A Solution for Radio Data Transmission Problem in Electrical Substation Remote Control

Darko Živanović, Ivan Mićović, Marjan Djurić, Vladimir Krstić, *Mihajlo Pupin Institute*

Abstract — **This paper presents a problem that occurred during transmission on Supervisory Control And Data Acquisition (SCADA) Systems used in Electric Power Industry of Belgrade, where long sequences consisting only of "0" or "1" appeared to lead to a transmission problem over the radio using protocol IEC101. One hardware and software solution for this problem is presented that is doing scrambling of data passed to the modem which firmware is closed. Fabricated board together with implemented software is also doing data descrambling at the reception.**

Keywords — **SCADA, IEC101, scrambling.**

I. Introduction

In SCADA systems many different protocols for data transmission between a control center and electrical substations are used. (IEC101 [1], DNP3, ADLP-80, ADLP-180, MODBUS [2]). Generally, there is no rule to what is used as a medium for data transmission, and usually some of available resources such as copper wires are used, optical cables or air.

These facts are characterizing remote control system of electrical substations in the Electric Power Industry of Belgrade (EPIB). Modernization of this system is a natural and continuous process. However, it is impossible to modernize the whole system instantly, and these types of changes are introduced progressively. Therefore, it is natural for this kind of systems that there are many types of protocols and mediums used for data transmission. But, what must maintain in all cases is functionality and reliability of the system.

This paper describes one solution for the problem that occurred when the system for data transmission over radio with protocol IEC101 implemented began to be used in the electrical substations remote control. To that period of time, the whole system worked correctly and was reliable while the protocols ADLP80 and ADLP180 were used. But, when protocol IEC101 was introduced into the system, communication was no longer possible at all. Problem occurred because of the long sequences of zeroes in frames in data transactions between control center and electrical substations. These arrays of zeroes caused interruption in the communication since the messages in control center received from electrical substations were uncompleted.

There are two ways to solve this problem: hardware and software solution. Both ways are doing data scrambling at the transmission side and data descrambling at the reception side. That way, data is modified so it is suitably adjusted for transmission over radio. Since in this case, only models for SCADA systems were available, and not software itself, data processing is done by introducing a new hardware in the system.

II. Communication System

The whole system offers reliable and always available data transmission for electrical substations remote control over radio. System is using standard, professional radio stations and specialized modem that is connected between terminal and radio station. Data transmission is based on polling of peripheral stations by the control center, and polled station reporting to the control center. Terminal data speed is in range from 1200 bits/s to 57600bits/s, while data speed over radio is in range from 800 bits/s to 19200 bits/s. For wireless communication 25 kHz bandwidth is used in UHF or VHF frequency band. MOTOROLA GM340 radio stations are used. Messages between control center and electrical substation are 3 bytes or 25 bytes long, but system also must support 128 bytes long messages [3].

Communication between terminal device (in control center or in electrical substations) is asynchronous, 10 bits long (1 start bit, 8 data bits and 1 stop bit), with data speed of 9600 bits/s. Communication is by standard RS-232 interface. Fig. 1 shows communication line between terminal and radio station, and position of the scrambling device in the system.

This paper is supported by Ministry of Science and Technological development, Republic of Serbia, Project TR11040.

Darko D. Živanović is with the Mihajlo Pupin Institute, Volgina 15, 11050 Belgrade, Serbia (phone: +381 11 277 29 53; fax: +381 11 275 59 78; email: darko.zivanovic@institutepupin.com).

Ivan Ž. Mićović,is with the Mihajlo Pupin Institute, Volgina 15, 11050 Belgrade, Serbia (phone: +381 11 277 29 53; fax: +381 11 275 59 78; email: ivan.micovic@institutepupin.com).

Marjan J. Djurić is with the Mihajlo Pupin Institute, Volgina 15, 11050 Belgrade, Serbia (phone: +381 11 277 29 53; fax: +381 11 275 59 78; email: mdjuric@kondor.imp.bg.ac.rs).

Vladimir R. Krstić is with the Mihajlo Pupin Institute, Volgina 15, 11050 Belgrade, Serbia (phone: +381 11 277 29 53; fax: +381 11 275 59 78; email: vladak@kondor.imp.bg.ac.rs).

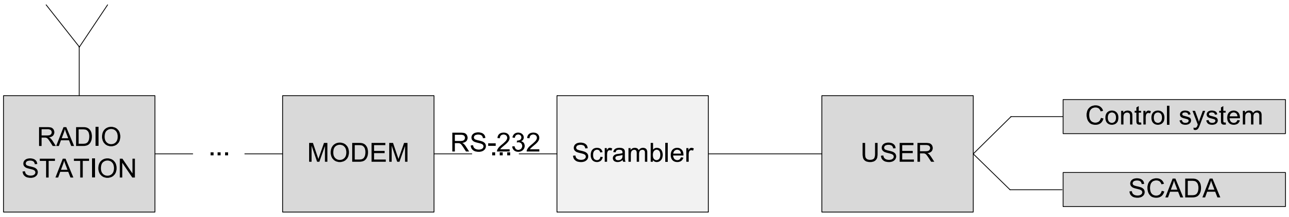

Fig. 1. Communication line between terminal and the radio station

System for the remote control of electrical substations is basically in star topology, where control system is polling peripherals (electrical substations, remote stations, SCADA - Fig. 2).

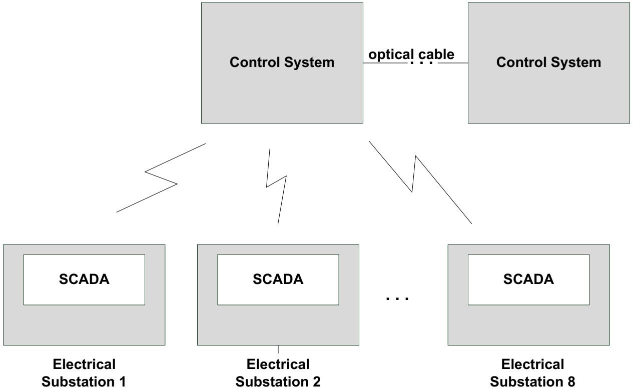

Fig. 2. Remote control center - Topology

III. Hardware and Software Architecture

A. *Hardware Architecture*

Hardware architecture of the device is highly dependent on the specification of the whole system. Scrambling device must intercept RS-232 lines before the modem, do scrambling on the data, and then pass scrambled data to the modem. Also, the board must be well designed, so that the same board with the same software must do both data scrambling at the transmission and data descrambling at the reception side.

Since voltages of RS-232 lines are in the range from -15V to +15V and scrambling board must have power supply of 3V3, MAX3238E [4] and MAX3243E [5] chips are introduced into the system. These chips have 5 driver and 3 receive lines, and 3 driver and 5 receive lines, respectively. Also, in order to secure 3V3 power supply for the board, voltage regulator LP2985 [6] is used to make the wanted power supply level from the 15V supply from the modem device. Microcontroller from PIC24F16KA102 [7] family is chosen because of the small resources needed for this kind of device. Fig. 3 shows PCB layout of the scrambling board, which is done in four layers, two routing layers and power and ground plane, with all assembled components. After the design is finished, the panel (board array) with 2 scrambling boards is created in order to mitigate fabrication costs. By having more boards on the panel, the stencil for populating of components is more expensive, so the proper trade-off must be done.

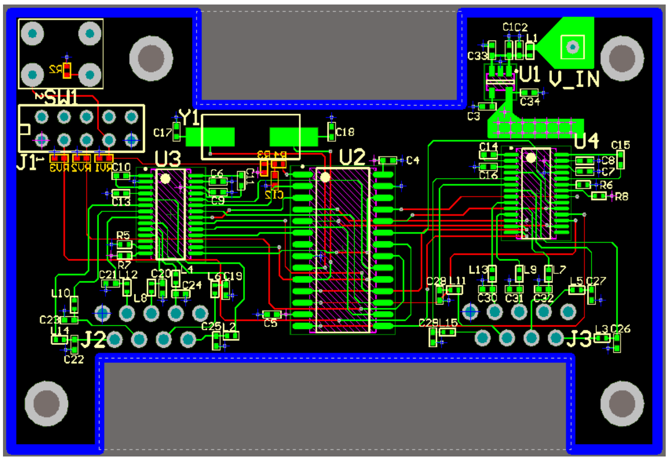

Fig. 3. PCB Design of scrambling device: *green – TOP, red - BOTTOM*

Power and ground plane make the board less prone to the effects of electromagnetic interference, and according to electromagnetic compatibility problem solving, each RS-232 signal is filtered right after entering the board. LC filters are used for each signal.

B. *Software Architecture*

Software architecture must be specialized, so the same board with the same software can be used both as the device for scrambling and descrambling the data, so that the same board can be used both at the transmitting and the receiving side.

Another problem software needed to solve is to secure correct programming of the modem. So, it must recognize entering the command mode ('+++' message), and secure that data is not scrambled in the command mode. Also, it must secure successful exit from the command mode by recognizing the right command message or when particular time expires and no data is received. So, in order to have the same software both for data scrambling and descrambling, the software in direction towards modem is doing data scrambling only while not in command mode (message '+++' hasn't arrived yet), and in opposite direction data scrambling is always done. Fig. 4 shows Mealy finite state machine which represents simplified software architecture for entering and leaving the command mode. The whole code is written, tested and debugged using Texas Instruments software tool Code Composer Studio v4 [8].

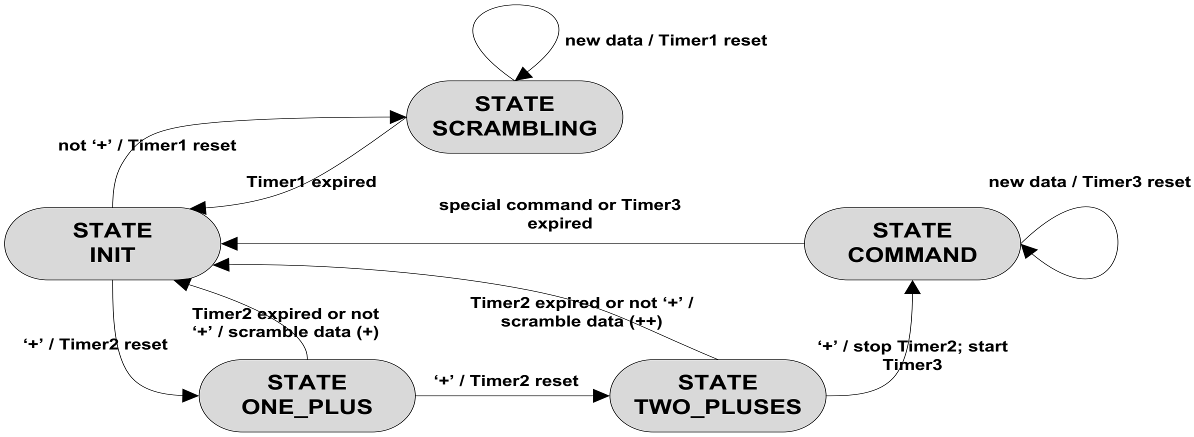

Fig. 4. Software architecture - Finite state machine

C. *Scrambling Method*

Scrambling method for the first version of scrambling device is simplified so that the system could be tested as soon as possible. Scrambling is done at the byte level, and every byte is scrambled with the random sequence. At the beginning of packet counters are reset and so the transmitter and the receiver are synchronized after every packet. For this version, scrambling is done only by bitwise "exclusive or" operation, and is doing XOR operation on the byte by the random number from the sequence. It is done until the end of packet. After that, counters are reset and scrambling is done with random sequence from the beginning.

D. *Testing*

The whole system was tested in the laboratory conditions, with transmitter transmitting the scrambled data over radio, and the receiver receiving and descrambling data at the reception. The data that was sent for scrambling was the one that contains large sequence of zeroes (256 bytes), which made problems while receiving the sequence without scrambling. At the reception, check was done in order to see if the received data was the one sent by the receiver. Valid entering of command mode is checked, and programming of the modem is done in order to check the support of different modes. Also, the whole system was validated on the field where the old systems had trouble with protocol IEC101, and with scrambling devices implemented all the problems were solved.

IV. Conclusion

The described work represents a valuable reference for solving communication problem using protocol IEC101 in electrical substations remote control. The future work will include improvements on the system, hardware and software, for eliminating problems with all the protocols used. Also, an optimization in software must be done, for scrambling to be as much as reliable as possible. Future work will also include implementation of some advanced scrambling technique [9][10], which will significantly improve performance of the system.

References

[1] International Standard IEC 60870-5-101, Telecontrol Equipment and Systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks, Second Edition 2003-02.

[2] Modicon Modbus Protocol Reference Guide, PI-MBUS-300, Rev. J, June 1996.

[3] Ministry of Science and Technological Development, Annual Report on the Project in 2009-2010, System for the Transfer of Information and Commands for Electrical Substations Control Center Over Radio Network, Technical Solution TR11040_4B.

[4] Texas Instruments, MAX3238E, 3-V to 5.5-V Multichannel RS-232 Line Driver/Receiver with ±15-kV ESD (HBM) Protection, SLLS710A, February 2006 – Revised April 2006.

[5] Texas Instruments, MAX3243E, 3-V to 5.5-V Multichannel RS-232 Line Driver/Receiver with ±15-kV IEC ESD Protection, SLLS657C, April 2005 – Revised February 2009.

[6] Texas Instruments, LP2985, 150-mA Low-Noise Low-Dropout Regulator with Shutdown, SLV522M, July 2004 – Revised March 2009.

[7] Microchip, PIC24F16KA102 Family Data Sheet, DS39927B, 2009.

[8] Code Composer Studio v4 User's Guide for MSP430, Texas Instruments, SLAU157K, May 2005 – Revised August 2009.

[9] Data Communication Over the Telephone Network – 4800/2400 bits per second Modem Standardized for use in the General Switched Telephone Network, Recommendation v.27, International Telecommunication Union ITU-T.

[10] Data Communication Over the Telephone Network – 9600 bits per second Modem Standardized for use on Point-to-Point 4-Wire Leased Telephone-Type Circuits, Recommendation v.29, International Telecommunication Union ITU-T.