TECHNICAL TRANSACTIONS | CZASOPISMO TECHNICZNE
AUTOMATIC CONTROL | AUTOMATYKA
1-AC/2013

ŁUKASZ ŚCISŁO*

CONTROLLER–SENSING ELEMENT COMMUNICATION USING UDP PROTOCOL

KOMUNIKACJA STEROWNIK–URZĄDZENIE POMIAROWE Z WYKORZYSTANIEM PROTOKOŁU UDP

Abstract

The main goal of this paper is an attempt to create a new approach to measuring equipment-PLC controller communication. Beside the individual communicational protocols supported and developed by PLC manufacturers, PLC controllers support also popular protocols like TCP or UDP. This allows an easy communication with computers and many devices supporting these protocols. This paper presents a control system, which allows the distance measurement where the data is sent to the PLC controller (SIEMENS S7-1200) using Ethernet bus. The data can be also accessed using Human Machine Interface on an operators screen. In the paper it is shown how to create such a communication system which can be implemented for measurement purposes and is ready for farther development in the future.

Keywords: Ethernet, UDP,UART, PLC, control systems, HMI, Profinet, industrial automation

Streszczenie

Głównym celem niniejszego artykułu jest opracowanie nowego podejścia do komunikacji urządzenie pomiarowe–sterownik PLC. Sterowniki przemysłowe, oprócz własnych protokołów komunikacyjnych, coraz częściej obsługują popularne protokoły komunikacyjne, takie jak TCP czy UDP. Umożliwia to komunikację z komputerami PC oraz wieloma urządzeniami obsługującymi wyżej wymienione standardy. W artykule pokazano sposób zaprojektowania i realizacji układu wykonującego pomiar odległości, który wyniki pomiaru przesyła do sterownika programowalnego SIEMENS S7-1200 za pośrednictwem magistrali Ethernet i protokołu UDP oraz do systemu kontroli na ekranie operatorskim HMI. Zaprezentowano sposób realizacji systemu komunikacji, łatwość jego implementacji dla systemów pomiarowych i możliwość rozbudowy o kolejne urządzenia.

Keywords: Ethernet, UDP, UART, sterowniki przemysłowe, HMI, Profinet, automatyka przemysłowa

* Łukasz Ścisło, M.Sc., Department of Automatic Control and Information Technology, Faculty of Electrical and Computer Engineering, Cracow University of Technology.

1. Introduction

Modern production processes require the use of very accurate and reliable controlling devices. For such a task Programmable Logic Controllers can be a very good choice. PLC`s are being widely used for controlling devices, machines and whole technological processes [7, 14, 15]. They have replaced systems based on transmitters. The advantages of using PLC controllers are their high reliability, relatively low costs, compact built and module structure which make the further development of a control system possible [9].

One of the most important advantages of controllers are many different protocols which can be used for communication purposes (TCP, UDP). Most of the modern controllers are provided with interfaces which allow connecting them into networks [6]. Moreover, most of the new PLC`s, HMI screens and programmators can communicate using Ethernet protocol (e.g. Siemens S7-1200 which communicates with computers and HMI devices using Ethernet/ Profinet protocol), it is difficult to find sensing equipment which can in an easy way send/ receive data from the PLC, using similar kind of communication [3, 4, 10, 12].

The paper has two main purposes. The first one is to show the way to use modern protocols for acquiring measurement data, which can be sent to any kind of the control platform. The second purpose is to present a method of creating a UDP connection for Siemens PLC family which is not mentioned in professional journals.

The article will be divided into four chapters. The first one is an introduction to the PLC systems; the examined problem is introduced and an explanation of the paper's aim is presented. The second chapter concentrates on problem analysis. The architecture of the proposed communication between measuring equipment and PLC controller is introduced. Moreover, the way to create such a communication system is explained in detail. The following chapter shows the test of laboratory prototype and the obtained results for the distance measurements. The last chapter consists of the summary and the description of possible future development of the proposed system.

2. Problem analysis

For many modern control systems, especially responsible for continuous monitoring of crucial elements, it is very important to obtain current measurements as fast as possible. It is especially needed for fast location of faults in mechanical systems [16]. Using programmable logic controllers it is possible to use many different communication methods. This paper especially shows the possibility of using UDP protocol instead of very popular TCP. UDP communication can increase significantly data transmission which can be very useful in industrial control systems.

The proposed system includes programmable logic controller Siemens S7-1200, HMI operators screen, two-way Ethernet/UART converter, microcontroller with analogue-to--digital converter and a distance sensor. Siemens S7-1200 includes two modules: central processing unit 1214C AC/DC/RLY and a network switch CSM 1277 SIMATIC NET. All the parts of the proposed system and their communication concept are shown in Fig. 1.

The measurement data from a range-finder is sent through Ethernet bus with the use of UDP protocol. The range-finder measures the distance from the barrier, data is being sent to the microcontroller which converts the data in a proper way and sends it to the PLC. The current measurement will be observed on HMI screen. The operator is able to decide when to start and stop the measurement and what the measurement parameters are.

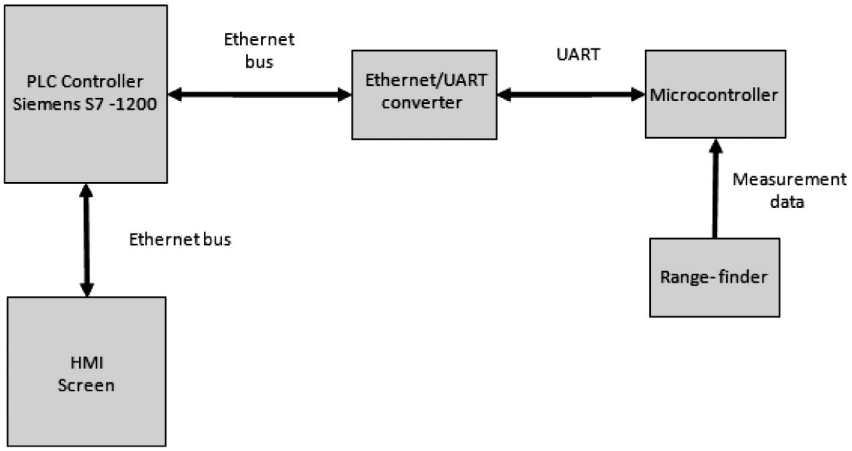

Fig. 1. The block diagram of the proposed system

Rys. 1. Schemat blokowy proponowanego systemu

2.1. UART Communication

UART (*Universal Asynchronous Receiver and Transmitter*) is a device used for serial asynchronous communication, which allows for an easy data transmission in a RS-232C standard [11]. UART has two lines for data transfer. For sending data "Tx" line is used and for receiving data "Rx" line is used (Fig. 2). Data is being transferred in frames which start from a start bit and next bits are data bits. Typically, there are 5 to 8 data bits [13]. The frame is ended with one or two stop bits. UART is serial asynchronous communication, and that is why no additional synchronizing signal is needed. Therefore, less conductors are needed for the transmission. However, in devices communicating using UART, it is important to set the same data transmission speed and the same frame format. Most of the modern microcontrollers have hardware support for serial UART communication. This communication can take place in half-duplex mode, which means that in the specific time only one device transmits data, or in full-duplex mode (both devices transmit data at the same time).

However, the serial communication is slower than parallel, so it is important from automation machines control point of view that much less wires are being used, which is a particularly great advantage when measurement data needs to be transmitted over long distances.

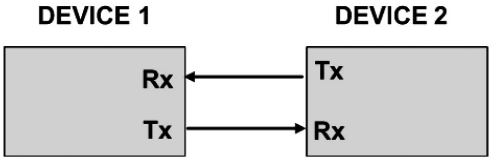

Fig. 2. UART communication

Rys. 2. Komunikacja UART

2.2. Ethernet/UART converter configuration

ATV5340 system converts messages received from programmable logic controller which are being sent by Ethernet bus. UDP protocol is used to communicate using the Ethernet bus. Finally the data is sent to microcontroller by UART interface. The configuration of AVT5340 system is made using a computer which is in the same network as ATV5340. In the web browser it is possible to insert the IP address assigned to the converter.

In the *network* tab the following attributes can be changed:
- MAC – only singular change is possible,
- IP – which is an address of the converter in the network,
- comment,
- subnetwork mask – for the converter,
- gate – parameter used when the converter communicates through the router.

In the *Hosts* tab IP addresses and port used for sending the data can be configured. In the COM tab two other parameters can be set:
- COM – which is responsible for transfer speed using UART interface. The choice between 2.4 kb/s to 1 Mb/s is possible,
- Overtime.

The converter can start data transmission using Ethernet bus when one of the two conditions is met:
- the buffer is full,
- the specific time since the first UART frame received is reached (time set in the Overtime parameter).

2.3. Microcontroller configuration

The microcontroller operates with 1 MHz frequency. To start voltage measurement and data transmission the correct command needs to be received by the microcontroller. The command format is shown in Fig. 3.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Not used					Sampling period		Measurement

Fig. 3. Command format

Rys. 3. Format rozkazu

Where bits:
- 2 and 1 – are responsible for sampling time:
  - 00 – measurement every 1 s,
  - 01 – measurement every 500 ms,
  - 10 – measurement every 250 ms,
  - 11 – measurement every 125 ms.

– 0 – start and end of the measurement:
  • 0 – measurement stop,
  • 1 – measurement start.

Commands which contain not used bits cause the measurement to stop (regardless of the bit 0 value). When the UART frame is received from the converter (connected to the microcontroller) an interruption is generated and the data received is compared to the command stored in the microcontrollers' memory. Four possible settings of voltage sampling periods are available. The change of the sampling period takes place when T0 timers' frequency divider is changed. The first voltage measurement takes place immediately after the command is received and the next three are taken every 20 ms from the first measurement. The results of the measurements are averaged and sent by serial connection to Ethernet/UART converter, which sends it farther to the PLC controller (S7-1200). The format of this data is 16-bit word, which is later translated to the distance value by the PLC.

Timer T0 is responsible for sampling period and every following measuring cycle starts with the interruption generated by the timer. Every interruption of T0 timer starts counting by timer T1. This timer generates interrupts every 20ms which start range-meters` voltage measurement. T1 executes three such cycles and goes to stop state. The measurement (sampling and A/D conversion) lasts about 0.5 ms and the whole measurement cycle lasts about 60.5 ms plus few clock cycles needed for voltage value averaging. That relatively long measurement cycle was introduced only because the range-meter used in the laboratory model has very low amplitude of oscillations of output voltage. When the measurement of long distances is introduced, the small change in output voltage causes significant changes in measured distance (that is one of the reasons to perform multiple measurements which are later averaged).

The microcontroller communicates with the AVT5340 converter with 9.6 kb/s velocity. The transmission time of 16 bit word takes about 2.1 ms. Both AVT5340 converter and microcontroller MSP430G2553 can reach up to 1 Mb/s transmission speed, but this requires the use of microcontrollers with the frequency of 16 MHz.

2.4. PLC and HMI configuration

PLC LAD application is created in the TIA (Totally integrated automation) Portal environment for the purpose of measurement process standard control. Moreover, to allow an easy access and presentation of the data, an additional HMI application is designed for KPN600 Panel. TIA is a system in the automation technology field which has been developed by Siemens for the last few years [5]. This strategy defines the interaction of extensive single components, tools and the services to achieve a full automation solution for the problem. The interaction performs integration across the four automation levels of the automation pyramid: management level (ERP, MES), operator's level (SCADA), controller and field's level (commonly called floor control level) level (Fig. 4) [8].

Although, usually the control level consists only of PLC or PLC with HMI panel it is proposed to include also other devices like: PDA's, smartphone's and tablets. All those devices are really able to connect directly to the PLC, but current fast development of network communication for programmable logic controllers including Ethernet and GSM communication may suggest that it is a matter of a short time for such application to be used

for control purposes. Developing a fully functional Android application for PLC – operator communication is currently under development. For this paper purpose only floor control level is considered (Fig. 4).

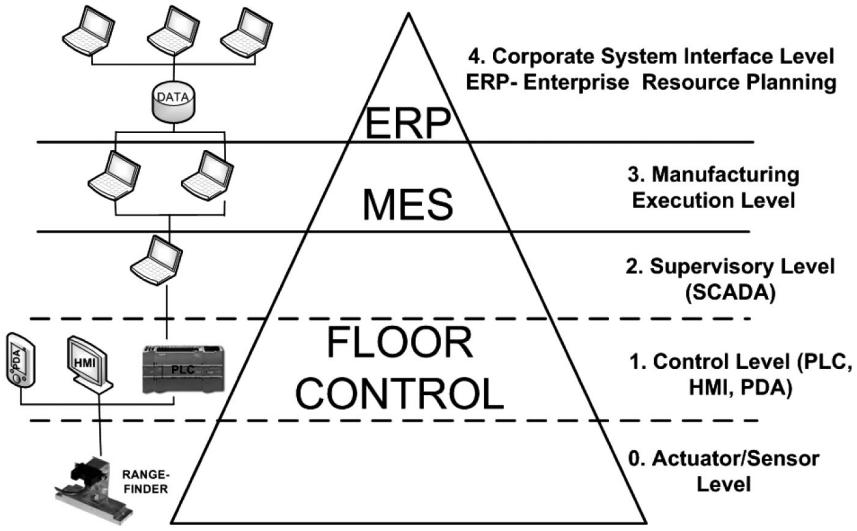

Fig. 4. Automation pyramid concept

Rys. 4. Piramida automatyzacji i zarządzania produkcją

There are two requirements for PLC control program for the proposed device:

– it has to allow the communication using UDP protocol,
– it has to be able to convert measurement data received from the converter.

To allow UDP connection three of the program blocks need to be configured (Fig. 5):

– TCON – which allows for the manual set-up of the connection with TCP, ISO-on-TCP and UDP protocol. TCON sets the connection parameters and gives the connection identification number,
– TUDEND – allows data transfer using UDP protocol,
– TURCV – allows data to be received using UDP protocol.

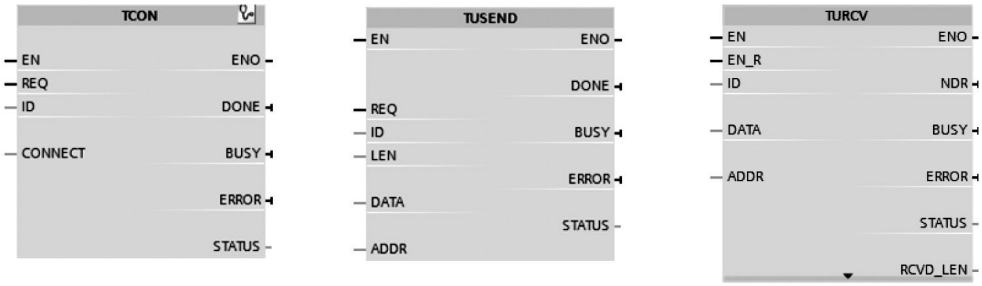

Fig. 5. PLC program blocks which need to be configured for UDP communication

Rys. 5. Bloki programowe PLC wymagające konfiguracji dla komunikacji UDP

The PLC program allows also for the conversion of the voltage measured by the range-finder and sent by the microcontroller. The value of the voltage is calculated using fallowing equation:

$$U = \frac{N_{\mathrm{ADC}} \cdot 3{,}3}{1023} \tag{1}$$

where:

U – voltage value,
N_{ADC} – value sent by the microcontroller.

3. Laboratory test of proposed system

The laboratory demonstration the device shown in Fig. 6 is used. The equipment consists of the microcontroller (MSP430G2553), Ethernet/UART converter (AVT5340) and a power supply unit. The system requires 3.3 V (microcontroller, converter) and 5 V (range-finder).

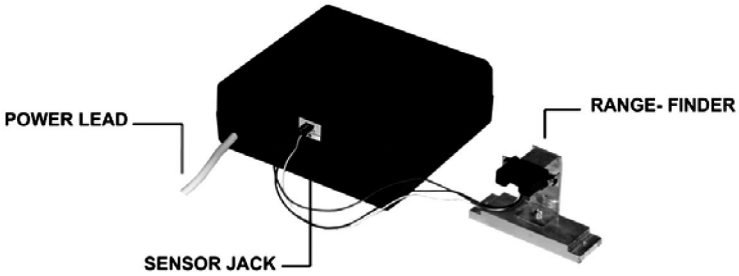

Fig. 6. The overview of the laboratory test set

Rys. 6. Części składowe układu laboratoryjnego

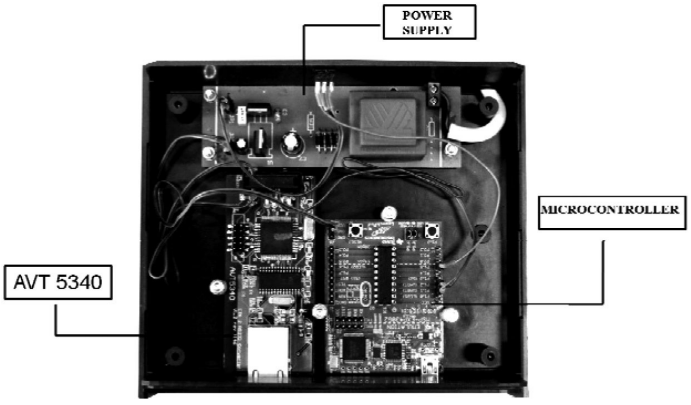

Fig. 7. The inside view if a laboratory test set

Rys. 7. Widok wnętrza układu laboratoryjnego

The configuration of the measuring cycle of the microcontroller is shown in Fig. 8:
- the measurements are held every 125–1000 ms,
- sampling time – 60.5 ms,
- data transmission to the converter – 2.1 ms.

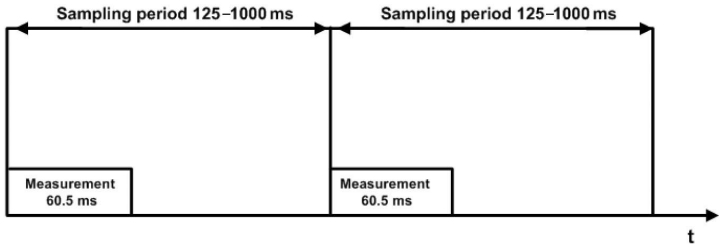

Fig. 8. Microcontrollers measuring cycle diagram

Rys. 8. Diagram cyklu pomiarowego mikrokontrolera

For a laboratory test of the proposed device two applications are used:
- PLC (Siemens S7-1200) application using TIA Portal environment,
- Human Machine Interface application for operators screen (KPN600).

TIA Portal is a new environment for industrial automation applications – especially PLC and HMI systems. It includes of STEP7 and WinCC environments. STEP7 is a system for PLC configuration and programming, which allows for using LAD and FBD languages for programming [7, 11]. WinCC flexible is a system for development of industrial operators' panels applications. The advantage of TIA Portal is an universal access to the program variables. The tags created in one of the programs mentioned above can be used by other applications and by other devices, which allows for an easier creation of a fault free control programs.

The test screen gives the possibility of choosing one of the three buttons (Fig. 9):
- measurement start – which causes a message to start the measurement to be sent to the microcontroller,
- measurement stop – allows to stop the measurement,
- options – opens a screen with additional options (Fig. 10).

Additionally, the field in the top right corner allows to choose a different sampling period. This option allows for a selection of up to four different values and a choice of a different period than the actual one which does not require a pause in a current measuring process.

Additional options allows the user to set the new variables:
- change of IP address and port of the device to which PLC wants to be connected to,
- change of the approximation function for distance measurement according to the voltage measurement (depends of the sensor used).

Figure 11 shows two of the characteristics where distance to output voltage fuction is obeserved. The rang-finder used for this device causes a small change in the output voltage when measuring long distances.

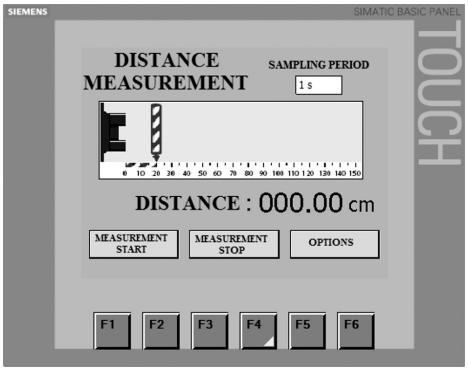

Fig. 9. HMI measurement test screen

Rys. 9. Ekran HMI pomiaru odległości

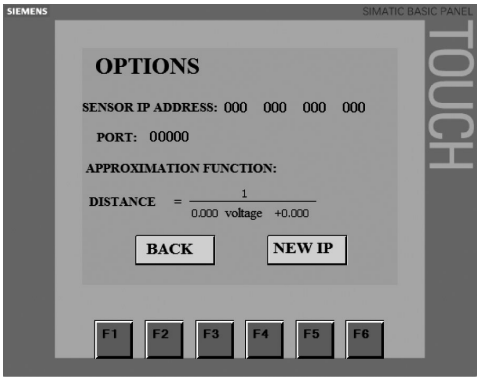

Fig. 10. HMI additional options screen

Rys. 10. Ekran HMI dodatkowych ustawień

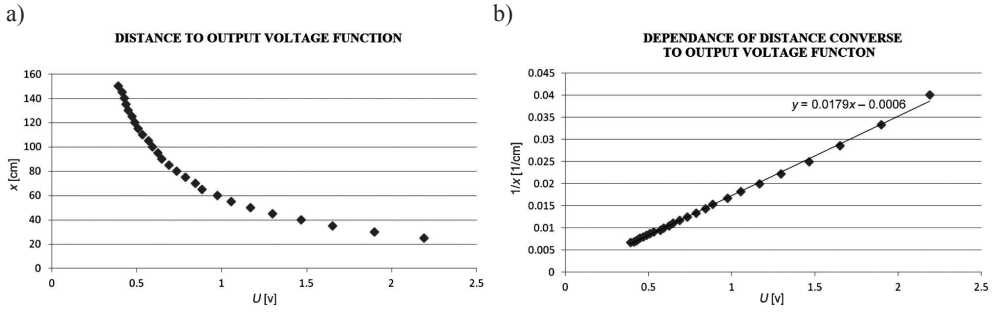

Fig. 11a) Distance to output voltage function (measuring range 25–150 cm), b) dependance of distance to output voltage function of the range-finder (measuring range 25–150 cm)

Rys. 11. Rys. 11a) Odległość w funkcji napięcia wyjściowego dalmierza (w zakresie od 25 do 150 cm), b) odwrotność odległości w funkcji napięcia wyjściowego dalmierza (w zakresie od 25 do 150 cm)

4. Conclusions

Usually, when sending measurement data to the programmable logic controller, analogue or digital modules of the controllers are used. In modern systems a wide range of network protocols is being used as well. The main advantage of using UDP communication comparing to TCP/IP is that it is much faster. It does not restrict the user to a connection based on communication model, so startup latency in distributed applications is much lower, as is operating system overhead. All the main settings like: flow control, acknowledging, transaction logging, etc. are up to program users. This means that the system user can only use the features that he really needs. The great advantage of UDP is also that broadcast and multicast transmission are available for the programmer. As it was mentioned the UDP allows a high transmission speed, with the maximum speeds enforced only by real network bandwidth. It must be remembered that actual speed is agreement of sender and receiver. The higher speed is an effect of two things:

– in case of the TCP/IP the receiver sends an acknowledgement to the sender to show that the data has been successfully received or has to be repeated. UDP protocol only acknowledges a successful sending of the data into the network and not the arrival of the data at the target station. The user program must take care of securing consistency and data preparation,
– the UDP header is rather short, compared to the TCP/IP header, therefore the UDP telegram can be created and processed much faster than the TCP.

Although it may seem that UDP is really unreliable, in case of continuous measurements where data is sent to PLC even when some packets are missing, it is no problem because usually the acquisition cycle is much slower for the user to be aware of missing the data. It must be also stated that UDP is suitable for small-to medium volumes of data (data volume: 1–2048 bytes) and TCP is suitable for transferring medium-to-large data volumes (data volume: 1–8192 bytes).

It is proposed to use a UDP protocol for measurement transmission to PLC instead of TCP. The biggest advantage of this, apart of higher speed, is that the configuration of devices and development of the software is much easier. Also, devices using this protocol can be used with any programmable logic controller regardless of the brand.

However, the presented in this article device is only used for distance measurement, it also can be used to connect other measurement equipment. Receiving data simultaneously from multiple hosts is much easier with UDP than with other protocols. The aim of the project is to find an efficient way for communication of industrial sensor equipment with the PLC controllers using Ethernet protocol. The laboratory test station allows not only to send data to such equipment, but also to any device supporting UDP protocol. However, the typical sensor is usually connected to the control device like PLC but using UDP communication can be used separately and can be, for example, connected directly to the computer.

The designed device is fully functional, however, it uses only a part of its potential because the rest fifteen input/outputs of the microcontroller are not used. Additionally five of those can be configured as analogue inputs. The device can be significantly expanded by means of connecting other sensing equipment. Moreover, Ethernet/UART AVT5340 converter, which is used for the device has two serial UART communication lines which allows to connect second microcontroller. This gives even greater possibility of farther development and operators availability to connect other sensors or actuators.

The concept of connecting measurement equipment using one of the internet protocol suite members gives an easier way to collect data for upper levels of automation pyramid (Fig. 4) or send the data directly to databases on the MES or ERP level. Such an approach can be used for distributed production scheduling. It can be very flexible, requirement-driven and reconfigurable so it acts as an open manufacturing system which can easily adapt to raid changes in market demands. Faster sensitive data transfer, using network protocols, in a more distributed way (accessed through PDA, phone, tablet and etc.) allows fast response to emergencies (machine failure, operator's absence, material shortage) and gives solution to a production problems (especially scheduling).

References

[1] Berger H., *Automating with SIMATIC S7-1200: Configuring, Programming and Testing with STEP 7 Basic V11; Visualization with WinCC Basic V11*, Publicis Publishing, 2013.

[2] Berger H., *Automating with SIMATIC S7-400 inside TIA Portal*, Publicis Publishing 2013.

[3] Berger H., *Automating with SIMATIC*, Publicis Kommunikationsag, 2003.

[4] Berger H., *Automating with STEP 7 in STL and SCL*, Publicis Corporate Pub, 2005.

[5] Berger H., *Automating with SIMATIC S7-300 inside TIA Portal*, Wiley-VCH, 2012.

[6] Bolton W., *Programmable Logic Controllers – Fifth Edition*, Newnes, 2009.

[7] Borden T., Cox R., *Technician's Guide to Programmable Controllers*, Cengage Learning, 2012.

[8] Koen P., Stromsdorfer C., *Distributed Applications in Manufacturing Environments*, The Architecture Journal, 10/2008, 40-44.

[9] Mitchell R., *PROFIBUS: A Pocket Guide*, ISA: The Instrumentation, Systems, and Automation Society, 2003.

[10] Müller J., *Controlling with SIMATIC*, Siemens, 2005.

[11] Petruzella F., *Programmable Logic Controllers*, McGraw-Hill, 2010.

[12] Pigan R., Metter M., *Automating with PROFINET*, Publicis Publishing, 2008.

[13] Raijkumar N., *Communication and Debug Platform for Smart Antenna DOA System: UART System Design in VHDL and Debug Platform in Labview*, VDM Verlag Dr. Müller, 2010.

[14] Ścisło Ł., *Multifunctional Control of a Proportioner*, Proceedings of the PhD Students and Young Scientists Conference, 2009.

[15] Ścisło Ł., *Integrated Control of the Heat Pump Heating and Cooling System*, Proceedings of the PhD Students and Young Scientists Conference, 2010.

[16] Zając M., *Wavelet Analysis for Location of Faults on Drive Transmission System*, Technical Transactions, vol. 1-AC/2012, Cracow University of Technology Press, 139-156.