Secured Communications for Networks with Configuration and Topology

Viša Tasic[1], Dragan R.Milivojevic[2], Vladimir Despotovic[3], Darko Brodic[4], Marijana Pavlov[5], Ivana Stojkovic[6]

[1]Institute of Mining and Metallurgy
Department of Industrial Informatics, Zeleni bulevar 35, 19210 Bor, Serbia
visa.tasic@irmbor.co.rs

[2]Institute of Mining and Metallurgy, Department of Industrial Informatics
Zeleni bulevar 35. 19210 Bor, Serbia
dragan.milivojevic@irmbor.co.rs

[3]University of Belgrade
Technical Faculty in Bor, Vojske Jugoslavije 12, 19210 Bor, Serbia
vdespotovic@tf.bor.ac.rs

[4]University of Belgrade
Technical Faculty in Bor, Vojske Jugoslavije 12, 19210 Bor, Serbia
dbrodic@tf.bor.ac.rs

[5]Institute of Mining and Metallurgy
Department of Industrial Informatics, Zeleni bulevar 35, 19210 Bor, Serbia
marijana.pavlov@irmbor.co.rs

[6]University of Niš
Faculty of Electronic Engineering, Aleksandra Medvedeva 14, 18000 Niš, Serbia
ivana.stojkovic@elfak.ni.ac.rs

ABSTRACT: *We studied the communication between nodes in the industrial networks in the field of copper mining. The industrial computer networks are used to observe the control of production process. With the help of the Programmable Logic Controller, we have collected the required data. The control network has two nodes. One is PLC and workstation which is used for visualization and interaction. We have introduced secure solutions for networks and also for the proper configuration and topology of the industrial networks.*

Keywords: Communications, Control System, Industrial Network, Monitoring

Received: 21 October 2022, Revised 2 January 2022, Accepted 11 January 2022

DOI: 10.6025/jisr/2023/14/1/17-22

I. Introduction

Three generations of computer control and monitoring systems, from mainframes to PC-based computer systems were implemented and developed in the Copper Mining and Smelting Complex Bor (RTB Bor) [1] during the last 20 years. Starting as a simple monitoring system in one of the company's factories, it grew to a complex industrial network that is covering local and geographically distributed plants.

The monitoring and control systems were constantly upgraded and improved until nowadays, both in terms of hardware devices and software support. Specific hardware solutions required the development of specialized communication protocols. This paper gives a brief overview of communications between nodes in the realized industrial networks throughout the years.

2. Synchronous Communications

The existence of the central host computer system (ICL 2958D) in RTB Bor at the beginning of 1990s [2] dictated the development of the specific communication solutions based on synchronous communications in the first generation of the monitoring and control systems. The implemented system had the following structure (as shown in Fig. 1):

- Distributed measuring stations (MS) installed at each transformer station,
- Data concentrators and remote workstations (RWS) installed at Control Centers,
- Host computers installed at Computer Centers in Bor (ICL 2958D) and Majdanpek (ICL ME29).

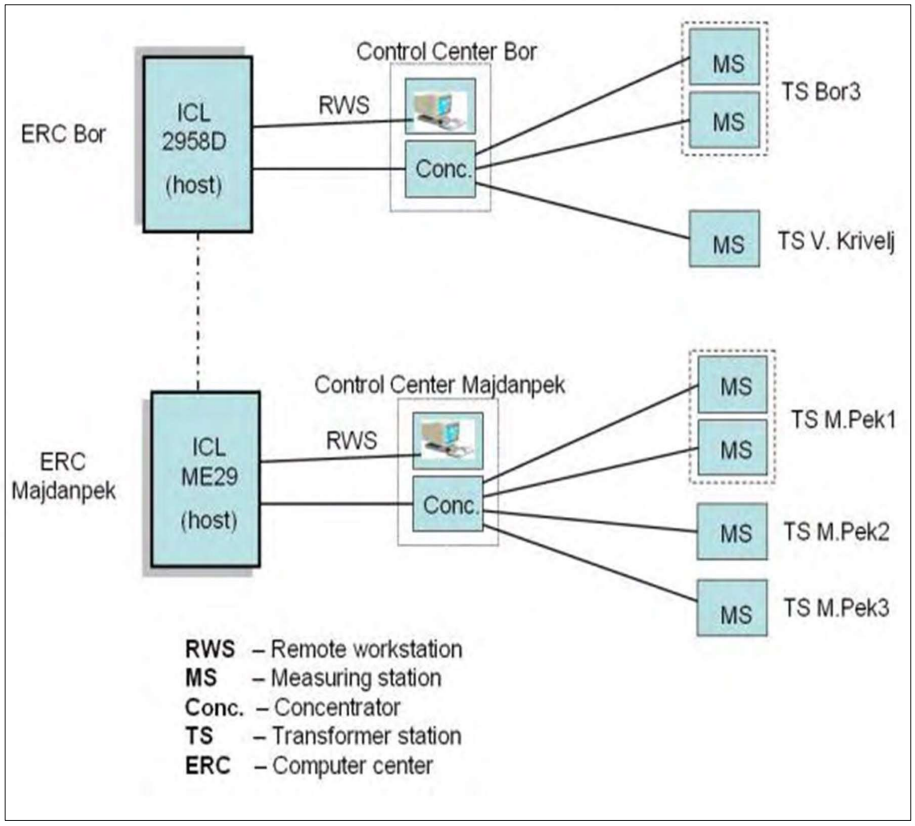

Figure 1. The configuration diagram of monitoring system [3]

The integral monitoring system was organized as a threelevel MAN network. Data concentrator (master node) was connected via base-band modems and leased lines with the measuring stations (slaves) at one, and host computer, at the other side. Communication protocol, BSCP (Binary Synchronous Communication Protocol) [4] was specially designed and applied in order to support real-time data transfer between all network nodes.

BSCP was designed for master-slave type of communications. Hence, one can differentiate two basic types of messages, Request Message and Reply Message. One communication cycle consists of a successful exchange of messages between two network nodes (master and slave) in both directions. Request message sent by the master node (data concentrator) initiates the data transfer, whereas reply message sent by the slave node ends the data transfer (one communication cycle). The format of the message is shown in Table 1.

Syn	SoB	Addr	ComS	Cat	State	Text	Etx	Bcc

- Syn – Synchronization character
- SoB – Start of Block
- Addr – Destination address
- ComS – Communication Status
- Cat – Category (type) of message
- State – Transmitter state
- Text – Useful information
- Etx – End of Text
- Bcc – Block Check Character

Table 1. Format of the message in bscp

According to its characteristics BSCP was not inferior to standard communication protocols of the same class (e.g. Modbus protocol). Compared to similar protocols one could note smaller header, while special “data packetization” increased its efficiency. Since it was based on synchronous communications it required specific hardware solutions in order to be used with personal computers. Hence, a communication module had to be developed for this purpose. A configuration diagram for one part of the control system is shown in Figure 2.

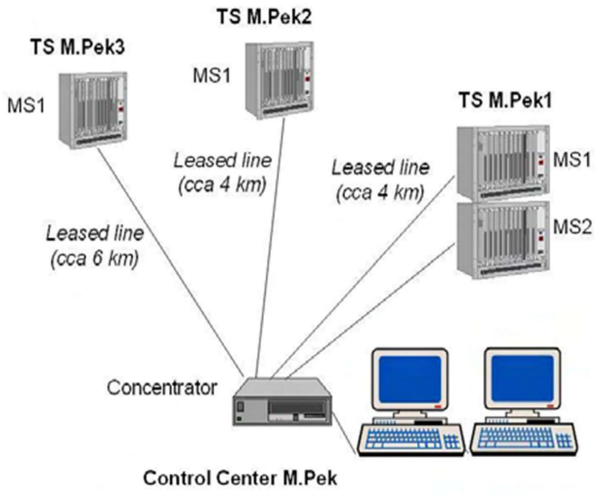

Figure 2. Example of the electrical energy consumption control system configuration diagram

3. Asynchronous Communications

The next step in development of the communications between nodes, in the realized industrial networks in RTB Bor, was the transition from synchronous toward asynchronous communications [5]. The new generation of Monitoring Measuring Station (MMS), fully designed and developed at the Department of Industrial Informatics of the Mining and Metallurgy Institute, was used as a Programmable Logic Controller (PLC), which was a slave node in a realized network. The master PC was added as an interactive workstation, forming an entity which was a core of the complex distributed control and monitoring system, as shown in Fig. 3.

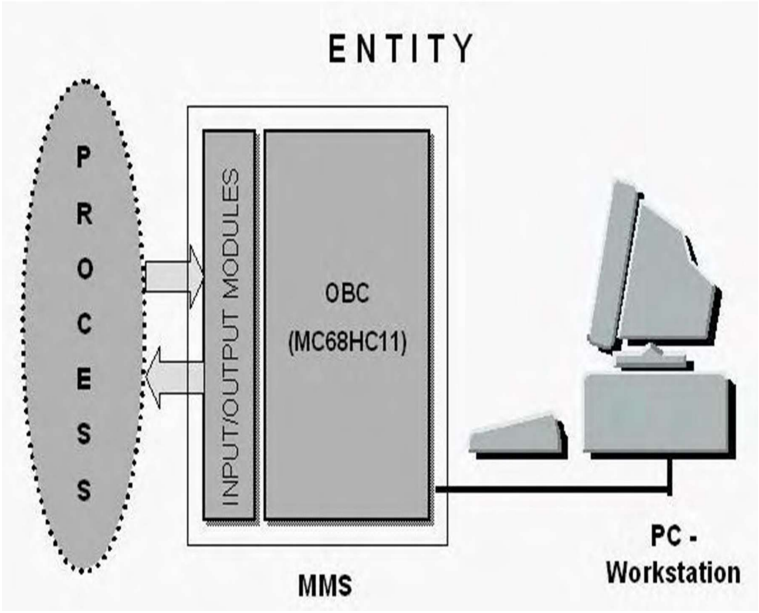

Figure 3. Simple control system - entity (MMS and PC)

In a hardware point of view, MMS contains the serial communication interface with direct back-to-back connection to standard PC RS232 serial port. The connection between PC and MMS is permanent. The two-node network runs according to the master-slave principle. The PC as a master node starts the session, maintaining the data transfer and regular end of the session. The MMS has to respond to every PC demand.

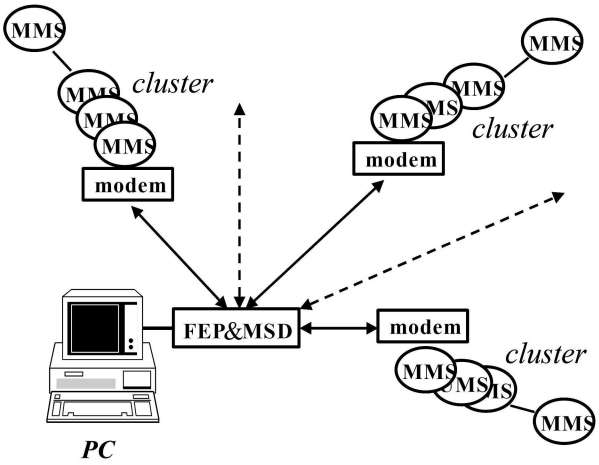

Figure 4. Control system configuration diagram [5]

Independently from the fact whether the local control is in use or not, data about the status of the process are transferred from MMS to PC. These data are processed on PC and results are presented in corresponding form on the screen and stored in external memory using the specially designed software. If the system performs remote control function, depending on the status of the process, commands are sent from PC to MMS, which initiates adequate actions and affects the process flow.
Designed and implemented network must satisfy several basic requirements:

-To provide correct and efficient data transfer to PLC in the shortest possible time from the time of their origination,

- To solve uniformly transfer of command to PLC while the command is active and actual

- To provide successive transfer of data from PLC to PC for the case that there are any faults in normal transfer.

FEP&MSD (Front End Processor and Modem Sharing Device) is a microprocessor device whose function is to ensure solid communication link with belonging PC, and to establish, maintain and control network operation of local and remote groups of PLCs (clusters shown in Figure 4). It is a central node in the network located next to PC and it is directly connected to one of its communication ports.

Physical connection between nodes is realized with twowire leased line. For conditioning of transfer signal simple assemblies are used as line amplifiers. Only the first one in the cluster is slightly more complex and is directly connected to the modem. Physical connection between nodes within the cluster is realized with two lines in multipoint. The distance from the first to the last MMS in the cluster may extend up to 2.5 km. One cluster, in theory, contains up to 128 nodes (MMS) but in practice only 16 has been used. Applied FEP&MSD devices may support up to 16 clusters.

DAd	SAd	EAd	Code	CSt	Text	EoM	Bcc

- DAd Destination Address
- SAd Source Address (Message originator)
- EAd End Address
- Code Status or Command
- CSt Communication Status
- Text Useful information
- EoM End of Message
- Bcc Block Check Character

Table 2. Format of the Message In Asp [5]

In order to support the data transfer in a realized network a complex communication subsystem is developed. It is based on the serial communication PC port (RS 232 C, Recommendation V24) and capabilities of the serial communications of the microcontroller MC68HC1, which is the basis of the MMS. Serial communication interface of the microcontroller is a full duplex asynchronous system that uses NRZ (Non Return to Zero) format with one START bit, 8-bit or 9.bit character and one STOP bit. Bitrates can be chosen between 600 and 78000 bps. 19200 bps are used in practice.

To be able to establish connections between network nodes and to achieve optimal speed and reliability of transfer a communication protocol named Asynchronous Serial Protocol (ASP) is designed [5]. There are two basic classes of messages in the ASP: Master message sent by the primary network node and Slave message sent by the secondary network node. Connection establishment and transfer control are initiated by the primary node (master). Prior to sending the master message a secondary network node (slave) has to be selected. The standard message format is shown in Table 2.

4. Conclusion

BSCP protocol is not inferior, according to its performances, to the protocols of the same class. Its main drawback is the fact that it is a synchronous communication protocol, hence it requires specific hardware, as well as the PC extending communication

module. Thanks to the precise definition of the time duration of transmission, this protocol is a very good choice for hard synchronization between network nodes. There are several industrial MAN networks in operation that use BSCP protocol. Data transfer efficiency between nodes has shown to be satisfactory for the applications they serve.

ASP requires no additional hardware on MMS or at PC, which is its main advantage compared to the BSCP. Software support is written in VC++ and Delphi. Both protocols showed high stability in operation, almost without lost messages.

First impression is that realized networks, by its characteristics, do not belong to the group of high performance solutions. For standard networks megabit transfer rates are present nowadays. However, for the purpose they are designed they have shown to be a very rational solution. Processes and events, which are monitored and controlled by such systems, are relatively slow (central heating system, water supply network, electrolytic copper refinery plant, etc.). Actual information about the state of these processes is generated at minute intervals or even more rarely, so that efficiency of communication system can not been questioned. Apart from favorable price/performance ratio, functioning of realized network has shown to be very efficient and reliable and especially resistant to poor communication conditions, thanks to solid transfer quality control and possibility of dynamic network reconfiguration.

Acknowledgement

This work was partly funded by the Grant of the Ministry of Education, Science and Technological Development of Republic of Serbia, as a part of Project No. TR33037 " Developement and Application of Distributed System for Monitoring and Control of Electrical Energy Consumption for Large Consumers".

References

[1] Tasic, V., Miloševic, N., Kovacevic, R. & Petrovic, N. (2010) Analysis of air pollution caused by particle matter emission from the copper smelter complex Bor (Serbia). *Chemical Industry and Chemical Engineering Quarterly*, 16, 219–228 [DOI: 10.2298/CICEQ090909011T].

[2] Radojkovic, M., Milivojevic, D., Jojic-Blagojevic, G. & Cajic, M. System for monitoring and control of electrical energy consumption in RTB bor. *Proceedings of the VII Scientific Convention on Microcomputers in Process Control Systems*, MIPRO'88. Rijeka, Croatia, 18-20.05.1988, pp. 5–31 – 5-35.

[3] Tasic, V., Despotovic, V., Brodic, D., Pavlov, M. & Milivojevic, D. (2013) "Twenty years of monitoring and control of electricity consumption in RTB Bor, Serbia," accepted for presentation on MIPRO - 36th International Convention, Opatia, Croatia.

[4] Milivojevic, D., Radojkovic, M. & Jojic Blagojevic, G., Dj (1990) Simon, S. Lalovic. In: Communication Subsystem of DSKP Systems. *Proceedings of the XIV International Conference of Information Technology*, Bk. 1, pp. 173.1–173.5, Sarajevo-Jahorina, BiH.

[5] Milivojevic, D.R. & Tasic, V. (2007) MMS in real industrial network. *Information Technology and Control*, 36, 318–322.