IEEE 802.15.4 Wireless Network Application in Real-Time PLC-Based Control Systems

Piotr Krasiński, Bartosz Pękosławski, and Andrzej Napieralski

Abstract—**Most of the modern industrial automation systems are based on Programmable Logic Controllers (PLC). Vast selection of communication networks are available for automation system designers. Nevertheless, contemporary standards were not designed with real-time wireless sensor networks in mind. Based on our experience in IEEE 802.15.4 networks and automation fields we discuss possible means which can make it possible to take most advantage of real-time wireless networks in traditional automation control systems.**

***Index Terms*—Wireless Sensor Network, Modbus, ZigBee, IEEE 802.15.4, PLC, Real-time, Industrial Automation**

I. Introduction

RECENT advances in wireless technology make it become more and more popular in industrial applications. Wireless Sensor Networks (WSN) can be utilized in security, supervision and control systems [1, 2]. In our department, a dedicated protocol for IEEE 802.15.4 wireless network was developed. Real-time operation is not normally implemented in ZigBee or other standard protocols. Special care was taken on low energy consumption. This was demanded by powering the sensor nodes from energy harvested from ambient vibrations. Most commercially available solutions utilize wireless Ethernet or GPRS technologies. Both deliver good interface possibilities with automation systems but lack as far as power consumption and price are concerned. Also real-time operation is rarely implemented. Integration of WSNs and traditional industrial control systems is still an open issue. In this paper some solutions for this problem are presented.

II. IEEE 802.15.4 based Wireless Sensor Networks

Advantages of IEEE 802.15.4 standard include low power consumption, diversified network architectures and high reliability. ZigBee standard describes third and higher levels of OSI model of IEEE 802.15.4 network [3]. Systems utilizing this standard include intelligent building automation, environmental condition monitoring, security and RF-ID systems. It can be also used in versatile industrial control and monitoring systems. Typical structure of industrial network with wireless nodes is presented in Figure 1.

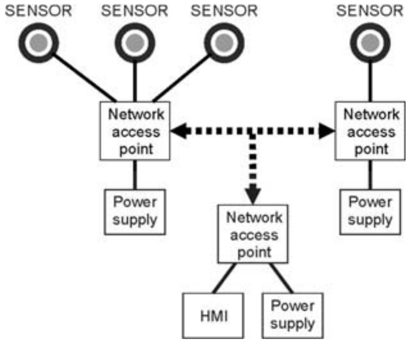


Figure 1. Typical industrial network

IEEE 802.15.4/ZigBee architecture advantages can be easily noticed in one of the projects conducted in our department [4]. Real-time, low power consuming network was needed in large generator vibration monitoring system. Network nodes were installed in remote and poorly accessible locations of the machine. Wires (both for power supply and for communication) were not to be used. Battery power supply was also not applicable because of explosion risk and the need of replacing them. Therefore, energy harvesting system was needed [5]. The disadvantage of this system was low power efficiency [6]. As a result, wireless network had to be especially designed to fulfil very strict power consumption requirements. The wireless nodes needed to enter sleep mode with a very low supply currents and they used special low power DC/DC converters [7, 8] Our IEEE 802.15.4 based network fulfilled the requirements.

III. Industrial Control Systems

Most of the industrial control systems are based on the Programmable Logic Controllers (PLC). The variety of such devices is vast and ranges from simple and inexpensive solutions for single machine control to very sophisticated systems utilized in most demanding and complex industrial applications.

Popular industrial controllers come with a support for different network platforms. Some systems feature a built-in support of real time protocols such as Genius or ProfiNET. Nevertheless, simple devices are limited only to MODBUS and text protocols. Therefore, because one of the requirements of this project was versatility, it was decided to consider only the MODBUS and text protocols.

P. Krasiński, B. Pękosławski and A. Napieralski are with the Department of Microelectronics and Computer Science, Lodz University of Technology, Lodz, Poland (e-mail: pkrasik@dmcs.pl)

The designer of the automation system is facing a problem when a wireless connection between a sensor and the PLC is required. Most of the currently available systems, based on Wi-Fi or GPRS, require efficient power sources. Power adapter or batteries are not always an answer. During the realization of the Polish Ministry of Science and Higher Education grant entitled “Real-time Wireless Sensor Network Supplied from Alternative Power Sources” a WSN powered by energy harvested from the vibrations was built. Conventional power sources were not applicable because wires were forbidden and impractical and batteries could cause explosion hazards.

An example of a typical, commercially available solution is a IO-Link product family from Balluff corporation. In this case, a number of sensors can be connected to a hub which is featured with a network port. Versions for different protocols are available. Nevertheless none is a wireless protocol. It is possible to connect the hub to the wireless network access point. Although this solution may be easy to establish, it does not fulfil the requirement for low power consumption. Both the hub and the access point can consume currents of hundreds of miliampers [9]. Another example of commercially available solution is a family of MGate products form MOXA corporation. A selection of gateways gives the designer a convenient solution to link an industrial network (for example Profibus or MODBUS) to Ethernet or wireless Ethernet. Besides, that for not power critical applications, this devices deliver a convenient solution, the current consumption of AWK-4131 Series access point are up to 890 mA and of MGate 5101-PBM-MN Series Profibus to TCP gateway 365 mA @ 12 VDC [10].

IV. MODBUS Protocol

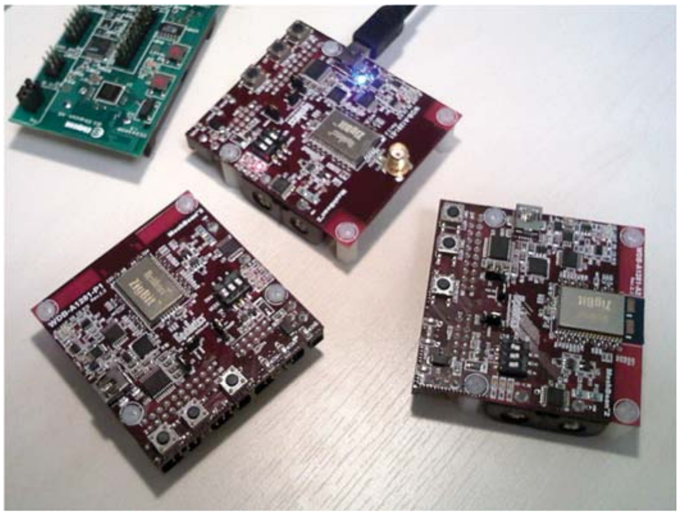
MODBUS protocol is one of the most popular protocols in industry. It was developed by Modicon Corporation in 1979 and since then, was implemented on many hardware platforms. The first version of the protocol is called MODBUS RTU and is based on RS-485 physical layer. In recent years an Ethernet version of MODBUS protocol was developed and called MODBUS TCP. Biggest advantages of MODBUS include its robustness, focus on industrial applications and that it is openly published and royalty-free. Consequently, a MODBUS based network can be easily built and ensure high interference immunity. Most PLC are featured with a built-in support of this protocol. Moreover, some families of microcontrollers also supports MODBUS. Libraries for the most popular families of microcontrollers are available.

V. Research Background

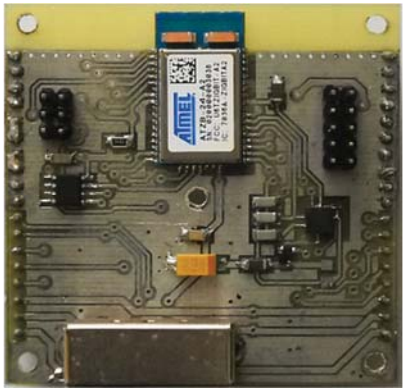
As it was shown in the previous paragraphs, designer of the automation system which requires real-time wireless connection of sensors is left with insufficient choice of solutions. Energy critical applications cannot make use of the commercially available devices. Basing on the experience gained during the realization of the Polish Ministry of Science and Higher Education grant entitled “Real-time Wireless Sensor Network Supplied from Alternative Power Sources” and on development of industrial systems a solution for this problem was suggested.

VI. The Hardware

The board of each sensor of the system comprises of IEEE 802.15.4 wireless network module and peripheral devices. The module comprises of an AVR microcontroller and necessary RF peripherals all integrated in compact and shielded package (Atmel ATZB-24-A2 module with ATmega1281 microcontroller and AT86RF230 ZigBee radio transceiver). Advantages of this solution include low price, high availability, good documentation and free development tools. Two solutions were used during the development process. At the beginning, Meschnetics evaluation boards, which are presented in Figure 2a, were utilized. To make the application of dedicated peripherals and power supply custom designed boards were used. The view of custom-designed PCBs of wireless node are shown in Figure 2b. The energy harvesting system was used. The transceivers are manufactured in different versions to suit versatile antenna types. Versions with built-in antenna and external antenna were considered. Texas Instrument Packet Sniffer was utilized to monitor the network traffic. Dedicated software delivered required communication functionality.



(a)

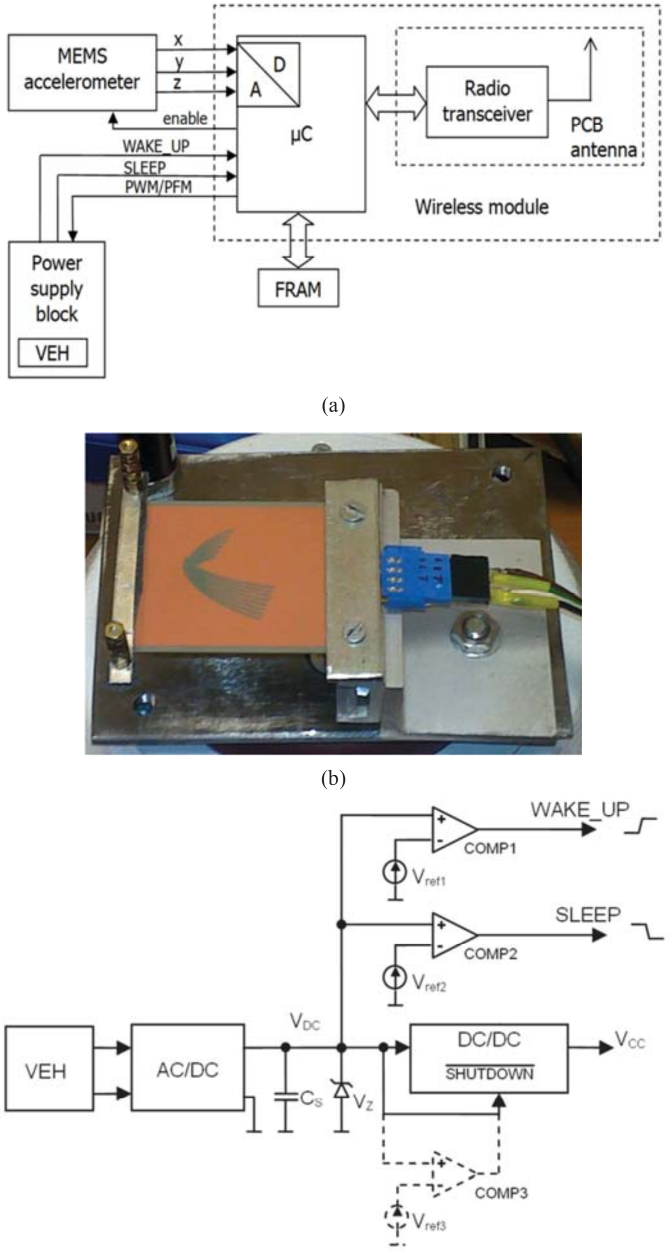


(b)

Figure 2. Meshnetics wireless network nodes (a) and custom-made PCB of wireless sensor node (b)

Wireless sensor nodes consist of power supply block with vibration energy harvester (VEH) and the main functional module with data acquisition, control and communication units. The wireless sensor node structure is shown in Figure 3a. The basic components of the functional module are triaxial micromachined accelerometer, Ferroelectric Random Access Memory (FRAM) chip, microcontroller and radio transceiver module mentioned above. An operation state of the data acquisition and transmission block depends on the state of WAKE_UP and SLEEP control lines, which are controlled by the power supply block.

Piezoelectric type of a VEH was used as a power source for wireless sensor nodes. Piezoelectric harvesters usually offer the highest generated electric power per generator volume and can be built basing on commercially available piezoelectric actuators, which makes these devices less expensive than off-the-shelf electromagnetic ones. Moreover, piezoelectric VEHs can be also constructed as micromachined devices, which makes them very attractive. The applied piezoelectric VEH consisted of a plate actuator with one of the ends clamped to the base and the other one with seismic mass fastened to it, which can move in one direction parallel to excitation vibration. Power levels up to 2.7 mW per cm^3 of piezoelectric element volume were available at vibration acceleration RMS value of 0.5 g and frequency of 100 Hz, corresponding to an AC electric machine rotor revolution frequency harmonic. The view of prototype piezolectric VEH is presented in Figure 3b.



(a)

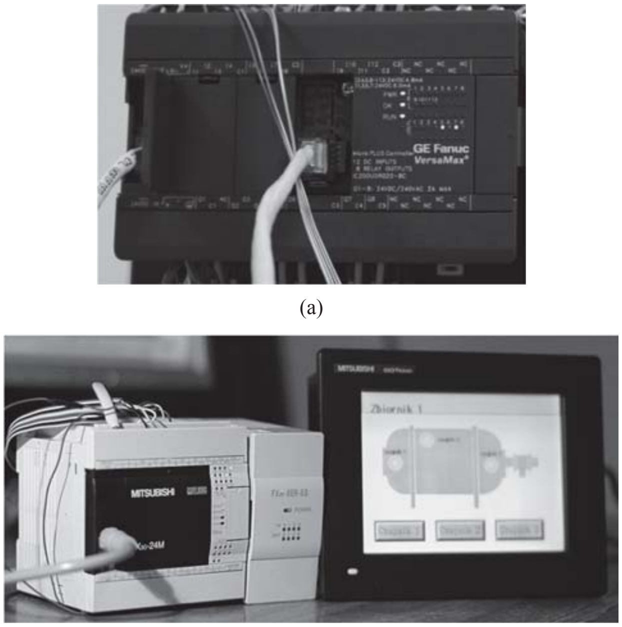
(b)

(c)

Figure 3. Block diagram of wireless sensor node (a), view of applied piezoelectric VEH (b) and adopted power supply block structure (c)

The applied power supply block structure (shown in Figure 3c) consists of AC/DC rectifier, energy storage supercapacitor, overvoltage protection Zener diode, buck-boost DC/DC converter and voltage comparators that monitor supercapacitor voltage level and control functional module power mode and DC/DC converter state. Some other energy harvesting power sources (such as a miniature photovoltaic cell) can be used instead of the VEH when the same power supply block structure is adopted and only small changes in hardware design may be necessary.

On of the targets of the developed system is universality and portability. Therefore, many PLC families were considered during development. Most of the work was done on GE Fanuc VersaMax Micro IC200UDR020 controllers. The most important parameters of the devices include 20 I/O points, built-in RS-485 port and additional expansion modules with more communication ports. Other PLC families included Mitsubishi FX-C and Panasonic FP-X devices. Common feature of all the devices was a built-in serial port with MODBUS protocol implemented. Figure 4 presents the applied PLCs.



(a)

(b)

Figure 4. PLCs used during research: GE Fanuc VersaMax Micro IC200UDR020 (a) and Mitsubishi FX-3G (b)

VII. The Network

Despite the fact, that many well established network protocols are available, none can fully suit given here requirements. To make things worse, a real-time functionality is featured only in a selection of more complex protocols. An example may be Genius and DeviceNet networks. Nevertheless, support for this networks is available in more advanced controllers or demand a separate, dedicated module. Due to the fact, that the solutions described in this paper were supposed to be universal, these network protocols were not used. On the contrary, Modbus RTU protocol is available even in the most simple solutions. It is also supported by many other industrial automation devices such as inverters or human interface devices. Therefore, only one network is needed for communication even in very complex applications.

A real-time functionality is not featured in Modbus protocol. Consequently, it is not recommended in applications where a system response time is critical. Serial I/O functionality, featured in PLCs, can deliver a solution. Most of the controllers are featured with an option to handle a customized serial protocol. As an example GE VersaMax industrial controllers will be considered and their programming in ladder language.

In GE family of PLCs, a Communication Request (COMM_REQ) block is used to initialize and execute communication. The first input variable of the function block determines the communication protocol and current activity. Other two are linked with the applied hardware and describe address of the communication module and port number. The same block is used to establish Modbus RTU and custom serial communication. As a result, the ladder program design methodology is the same for both considered protocols. The view of the COMM_REQ block in Proficy Machine Edition environment is shown in Figure 5.

Figure 6 presents the proposed network topology. The network consists of WLN segments that connect sensor and actuator nodes with coordinators and WN segments which interconnect PLCs and coordinator nodes. Communication in WN segments is based on Modbus protocol. WLN segments use IEEE 802.15.4 physical layer.

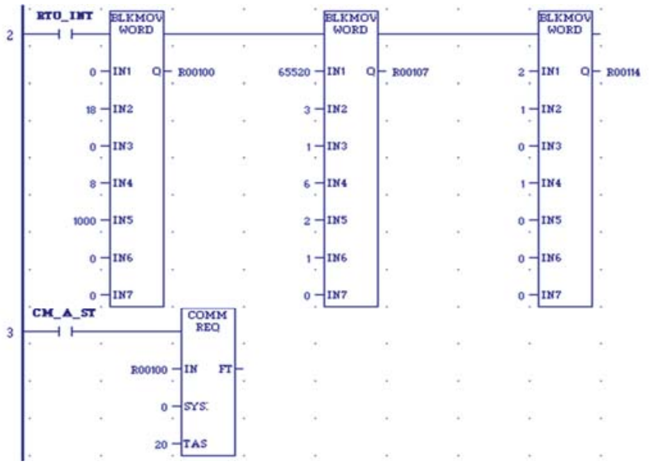
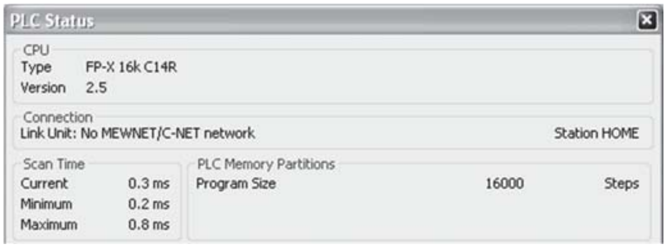


Figure 5. Modbus programming example in GE Proficy ME

One of the PLC features can be also used as a time restricting feature as shown in Figure 7. Scan time of the PLC program can be monitored and fixed in some applications. Scan time can be monitored not only with external computer but also within the program itself. For example, in Panasonic FP series PLC DT90022 register stores current scan time. If the scan time rises beyond a threshold value special steps can be taken. For example communication with HMI can be limited. Moreover, it is possible to force a constant scan time. This feature together with PLC outputs properties would result in guaranteed maximum response time. However, this approach can be recommended only in certain applications. In this method, response time can be longer than possible in current conditions and the CPU will spend some of the scan time idling.


PLC Status

CPU
Type FP-X 16k C14R
Version 2.5

Connection
Link Unit: No MEWNET/C-NET network Station HOME

Scan Time
Current 0.3 ms
Minimum 0.2 ms
Maximum 0.8 ms

PLC Memory Partitions
Program Size 16000 Steps

Figure 7. Run parameters of Panasonic FP-X C14R PLC (during tests)

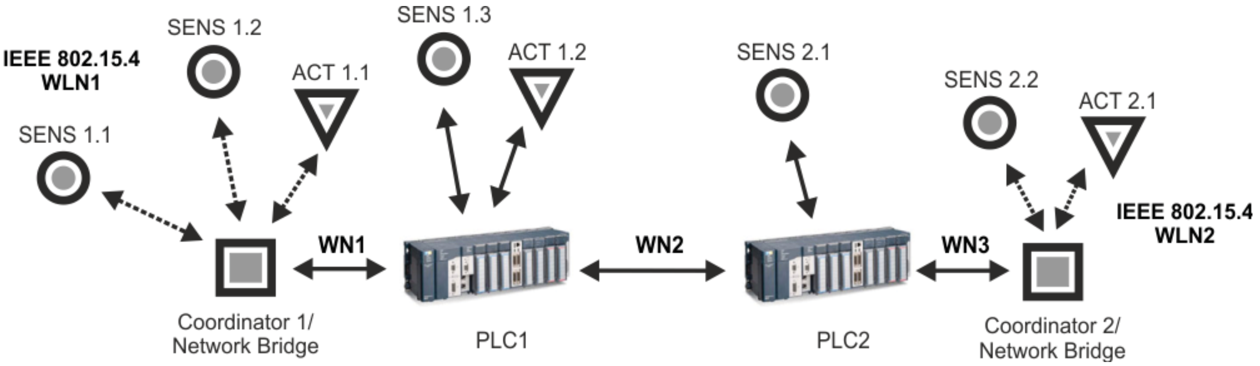


Figure 6. Described network topology

VIII. CONCLUSIONS

Industrial automation systems can take advantage from the integration of the real-time wireless sensor networks based on IEEE 802.15.4 standard. By utilizing a variety of available PLC features and affordable network modules it is possible to broaden the range of WSN applications in modern automation systems. Industrial solutions designers can make use of rich selection of tools available in modern PLCs. As it was described above, the system can be based on standard communication platforms and does not limit the designer of the system to a narrowed selection of controllers. A PLC-based automation control system can take advantage of a custom developed real-time wireless sensor network protocols.

REFERENCES

[1] H. Zhou; F. Zhang; J. Liu; F. Zhang: A Real-Time Monitoring and Controlling System for Grain Storage with ZigBee Sensor Network, 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009, WiCom '09, IEEE Conference Publications, E-ISBN : 978-1-4244-3693-4

[2] T. Ahonen, R. Virrankoski, M. Elmusrati, "Greenhouse Monitoring with Wireless Sensor Network", Proceedings of the IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications", Beijing, China, pp. 403–408, 12–15 October 2008

[3] IEEE Standards. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Computer Society

[4] B. Pękosławski, P. Pietrzak, M. Makowski, Ł. Szafoni, A. Napieralski, Study on Application of Piezoelectric Vibration Energy Harvesters for Powering of Wireless Sensor Nodes in Large Rotary Machine Diagnostic Systems, Technical Proceedings of the 2009 NSTI Nanotechnology Conference and Expo, NSTI-Nanotech 2009, 1, Houston, Texas, USA, May 3-7, 2009, pp. 530-533, 2009

[5] B. Pękosławski, P. Pietrzak, M. Makowski, A. Napieralski, "Zagadnienie modelowania generatorów przeznaczonych do zasilania bezprzewodowych modułów pomiarowych z energii odzyskiwanej z drgań mechanicznych", Materiały XIII Sympozjum Podstawowe Problemy Energoelektroniki, Elektromechaniki, Mechatroniki, PPEEm'2009, Wisła, Poland, December 14-17, 2009, Archiwum Konferencji PTETiS, 27, pp. 63-67, January 2010

[6] B. Pękosławski, P. Pietrzak, M. Makowski, A. Napieralski, "Enhancement of piezoelectric vibration energy harvester output power level for powering of wireless sensor node in large rotary machine diagnostic system (extended paper)", Sigma NOT, Elektronika-Konstrukcje, Technologie, Zastosowania, R.50, 12, pp. 31-35, December 2009

[7] B. Pękosławski, A. Napieralski, "Blok zasilania bezprzewodowego modułu pomiarowego współpracujący z generatorem odzyskującym energię drgań mechanicznych", Sigma NOT, Przegląd Elektrotechniczny (Electrical Review), R.86, 9, pp. 293-297, September 2010

[8] B. Pękosławski, P. Krasiński, A. Napieralski: Power Processing Circuits for Wireless Sensor Nodes Utilizing Energy Harvested from Mechanical Vibrations, Mixed Design of Integrated Circuits and Systems (MIXDES), 2011 Proceedings of the 18th International Conference, pp. 632 - 637, 2011

[9] Balluf Produsts + News, Doc. no. 871424, edition 1210, 2013

[10] MoxaMaster Catalog Vol. 121, 2012 Moxa Inc.

Piotr Krasiński was born in Łódź in 1984. He received a MSc degree in electronics and telecommunication in 2007 and is currently a PhD student at the Lodz University of Technology.

Mr. Krasiński is mainly involved in projects related with wireless sensor networks and industrial automation systems. He was a member of the team working on the Polish Ministry of Higher Education grant: "Realtime wireless sensor network powered from alternative power sources".

Bartosz Pękosławski was born in Lodz, Poland in 1981. He received MSc degree in electronics and telecommunications and PhD degree in electronics from the Technical University of Lodz, Poland in 2005 and 2010, respectively.

He works as an Assistant Professor at the Department of Microelectronics and Computer Science, Technical University of Lodz. His research interests include machine technical condition monitoring and diagnostic systems as well as ambient energy harvesting solutions for powering of wireless sensor nodes. Recently he is involved in a design of power processing circuit for truck recognition system in bridge structural health monitoring system (TULCOEMPA project).

Andrzej Napieralski received the M.Sc. and Ph.D. degrees from the Lodz University of Technology (LUT) in 1973 and 1977, respectively, and a D.Sc. degree in electronics from the Warsaw University of Technology (Poland) and in microelectronics from the Université de Paul Sabatié (France) in 1989. Since 1996 he has been the Director of the Department of Microelectronics and Computer Science. Between 2002 and 2008 he held a position of the Vice-President of TUL. He is an author or co-author of over 950 publications and editor of 21 conference proceedings and 12 scientific Journals. He supervised 48 PhD theses; six of them received the price of the Prime Minister of Poland. In 2008 he received the Degree of Honorary Doctor of Yaroslaw the Wise Novgorod State University (Russia).