TESTING PROCEDURE FOR GSM

1. When PLC receives the short message of control data from the user; it will automatically report the status of PLC output to the user.
2. When the data in the register of PLC changes it will automatically send an updated data to the user handset.
3. When the user wants to know the status of PLC. The user sends the short message to the PLC. The PLC will reply with the status of the OUTPUT.

IX. WEB INTERFACE

A typical HTTPS based web server is build using the Ethernet library of microcontroller. To send a request HTTP program establish a TCP connection to the HTTP server .The web server with HTTP protocol stack, will be handling HTTP requests which mainly deals with sending HTML for display in a web browser and it also shows static web pages that allow the user to control the I/O of PLC.

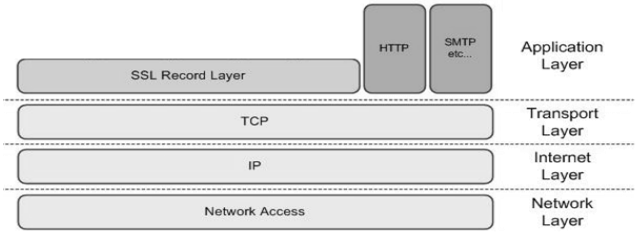

Fig. 7: TCP/IP model without SSL

A. ENCRYPTION AND AUTHENTICATION

To achieve a secure communication on computer network, and also on Internet Hypertext Transfer Protocol Secure (HTTPS) is used. Technically, it is not a protocol in itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS (Secure Socket Layer (SSL) or Transport Layer Security (TLS) Protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

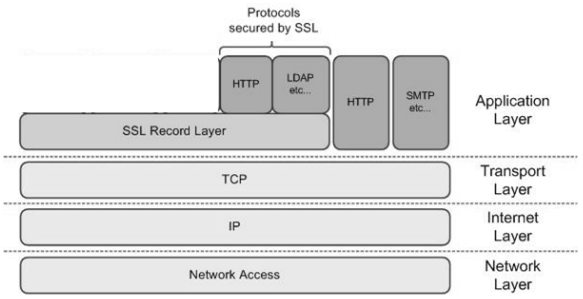

Fig. 8: added SSL sub-protocols in the TCP/IP model

As shown in the figure-8 everything in the HTTPS message is encrypted in the lower sub layers of application layer, including the headers, and the request/response load. So the attacker can only know the fact that a connection is taking place between the two parties, already known to him, the domain name and IP address

B. SCREEN SHOT OF THE WEBSERVER

This System has been has been tested with MICROLOGIX - 1400 SERIES A MODEL NO- 1766-L32BXB type PLC. The microcontroller is ARDUINO MEGA 2560, GSM modem is SIM 3OO and the Ethernet module is Enc28J60.

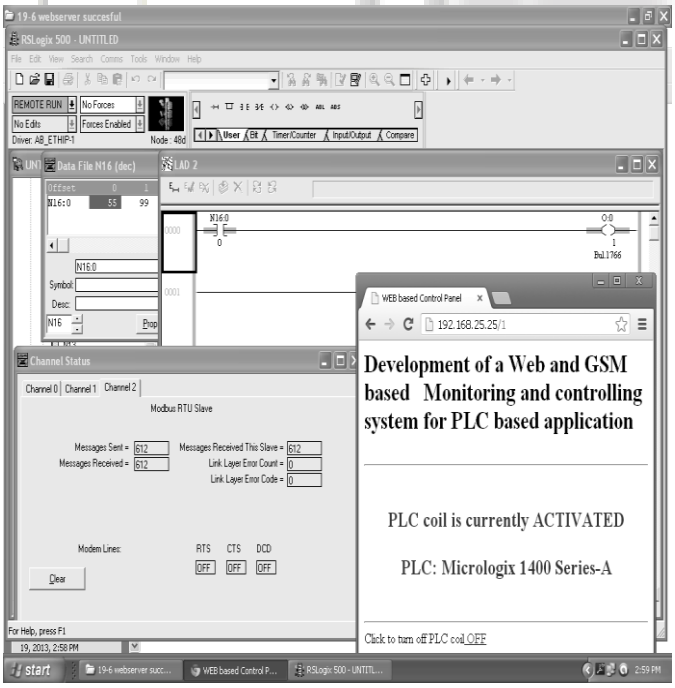

Fig. 9: implementation of web server and software environment of PLC

X. ANALYSIS OF RTT

The round trip time for the packets has been analysed using network analyser which is given below.

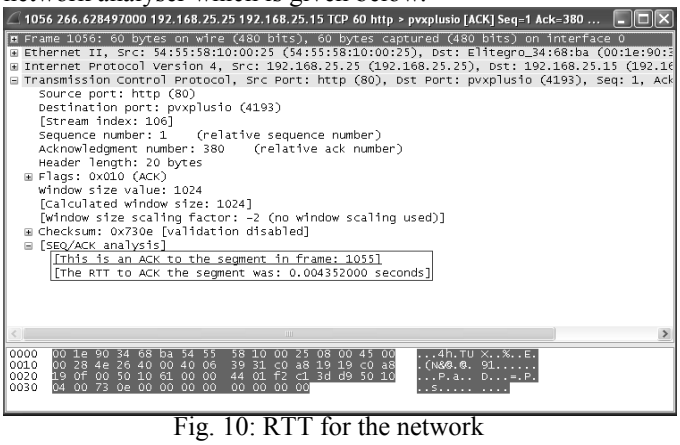

Fig. 10: RTT for the network

XI. CONCLUSION

This system is beneficial over the traditional system in terms of remote monitoring, control and maintenance. The system also reduces the technical requirement for monitoring and diagnosis in enterprises. And the presence of two options allows users to control the PLC through either GSM or through internet. But controlling through internet offers enough security using RSA encryption with the help of SSL over HTTPS protocol as compared to GSM ciphering by the telecom operator.

REFERENCES

[1] Zafer Aydogmus, Omur Aydogmus, "A Web-Based Remot `Access Laboratory Using SCADA", IEEE Transactions on education, Vol. 52, No. 1, February 2009, pp. 126-132.

[2] H. Kleines, J. Sarkadi, F. Suxdorf, K. Zwoll, Measurement or rea Time Aspects of Simatic PLC operation in the context of physics experiments,IEEE Transactions on Nuclear Science 51 (3) (2004)

[3] R. Kirubashankar, K. Krishnamurthy, J. Indra, B.Vignesh "Design And Implementation of Web Based Supervisory Control and Information System" International Journal of Soft Computing and Engineering (IJCSE) ISSN: 2231-2307, Volume -1, Issue-4, September 2011

[4] Xin Zhao , Wei Liang , "Research on the Remote Monitoring And Intelligent Fault Diagnosis System ", Sch. Of Computer & Electronic Eng., Hunan University of Commerce, Changsha, Wireless Communication, Networking and Mobile Computing(WiCOM'08),2008 pp.1-4.

[5] K. T. Erickson, "Programmable logic controllers," IEEE Potentials , vol.15, pp. 14–17, Feb./Mar. 1996

[6] http://www.arduino.cc/en/Main/ArduinoBoardMega

[7] ab.rockwellautomation.com/Programmable.../MicroLogix-1400 [

[8] K. T. Erickson, "Programmable logic controllers," IEEE Potentials, vol.15, pp. 14–17, Feb./Mar. 1996.

