Application of a New SS7-SIGTRAN Protocol Interchanger Software and Hardware in the Communication between Remote Terminal Units (RTU) and Supervisory Control and Data Acquisition System (SCADA)

Md. Junayed Sarker[1], Hamza Kadir[2], Nafis Kabir[3], M. Aminul Islam[4], Moinul Momen[5]

[1]Department of EEE, Ahsanullah University of Science and Technology, Dhaka, Bangladesh.
[2]Department of EEE, Islamic University of Technology, Dhaka, Bangladesh
[3]Department of EEE, Bangladesh University of Engineering and Technology, Dhaka, Bangladesh.
[4]Department of CSE, Ahsanullah University of Science and Technology, Dhaka, Bangladesh.
[5]Department of Core Network Integration Engineer, LM Ericsson Bangladesh Ltd.

Summary
This proposal provides new Signaling System No. 7 (SS7) to IP based Signaling Transport (SIGTRAN) protocol interchanger software and hardware to implement an improved communication infrastructure connecting the supervisory system to the Remote Terminal Unit.

Key words:
SCADA, RTU, SS7, SIGTRAN

1. Background

Data and telecommunication form an essential part of a power system control (PSC) structure as broadband communication capabilities open up possibilities that were not realistic only a decade ago. These new possibilities should be exploited in a structured and efficient way, providing more effective power system operation, which in turn is a necessity for the power companies in a deregulated market. Hence, many new communication techniques can be applied through some extensive research work in Supervisory Control and Data Acquisition (SCADA) system to increase the efficiency and reduction of the cost of it.

2. Theoretical Framework

Remote data monitoring is required in many industries and applications such as oil & gas, power, waste treatment and environment monitoring. In these applications, a fairly large number of remote Terminal Units (RTUs) in remote and/or hazardous locations collect data from devices and send log data and alarms to a SCADA terminal in a central control room (CCR) [Figure 1]. Telemetry devices installed between the RTUs and the SCADA system send and receive the data. Some big concerns about using telemetry are cost (initial expenditure and communications fees) and communications stability. As the IT network infrastructure improves in remote areas, commodity network infrastructure can be more readily used in telemetry applications, reducing initial startup costs and affording relatively stable communications.

The present SCADA monitoring system uses microwave links for communication between RTUs and Sub-Master Station. Similarly for the communication between the Sub-Master Station and Master Station, again microwave links are used. This involves huge cost for the related microwave equipments and bandwidth rental cost. A more convenient and cost effective way will be to replace these microwave links by the nationwide SS7 or IP network. In my research work, I would like to develop such a software and related hardware which will replace these costly microwave links by the existing SS7 or IP network. The hardware namely E1 card, will be used to collect data from RTUs and transmit it to the Sub-Master Station via the existing SS7 network of the PSTN operators. Existing IP network will be used for the communication between the Sub-Master Station and the Master Station. A SS7 to SIGTRAN (IP) interchanger software will be developed for converting the SS7 data into IP based SIGTRAN data.

Manuscript received October 5, 2009
Manuscript revised October 20, 2009

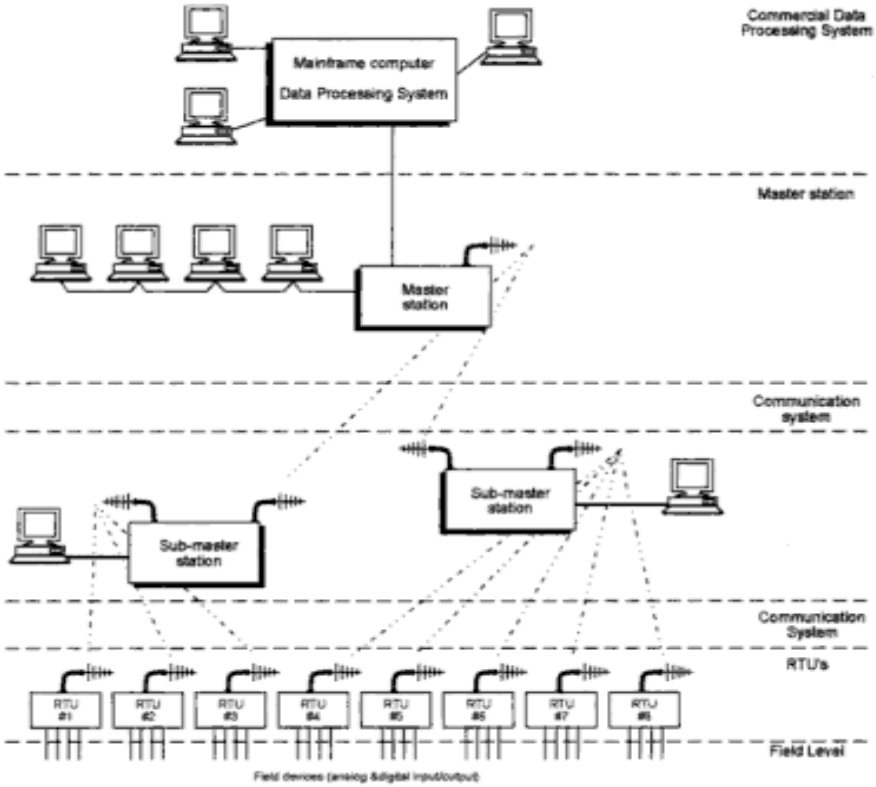


Fig 1. Typical SCADA system

3. Proposed Software Architecture

Protocol can be defined as the rules governing the syntax and synchronization of communication. We have worked with two protocols: SS7 and SIGTRAN.

Signaling System no. 7 (SS7) is a set of telephony signaling protocols [3], which are used in the telephone network. SS7 provides a universal structure for telephony network signaling, messaging, interfacing and network maintenance [4]. SIGTRAN is the name given to an IETF working group that produced specifications [5] for a family of protocols that provide reliable datagram service and user layer adaptations for SS7 and ISDN communications protocols. Our developed software along with our designed hardware is capable of taking data from telephone network and convert that to SIGTRAN protocol data defined by ITU-T [3][4][5]. Our developed software takes SS7 protocol data from SS7 network through designed USB E1 card then converts it to SIGTRAN data and transmits that data through Ethernet port. The working principle of our developed hardware and software is like,The first part of the development of our software was to develop the protocol stack of SS7 and SIGTRAN protocol.

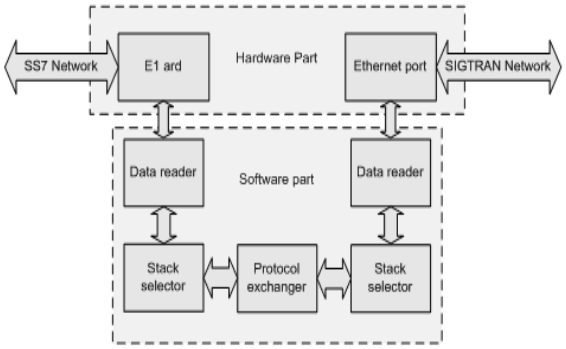


Fig. 2. Working principle of the proposed system

SS7 Stack: The SS7 protocol stack borrows partially from the OSI Model of a packetized digital protocol stack. OSI layers 1 to 3 are provided by the Message Transfer Part (MTP) of the SS7 protocol; for circuit related signaling, such as the Telephone User Part (TUP) or the ISDN User Part (ISUP), the User Part provides layers 4 to 7, whereas for non-circuit related signaling the Signaling Connection and Control Part (SCCP) provides layer 4 capabilities to the SCCP user [8].

Manuscript received October 5, 2009
Manuscript revised October 20, 2009

The MTP[11] covers the transport protocols including network interface, information transfer, message handling and routing to the higher levels. SCCP is a sub-part of other L4 protocols, together with MTP3 it can be called the Network Service Part (NSP), it provides end-to-end addressing and routing. TUP is a link-by-link signaling system used to connect calls. ISUP provides a circuit-based protocol to establish, maintain and end the connections for calls. TCAP is used to create database queries and invoke advanced network functionality mobile services (MAP), etc. [9]

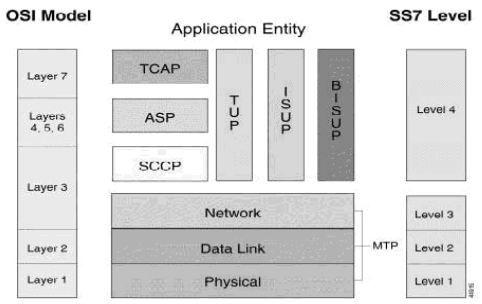


Fig. 3. SS7 protocol stack [8]

SIGTRAN Stack: The SIGTRAN protocols specify the means by which SS7 messages can be reliably transported over IP networks. The architecture identifies two components:

- A common transport protocol for the SS7 protocol layer being carried and
- An adaptation module to emulate lower layers of the protocol.

For example, if the native protocol is MTP (Message Transport Layer) Level 3, the sigtran protocols provide the equivalent functionality of MTP Level 2. If the native protocol is ISUP or SCCP, the sigtran protocols provide the same functionality as MTP Levels 2 and 3. If the native protocol is TCAP, the SIGTRAN protocols provide the functionality of SCCP (connectionless classes) & MTP Levels 2 & 3.

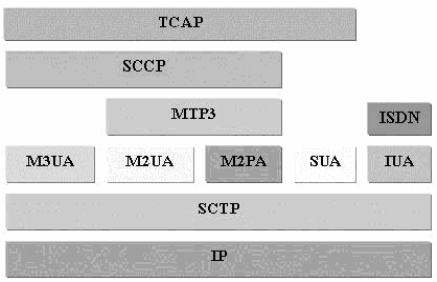


Fig 4. SIGTRAN protocol stack [10]

The task of the data exchange between SS7 and SIGTRAN protocol is performed according to the following structure,

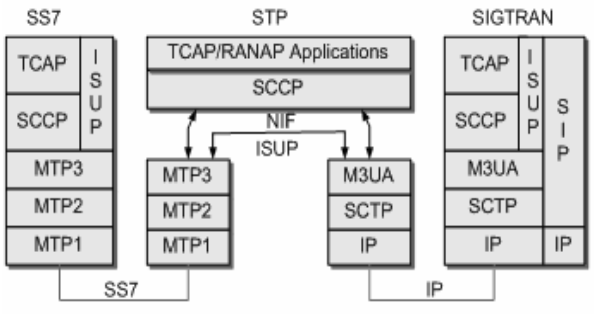


Fig. 5. SS7 and SIGTRAN protocol interconnection structure [13]

Our software exchanges SS7 protocol data via our designed USB E1 card and SIGTRAN protocol data from Ethernet port. This exchange of data between two different protocols takes place by analyzing the data [14] and maintaining the structure mentioned in figure 6. There are three part of the software which performs the data exchange operation. They are,

- Data reader
- Stack selector and
- Data exchanger

"Data Reader" window of our software is used to take SS7 data via E1 card or SIGTRAN data via Ethernet port. At first, the user has to specify the source to extract data for exchange. The selected source will be used as the base protocol which will be converted to the other protocol data. The software performing this task is shown below,

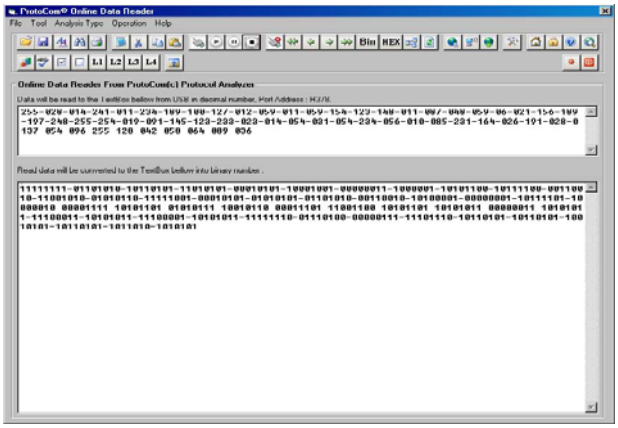


Fig.6."Data reader" window of our developed software

"Stack Manager" window of our software lets the user to choose which message in the SS7 data is to be exchanged.

It is very useful operation when the SS7 data length is very high. By choosing specific message, then user can reduce the number of exchanged messages so that only the desired message is transmitted. The software window of "Stack Manager" is shown below:

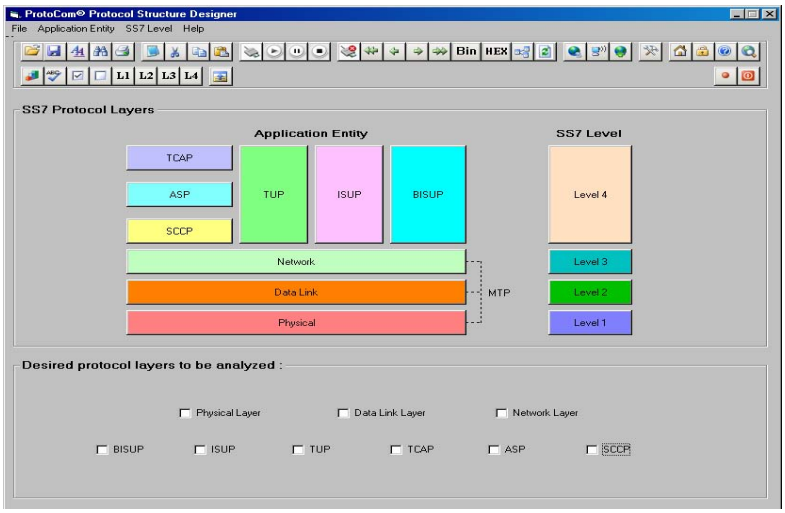


Fig.7. "Stack manager" window of our developed software

"Data Exchanger" is the last part of our software with which the selected portion of the base protocol is exchanged with other protocol. The software window performing data exchanging is shown bellow,

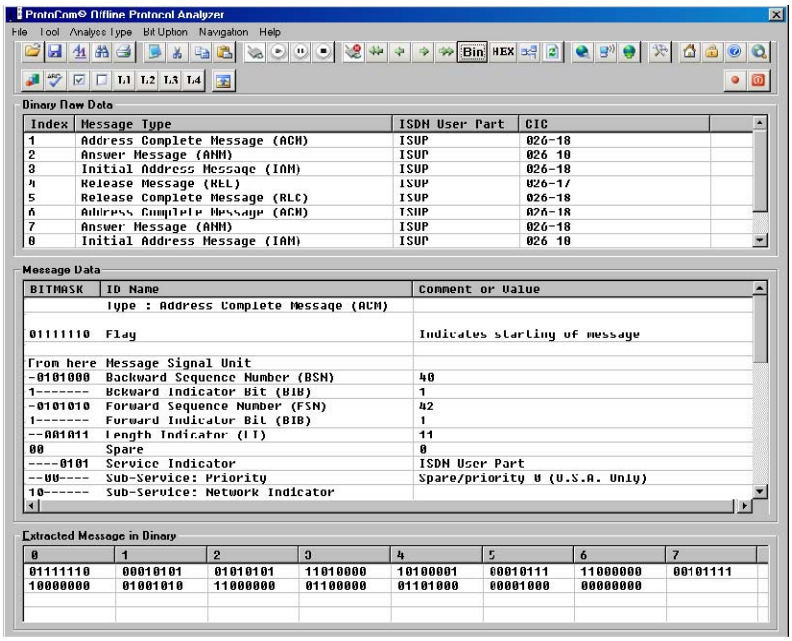


Fig.8. "Data exchanger" window of our developed software

4. Proposed Hardware Architecture

For reading data from SS7 link, we have designed a USB E1 card with which the data of signaling channel of SS7 link can be directly read to our developed software. Our USB E1 card is an enhanced third-generation hardware that consolidates the essential pieces of industry-standard test equipment into a powerful, PC-Based USB E1 solution.

PEF2256: The FALC56 is the latest addition to Infineon's FALC® family of sophisticated E1/T1/J1 framer and Line Interface Unit (LIU) transceivers which supports all standard E1/T1/J1 functions. [16]

ATmega16: The ATmega16 is a low-power CMOS 8-bit microcontroller based on AVR enhanced RISC architecture, which achieves 1 MIPS/MHz throughput allowing optimization of power consumption. [17]

FT245BM: The FT245BM is the 2nd generation of FTDI's popular Single Chip USB Parallel FIFO bi-directional Data Transfer I.C. The FT245BM provides an easy cost-effective method of transferring data to / from a peripheral and a host P.C. at up to 8 Million bits (1 Megabyte) per second. [18]

74HC244: These octal buffers and line drivers are designed specifically to improve both the performance and density of 3-state memory address drivers, clock drivers, and bus-oriented receivers and transmitters.

Using these ICs we have designed the USB E1 card. For avoiding complex PCB, we have designed the E1 card in two parts. They are,

1. **Transceiver module**: It includes transceiver IC, synchronizing clock, impedance matching transformer, transient voltage suppressor and connector for E1 link.
2. **Controlling module**: It includes microcontroller, USB interface, clock, serial and Parallel interface and power supply unit.

The schematics of the controlling and transceiver module are shown bellow:

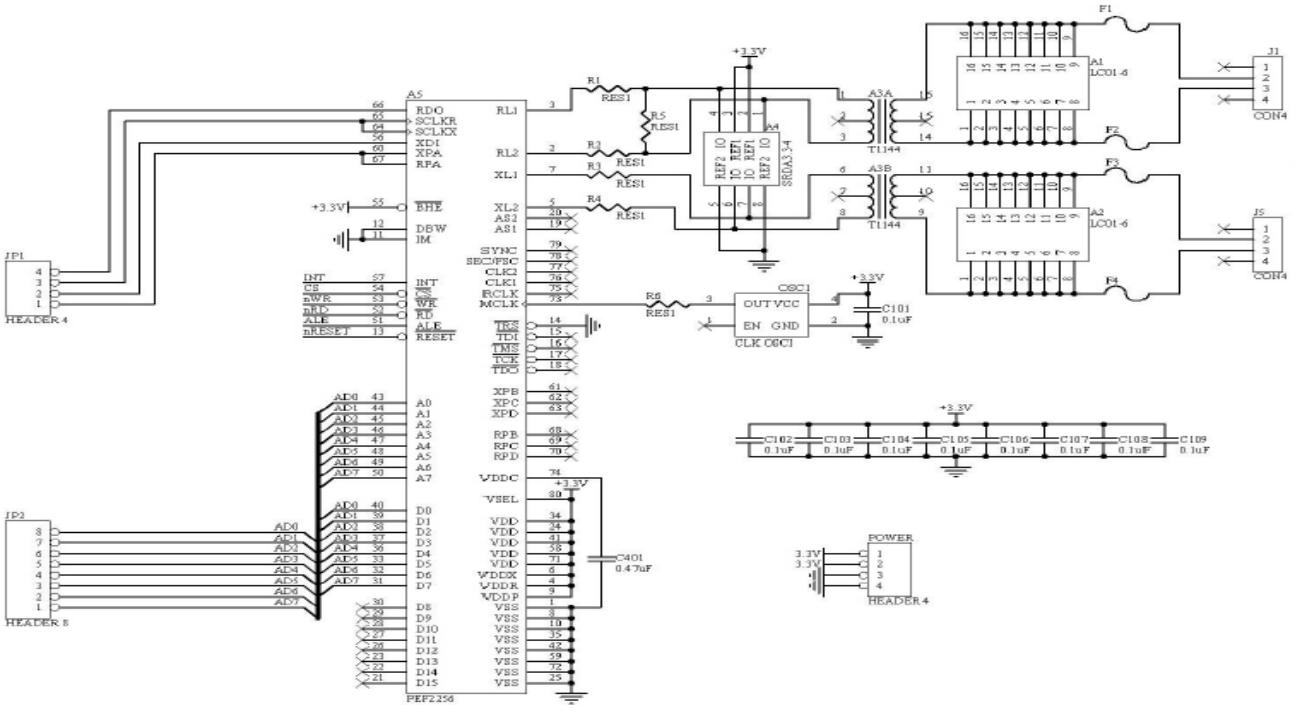


Fig. 9 Transceiver module of the E1 card

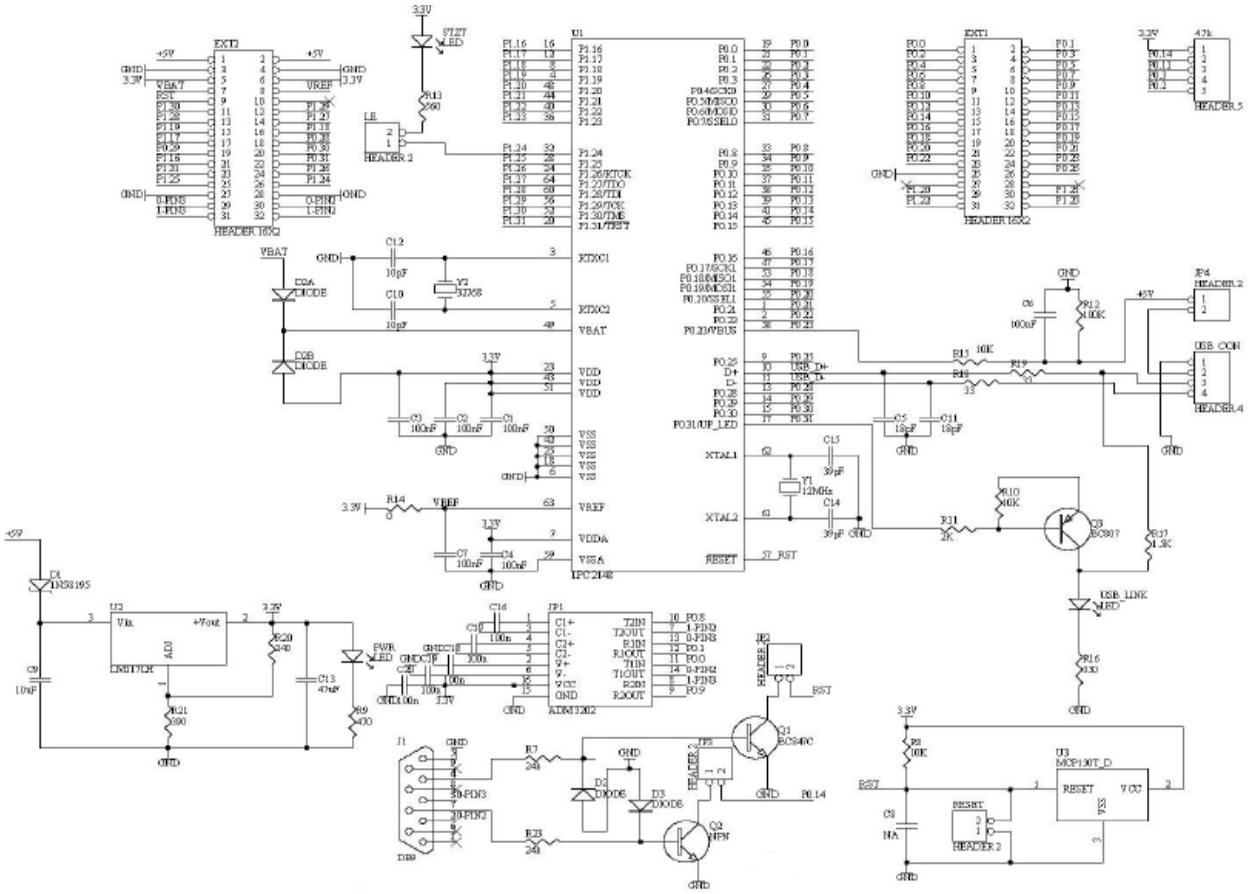
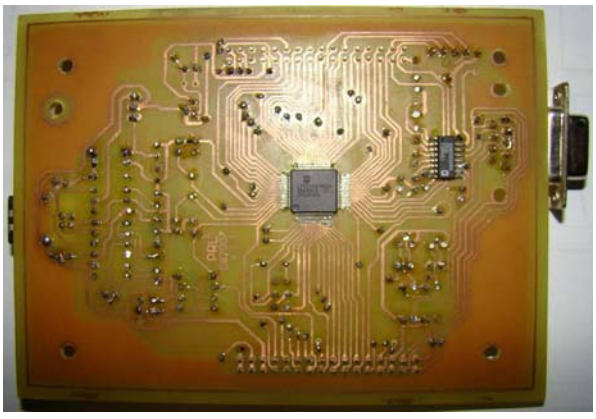


Fig. 10 Controlling part of the E1 card.

5. Current status

The hardware designing part is completed and a prototype is accomplished. Now, I would like to modify this hardware so that it can be used with my proposed system.

(a)



(b)

Fig. 11 (a) Top and (b) Bottom layer of the designed PCB of the E1 card

SS7 and SIGTRAN data can be read [Figure 5] according to the selected structure [Figure 6] and exchanged using our hardware and software [Figure 7] successfully. This shows that the interfacing of SCADA network and IP network can be done successfully. One of the major achievements of our work is the tremendous reduction of the cost. The manufacturing cost of the hardware is very minute compared to the market price of similar range hardware. A PCI slot E1 card costs about $500 in the current market whereas our hardware costs only $35.

Acknowledgement:

We would like to highly acknowledge Shirajum Munir, G M A Ehsanur Rahman and Nizamuddin for their technical support regarding the schematics and simulation.

Reference

[1] Practical Modern SCADA Protocols By Gordon R. Clarke, Deon Reynders, Edwin Wright
[2] Communications Technology Guidelines for EMS/SCADA Systems By Donald J. Marihart, Fellow, IEEE
[3] ITU-T Recommendations, Q.700 to Q.716.
[4] Fred Halsal, Multimedia communication.
[5] IETF reference document "Framework Architecture for Signaling Transport", RFC-2719, http://www.ietf.org/rfc/rfc2719.txt.
[6] Performance Technologies protocol standard document. www.pt.com.
[7] Chukarin, A. Pershakov, N. Samouylov. 'Performance of Sigtran-based Signaling Links Deployed in Mobile Networks.' ConTel 2007.
[8] Dawis, E.P. 'Architecture of an SS7 protocol stack on a broadband switch platform using dualistic Petri nets.' Communications, Computers and signal Processing, 2001. PACRIM.
[9] ITU-T reference document Q.701, Page 5.
[10] "Tutorial on Signaling System 7 (SS7)" from Performance Technologies, Page 6. www.pt.com.
[11] ITU-T reference document Q.700 page 14.
[12] SIGTRAN Protocol Suite by Jim Darroch, Page 8.
[13] Reference document on "SS7 over IP signaling transport and SCCP" by International Engineering Consortium, Page 16. www.iec.org.
[14] Signaling System # 7 protocol analyzer software. www.gl.com/ss7.html.
[15] GL communication protocol analyzer software standard www.gl.com/protocol_analysis.html.
[16] Falc2256 product brief of Infenion Technologies, Page 1. www.infenion.com.
[17] ATmega16L Datasheet from ATMEL Corporation. Page 1. www.atmel.com.
[18] FT245BM datasheet from Future technologies Ltd. Page 1. www.ftdichip.com
[19] A New SS7-SIGTRAN protocol Interchanger Software and Hardware to Implement an Improved Distributed Database Based ATM Network Using Existing IP Network By M. S. Munir, K.Ahmed, A. S. M Shihavuddin, M. J. Sarker.

Md. Junayed Sarker received B.Sc. in Electrical and Electronic Engineering degree from Islamic University of Technology (IUT) in 2007. Currently he is working as a Lecturer in the Department of Electrical and Electronic Engineering at Ahsanullah University of Science and Technology (AUST), Dhaka, Bangladesh. He worked for LM Ericsson Bangladesh Limited in the department of Radio Access Network (RAN) as a services engineer.

Hamza Kadir received his B.Sc. Engg. Degree in Electrical and Electronic Engineering from Islamic University of Technology (IUT) in October, 2007. Currently he is working at AREVA T&D Bangladesh, NLDC (National Load Dispatch Centre) Project. It is a Supervisory Control and Data Acquisition (SCADA) deployment project for 104 Grid Stations (including 22 power stations) of Power Grid Company of Bangladesh (PGCB), the semi-government organization for the Country Power Grid.

Nafis Kabir is a student of M.Sc. in Electrical and Electronic Engineering (EEE) discipline in Bangladesh University of Engineering & Technology (BUET). He received his graduation from Islamic University of Technology (IUT) in 2007. Alongside study, he is working as Training Executive in the Faculty of Avionics in Bangladesh Airlines Training Centre (BATC), a subsidiary organ of Biman Bangladesh Airlines Ltd.

M. Aminul Islam received B.Sc. in Computer Science and Information Technology from Islamic University of Technology (IUT) in 2007. Currently he is working as a Lecturer in the Department of Computer Science and Engineering at Ahsanullah University of Science and Technology (AUST), Dhaka, Bangladesh. He worked for Patuakhali Science and Technology University in the faculty of Computer Science and Engineering as a Lecturer.

Moinul Momen received B.Sc. in Electrical and Electronic Engineering from Islamic University of Technology (IUT), Gazipur, Bangladesh in 2007. Currently he is working as a Core Network Integration Engineer in LM Ericsson Bangladesh Ltd. He worked for Grameen Phone Bangladesh Limited as System Engineer in the department of Transmission Planning.