TELKOMNIKA, Vol.11, No.4, December 2013, pp. 819~826
ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v11i4.1928

A Review of Communication Protocols for Intelligent Remote Terminal Unit Development

Mohd Ruddin Ab Ghani[1*], Wan Nor Shela Ezwane W. Jusoh[1], Mohd Ariff M.Hanafiah[1], Siti Hajar Raman[1], Zanariah Jano[2]
[1]Faculty of Electrical Engineering, [2] Centre for Languages and Human Development,
[1,2]Universiti Teknikal Malaysia Melaka (UTeM), 76100, Durian Tunggal, Melaka, Malaysia
*Corresponding author, e-mail: dpdruddin@utem.edu.my

Abstrak

Makalah ini menelaah semua kemungkinan protokol komunikasi antarmuka untuk unit terminal jarak jauh (RTU). Sistem "Supervisory Control dan Data Acquisition" (SCADA) adalah stasiun sentral yang dapat berkomunikasi dengan jaringan lain yang menggunakan protokol ini. Pada dasarnya, arsitektur dari semua jaringan didasarkan pada tujuh lapisan interkoneksi sistem terbuka (OSI) dan International Standard Organization (ISO). Tujuan perancangan protokol ini adalah untuk memeriksa status semua perangkat input dan output di lapangan dan membuat laporan yang sesuai dengan status saat ini. Protokol dan parameter komunikasi yang sesuai antara piranti penghubung akan dimasukkan dalam merancang sebuah sistem SCADA yang kompleks. Protokol yang tersedia untuk mengembangkan komunikasi RTU adalah Modbus/ASCII, protokol jaringan terdistribusi (DNP3), controller area network (CAN), International Electro-technical Commission (IEC 60870), dan protokol kendali transmisi/protokol internet (TCP/IP).

***Kata kunci**: SCADA, RTU cerdas, protokol komunikasi, ISO, OSI*

Abstract

This paper reviewed all the possible interfacing communication protocols for remote terminal unit (RTU). Supervisory Control and Data Acquisition (SCADA) system is a central station that can communicate with other network using the protocol. Fundamentally, the architectures of all networks are based on the seven layers of open system interconnection (OSI) and International Standard Organization (ISO). The objective of designing the protocols is to check the status of all the input and output field devices and send the report according to that status. The corresponding protocol and communication parameters between the connecting devices will be included in designing a complex SCADA system. The available protocols to develop the communication of RTU are Modbus/ASCII, distributed network protocol (DNP3), controller area network (CAN), International Electro-technical Commission (IEC 60870), and transmission control protocol/internet protocol (TCP/IP).

***Keywords**: SCADA, Intelligent RTU, communication protocols, ISO, OSI*

1. Introduction

Supervisory control and data acquisition (SCADA) system consists of remote terminal unit (RTU), SCADA hosts, control process equipment and system from multiple locations, field devices monitor, and exchange data from various distributed control systems along the local and wide area network. The function of RTU in SCADA system is to collect the data gathered from remote side, based on data from sensor or other equipments [1]-[6]. Generally, the RTUs are able to transfer their configuration and control programs dynamically from several central stations. Several local programming units can be used to trigger the RTUs. The basic peer-to-peer communication can possibly communicate among RTUs. Designing a complete communication system is the first task before deciding on a physical communication technology for distribution automation (DA). A few of the most common protocols used for DA are:

- Modbus /ASCII:

Modbus is an open serial (RS-232 or RS-485) protocol derived from the master/slave architecture. It is a widely accepted protocol due to its ease of use and reliability. Modbus, an application layer messaging protocol, provides Master-Slave communication between devices linked through buses or networks. On the OSI model, services can be specified by function codes. The function codes of Modbus are elements of Modbus request/reply PDUs (protocol

Received July 23, 2013; Revised October 8, 2013; Accepted October 26, 2013

data units). In ASCII format, the messages are readable and encoded with hexadecimal value, represented by comprehensive ASCII characters. The characters used for this encoding are 0…9 and A…F. For every byte of information, two communication-bytes are used because every communication-byte can only define 4 bits in the hexadecimal system [7].

- Distributed network protocol (DNP3):

To recover historical data and record incidents, DNP3 is used as it is a reliable and practical communication protocol. The benefit of using DNP3 is it will decrease rate of accidents by handling with ease the events of emergencies and real time data which are transferred from server to master computer. Besides, the problem of channel jam can be solved by the link data layer DNP3 protocol because it supports emergent data transmission [8].

- Controller area network (CAN):

CAN is the best choice in industrial embedded networking for it is economical and represents a higher-layer protocol. CAN is a proven protocol with an extremely high level of reliability and its dominance in a fieldbus system for the embedded solution [9].

- International electro-technical commission (IEC 60870):

International Electro-technical Commission (IEC) is developed for Tele-control Unit. The accuracy of history events log built by master station is based on various measures from specified time synchronization and confirmation message. Data are reported spontaneously without any request from master station because it has a permit device to give the data different priorities [10].

- Transmission control protocol/internet protocol (TCP/IP):

A TCP/IP protocol consists of a layered architecture where each layer describes several functionalities which can be supported by a protocol. The responsibility of each layer often has more than one protocol options. TCP/IP consists of four layer systems namely Data Link Layer, Transport Layer, Application Layer, and Network Layer [11].

2. Communication Protocols Architecture

Communication is a transmission of information among points of origin and point of reception without altering the sequence or structure of the information content. Data communication involves the exchange of digitally encoded information between two devices through transmission media. Data communication in SCADA is more important than before because systems are becoming more distributed. The quality of SCADA information depends on whether real time information is complete, accurate, timely and reliable and supervisory control must be secure, reliable and timely as well. Figure 1 shows the data communication components:

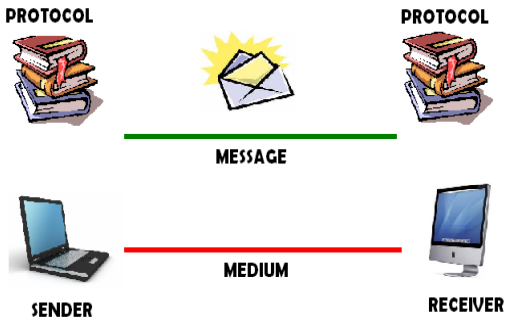

Figure 1. Data Communication Components

2.1. Modbus/ASCII

Traditional RS-232, RS-422, RS-485 and Ethernet services are supported by Modbus protocol which is composed of ASCII, RTU, and TCP transmission mode. While ACII mode or RTU mode uses serial port Modbus device, Modbus/TCP mode uses Ethernet device. The communication parameters and transmission mode must be equal to all devices in Modbus network.

The data structure, command, message and the way how to respond are regulated by Modbus protocol. First, Master sends a message and slave receives the message. Then, the message response is created and is sent back to the master to respond to the query. The data of slave can be modified directly by master through messages.
When using Modbus protocol to communicate, the message and address can be identified by the structure of Modbus message which determines that every controller has only one device address. Controller will create a response if the master needs it then send it to the query using Modbus protocol. Figure 2 is a standard Modbus Master/Slave Query-Response Cycle.

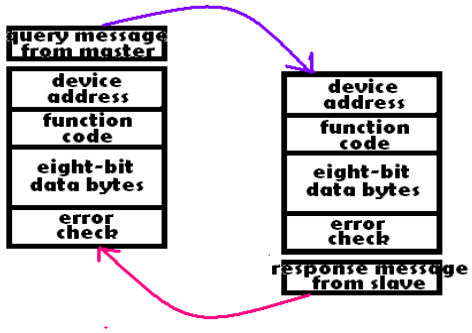

Figure 2. Cycle of Modbus master-slave query-response [12]

Table 1 . Comparison of ASCII and RTU [7]

	ASCII	RTU
Transmission efficiency	Low	High
Program processing	Direct, easy for debugging	Indirect, slightly complex
Start bit	1	1
Data bits	7	8
Character	ASCII 0…9 and A…F	Binary 0…255
Parity with stop bit	Even/odd =1, none=2	Even/odd =1, none=2
Error check	LRC Longitudinal Redundancy Check	CRC Cyclic Redundancy Check
Frame start	Character ':'	3.5 chars silence
Frame end	Character CR/LF	3.5 chars silence
Gaps in message	1 sec	1.5 time char length

Data have to be checked by the Modbus protocol. LRC is used to check ASCII mode whereas 16 bit CRC to check the RTU mode. TCP protocol is a connection-oriented reliable protocol and TCP mode is not necessary to undergo an extra check. Table 1 is a comparison between ASCII mode and RTU mode. The data transmission efficiency of ASCII mode is lower compared to RTU mode. Hence, RTU mode is needed in order to send a large volume of data.

2.2. Distributed network protocol (DNP3)

The DNP3 is a protocol used for facilitating communication between SCADA systems and devices such as RTUs. The development of DNP3 standards enables easy and reliable interoperability between nodes in a SCADA system. DNP3 is an open, robust, intelligent and effective modern SCADA protocol. It can

- allow multiple masters and peer-to-peer operations.
- segment message into multiple frames to ensure excellent error detection and recover.
- respond without request (unsolicited).
- request and respond with multiple data type in single messages.
- allow user to define objects including file transfer.
- assign priorities to data items and request data item periodically based on their priority
- include only changed data in response message.
- support time synchronization and standard time format.

The DNP3 is also known as a layered architecture protocol. DNP3 adheres to the simplified three layer standards proposed by the International Electro-technical Commission (IEC) rather than adheres to the Open System Interconnection (OSI) seven layer protocols for

basic implementation [13]. IEC refers this as the Enhanced Performance Architecture (EPA). EPA is enhanced by DNP3 by adding a fourth layer to allow the message segmentation, and this layer is called a pseudo-transport layer.

In DNP3, data is structured into data types. Each data type is an object group, including:

- Analog output (multiple-bit values whose status may be read, or that may be controlled directly or through Select-Before-Operate (SBO) type operations).
- Counters.
- Analog input (multiple-bit read-only values).
- Binary output (single-bit value whose status may be read, or that may be pulsed or latched directly or through SBO type operation).
- Binary input (single-bit read-only values).
- File transfer objects.
- Time and date.

A typical Experion DNP3 architecture is shown in Figure 3.

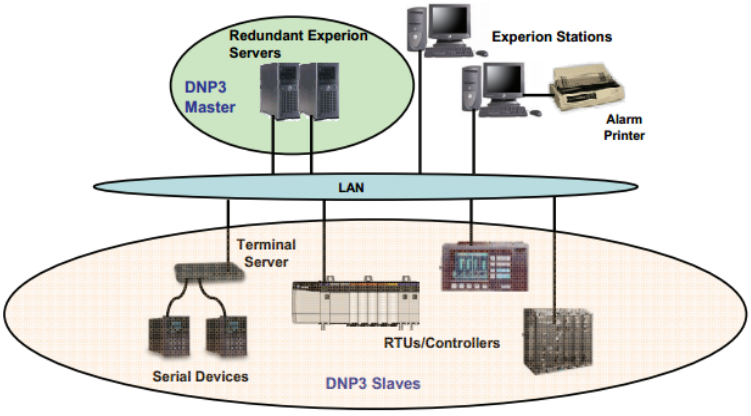

Figure 3. Experion DNP3 architecture [14]

The benefits of Experion DNP3 interface are its adherence to the standard-based protocol which enables easy integration and provides flexibility and functionality that exceeds conventional communication protocols. Besides, the infrastructure such as alarms and events, trends, historization and Distributed System Architecture generates ease of engineering and maintenance. The powerful protocol features make the communication interface efficient and robust.

2.3. Controller area network (CAN)

In CAN message format, the sensor data is sent over the RTU bus. This section reviews CAN protocol developed by Robert Bosch who has been designing a real time networks [15]. In various real time application, CAN protocol would be a standard factor to connect the electronic control units [16].

CAN has a number of advantages than Ethernet TCP/IP. It is used as fieldbus systems for embedded solutions. Their benefits include

- very low resource requirement.
- low cost implementation.
- no message collision.
- extreme Reliability and Robustness.
- very short error recovery time.
- real time application design.

However, CAN has also some limitation on its performance and the most significant is that it has limited network length in which the baud rate is ~120 feet at 1Mbit/sec. The disadvantages include

- limited bandwidth.
- limited network length (depending on baud rate).
- limited baud rate of 1Mbit/sec.

Figure 4 shows the relationship between baud rate and supported network length:

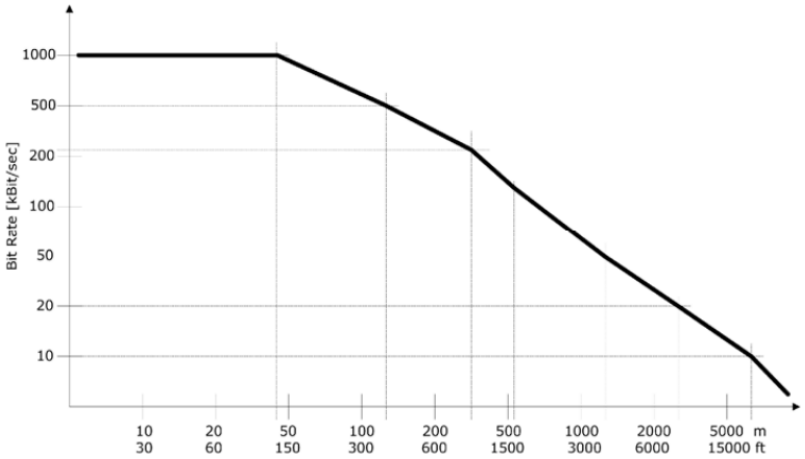

Figure 4. Relation between baud rate and supported network length [10]

2.4. Transmission control protocol/internet protocol (TCP/IP)

Addressing, packaging and routing function are the responsibilities of Internet layer. Internet layer is slightly similar to the network layer of the OSI model. IP, ARP, ICM and IGMP are core protocols of the Internet layer which are shown in Table 2.

The Host-to-Host Transport layer is also known as the transport layer. It provides the datagram communication services and application layer with session. The transport layer covers the responsibilities of the OSI Transport layer and some of the responsibilities of the OSI Session layer. TCP and User Datagram Protocol (UDP) are core protocols of the Transport layer. While this is shown in Table 3, Figure 5 shows the TCP/IP protocol architecture.

Table 2. Detail of core protocol of Internet Layer [17]

Internet Layer	Detail
Internet Protocol (IP)	The responsibility of routing and the fragmentation, IP addressing and reassembly of packets is under routable protocol.
Address Resolution Protocol (ARP)	The hardware address is the example of responsible for the resolution of the internet layer address to the Network Interface layer address.
Internet Control Message Protocol (ICMP)	Responsible for reporting errors due to the unsuccessful delivery of IP packet and providing diagnostic functions.
Internet Group Management Protocol (IGMP)	Responsible for the management of IP multicast groups.

Table 3 . Detail of core protocol of Transport layer [17]

TCP (Transmission Control Protocol)	**UDP (User Datagram Protocol)**
TCP is responsible for the sequencing and acknowledgement of packet sent, the recovery of packets lost during transmission, and the establishment of a TCP connection. It provides a one-to-one connection-oriented and reliable communications service.	UDP is used when the small amount of data transferred such as the data that would fit into a single packet, when the overhead of establishing a TCP connection is not desired or when the applications of upper layer protocols provide reliable delivery. Provides a one-to-one or one-to-many, unreliable communication service and connectionless.

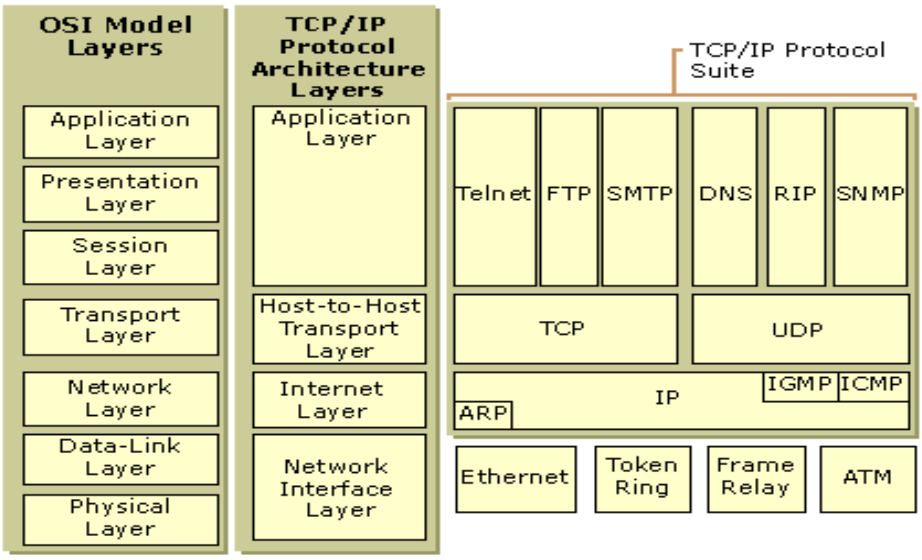

Figure 5 . TCP/IP protocol architecture [17].

The advantages of TCP/IP are as follows:

- Proficient bandwidth usage: IP is based on datagram technology. Packet switching utilizes bandwidth efficiently than circuit switching for non-constant bit rate.
- Service Integration: IP handles data and streaming media. It reduces the number of links needed.
- Reliable: IP transports layer by design which offers an inherently reliable transmission.
- A living and proven technology: IP technology is always evolving to constantly cater for the needs of many classes of applications.

3. Results

This section covers how to select a suitable communication protocol for Intelligent RTU.

3.1. Intelligent RTU features

The intelligent RTU communication protocol on a 2 or 4 RS485 wire has the following basic features [18]:

- 8-bit ASCII based protocol allows simple terminals and terminal emulators to poll/test remotes.
- Explicit use of message re-sync character allows positive identification of message start and multiple types of RTUs residing on the same network.
- Up to 16 RTUs can reside on a single line (4bit address) and up to 16 commands can be defined (4bit command identifier).
- Up to 16 digital inputs, digital output, analogue input and counters per RTU.
- Up to 15 different model (types) of RTU on a single communication line.
- Up to 15 preset configurations of RTU.
- Up to 8 alarms per RTU type can be defined.
- Pulsing of digital output (0.5-8s on time, increments of 0.5s) with single command.
- Ability to read and write configuration table pages in EEPROM.

3.2. ASCII protocol design

The central controller is a master for the control network and the slave nodes (or device net) are represented by all RTUs. The different areas can be identified and distributed by different stations. The protocol comes from the query/respond transaction of master-slave. This paper presents a protocol design in TEXT ASCII and the operation starts with a command that always waits for query from a computer and a response command will be responded by the

node as illustrated in Table 1. The computer command and the RTU response command is shown in Figure 6.

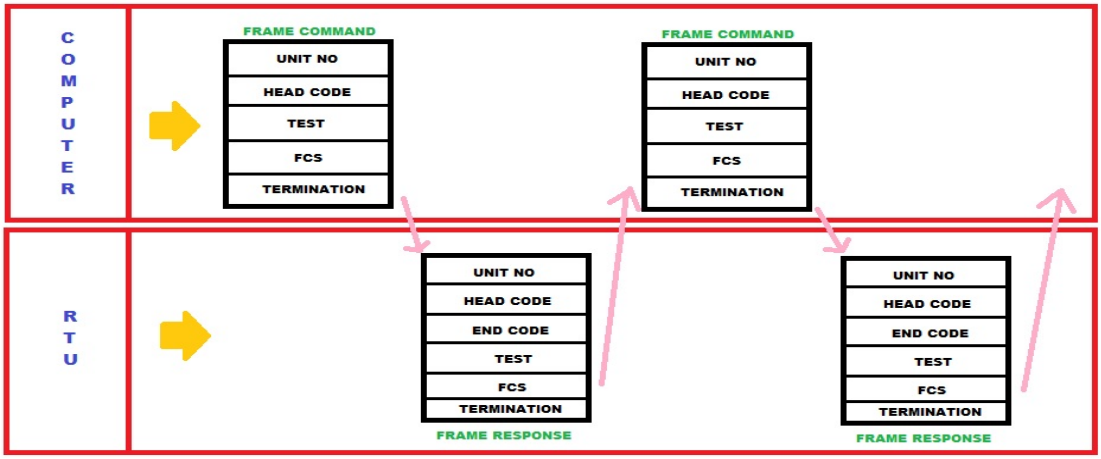

Figure 6. Computer command and RTU response command [18].

3.3. Hyperterminal views

The result of this method will be displayed on Hyperterminal interface. Table 4 shows the command and response command .

Table 4. Command and response command

Commands	Request Syntax	Response Syntax
PING	['#'][addr]['0'][bit][<CR>]	['$'][addr]['0'][RTUtype][RTUconfig][<CR>]
SCAN_DI	['#'][addr]['1'][bit][<CR>]	['$'][addr]['1'][DI3:0][DI7:4][DI11:8][<CR>]
SCAN_AI	['#'][addr]['2'][channel][<CR>]	['$'][addr]['2'][channel][AI3:0][AI7:4][<CR>]
SET_DO_BIT	['#'][addr]['3'][bit][state][<CR>]	['$'][addr]['3'][status3:0][status7:4][<CR>]
SET_DO_NBL	['#'][addr]['4'][nibble][state][<CR>]	['$'][addr]['4'][status3:0][status7:4][<CR>]
SET_DO_BYTE	['#'][addr]['5'][byte][state_LSn][state_MSn][<CR>]	['$'][addr]['5'][status3:0][status7:4][<CR>]
PULSE_DO_BIT	['#'][addr]['6'][bit][time_on][<CR>]	['$'][addr]['6'][status3:0][status7:4][<CR>]
SCAN_DO_BYTE	['#'][addr]['7'][byte][<CR>]	['$'][addr]['7'][byte][D0_LSn][D0_MSn][<CR>]
READ_STATUS	['#'][addr]['8'][<CR>]	['$'][addr]['8'][status3:0][status7:4][<CR>]
RESET_ALARM	['#'][addr]['9'][bit][<CR>]	['$'][addr]['9'][status3:0][status7:4][<CR>]

4. Conclusion

In conclusion, existing communication protocols of Remote Terminal Unit for the design architecture from user's insight are reviewed in this paper. The distributed network protocol supports only the data link layer, physical layer and application layer within the open system interconnection model. The physical layer is the least supported. In general, the future of Distribution Automation communication will be more intelligent and move to the pole-top, and these smarter devices will be communicating peer-to-peer to implement an advanced auto-restoration algorithm. Thus, the result of this study indicates that the selection of the communication protocol will affect the development of RTU.

Acknowledgements

The authors would like to thank the Ministry of Education, Government of Malaysia and the Universiti Teknikal Malaysia Melaka (UTeM) for funding this study.

References

[1] M.M Ahmed, W.L Soo, M. A. M. Hanafiah and M. R. A. Ghani., Development of Customized Distribution Automation System (DAS) for Secure Fault Isolation in Low Voltage Distribution Automation in Luiz Affonso Guides (Ed), Programmable Logic Controller, (Rijeka, Crotia, In Tech, 2010) 131-150.

[2] M.M Ahmed, W.L Soo, M. A. M. Hanafiah and M. R. A. Ghani, Customized Fault Management System for Low Voltage (LV) Distribution Automation System in Wei Zhang (Ed*)*, Fault Detection (Rijeka, Crotia, In Tech, 2010) 51-70.

[3] W.N.S.E Wan Jusoh, M.A.M. Hanafiah, M.R.A. Ghani, S.H.Raman, *Remote Terminal Unit (RTU) Hardware Design and Implementation Efficient in Difference Application*. 2013 IEEE 7th International Power Engineering and Optimization Conference (PEOCO), Langkawi Malaysia, 3-4 June 2013, 570-573.

[4] W.N.S.E Wan Jusoh, M.A. Mat Hanafiah, M.R. Ab. Ghani, A. Jidin, S.H. Raman, *Development of Remote Terminal Unit (RTU) for the New Function of Distribution Automation System (DAS)*. Power and Energy Conversion Symposium (PECS 2012*).* Melaka Malaysia, 17 December 2012, 310-312.

[5] S.H. Raman, M.R. Ab. Ghani, Z.A. Bharudin, M.A.M. Hanafiah, W.N.S.E. Wan Jusoh, *The Implementation of fault Management in distribution Automation System Using Distribution Automation System (DAS) in Conjunction with SCADA*. Power and Energy Conversion Symposium (PECS 2012), Melaka Malaysia, 17 December 2012, 305-309.

[6] M.M Mat Hanafiah,S.H. Raman, W.N.S.E. Wan Jusoh, M.R. Ab Ghani, Z.A. Baharuddin, Development of a Novel Fault Management in Distribution System using Distribution Automation System in Conjunction with GSM Communication. *International Journal of Smart Grid and Clean Energy*. 2013; 2(3): 330-335.

[7] John Rinaldi, *An Introduction to Modbus RTU addressing, Function Code and Networking*, 2010.

[8] Ling Cheng, *Study and Application of DNP3.0 in SCADA System*. 2011 International Conferences on Electronic & Mechanical Engineering and Information Technology, 12-14 August 2011, 4563-4566.

[9] Wilfried Voss, *The Future of CAN/CAN open and the Industrial Ethernet Challenge*, President esd electronics, Inc USA, 2011.

[10] Sanchez. Using Internet Protocols to Implement IEC 60870-5 Tele-control Functions. IEEE Transactions on Power Delivery. 2010; 25(1): 407-406.

[11] Himanshu Arora. *TCP/IP Protocol Fundamental Explained with a Diagram*. 2011.

[12] Daogang Peng, Hao Zhang, Jiannian Weng, Hui Li, Fei Xia., *Design and Development of Modbus/RTU Master Monitoring System Based on Embedded PowerPC Platform.* IEEE International Symposium on Industrial Electronic (ISIE 2009). Seoul Olympic Parktel, Seoul, Korea, July 5-8, 2009, 2148-2152.

[13] Rao Kalapatapu. *Scada Protocol and communication trends, The Instrumentation System and Automation Society*. Presented at the ISA 2004, 5-7 October 2004, Reliant Center Houston, Texas, 2004.

[14] Product Information Note Experion DNP3 Interface, Jun 2009.

[15] Bosch, CAN specification Ver 2.0, Robert Bosch GmbH, Stuttgart, Germany, Chuck Power Motorola MCTG Multiplex Application, 5 April 1995.

[16] Sanjay Gupta, CAN facilities in Vehicle Networking, SAE paper 900695, 1995, pp. 9-16.

[17] Mei Yang, Protocol Architecture TCP/IP and Internet Based Application, 25 August 2013.

[18] Suphan Gulpanich, Arjin Numsomran, Vittaya Tipsuwanporn, Kitti Tirasesth. *Distributed control of Network devices with Remote Terminal Unit*. IEEE International Conference on Industrial Technology (ICIT 2005). Hong Kong. 2005: 823- 828.