IEEE 802.15.4 wireless network integration with PLC-based industrial networks

Piotr Krasiński, Lodz University of Technology

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.

1. Introduction

Recent advances in wireless technology makes it become more and more popular in industrial applications. Wireless Sensor Networks (WSN) can be utilized in security, supervision and control systems. Some of them demands real time operation of the network. Most popular standard for WSNs is IEEE 802.15.4 which describes both physical and software layers of network devices [1]. Nevertheless, it does not have built in real-time functionality support [2]. Moreover, integration of WSNs and traditional industrial control systems is still and open issue. In this article some solutions for this problem are presented.

2. 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 [2]. 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.

IEEE 802.15.4/ZigBee architecture advantages can be easily seen in one of the projects realised in our department [3],[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. The disadvantage of this system was low power efficiency [5]. As a result, wireless network had to be especially designed to fulfil very strict power consumption requirements. Our IEEE 802.15.4 based network fulfilled the requirements.

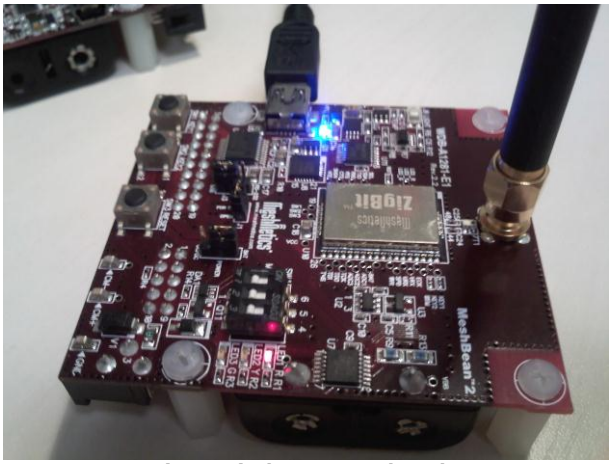

Fig.1. Wireless network node

3. 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 cheap solutions for single machine control to very sophisticated systems utilized in most demanding and complex industrial applications. Even the most simple PLCs have a built in communication port. Using unified communication protocols it is easy to expand or rebuild an existing system even with devices from different manufacturers or from different classes. It is also possible to link autonomous systems to get an integrated and centrally supervised system. Some systems features a build in support of real time protocols like Genius or ProfiNET. Nevertheless, simple devices are limited only to MODBUS and text protocols. This attribute makes it possible to integrate industrial networks with new, peripheral devices. In this article, possible methods of integrating the PLC-based network with IEEE 802.15.4 wireless network are discussed.

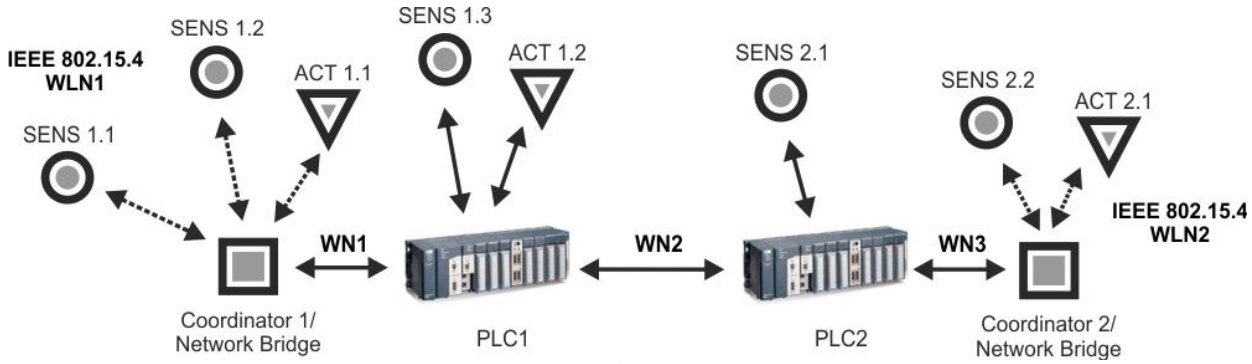

Fig.2. Example of described network

4. MODBUS protocol

MODBUS protocol was developed in 1979 by Modicon Corporation. It became a standard for industrial communication. Firstly, the protocol was based on RS-485 physical layer. This version is called MODBUS RTU. In recent years a MODBUS version for Ethernet hardware was developed and called MODBUS TCP. Some of the reasons of MODBUS success include its robustness, focus on industrial applications and that it is openly published and royalty-free. As a result, a MODBUS based network can be easily built and ensure high interference immunity. Support of this network is built-in most of PLCs. Moreover, some families of microcontrollers also supports this protocol which makes it easy to build a new device compatible with the standard. Even if a use of a non-MODBUS microcontroller is required a custom tailored library can be included in the program and MODBUS functionality can be achieved.

5. The Motivation

During the realization of the Polish Ministry of Science and Higher Education grant entitled "Real-time Wireless Sensor Network Supplied from Alternative Power Sources" work on IEEE 802.15.4 based real-time protocol was performed. The primal use of the network was in power plant generator vibration monitoring system [6],[7]. Real-time operation and low power consumption were the priorities during the development process. In parallel with this activity PLC based industrial systems were developed. This resulted in a plan to integrate both solutions which will result in one, universal network that will take advantage of real-time properties of wireless network and transfer them to classic wired networks.

6. Hardware platform

IEEE 802.15.4 wireless network is based on Atmel-Meshnetics ZigBit transceivers. This devices comprises of an AVR microcontroller and necessary RF peripherals all integrated in compact and shielded package. More advantages include low price, high availability, good documentation and free development tools. The transceivers were mounted on two board families. The Meschnetics manufactured evaluation boards and especially designed ones. The later were optimised for operation under power supplied from vibration energy harvesting system.
The transceivers are manufactured in different versions to suit versatile antenna types. Versions with built-in antenna and external antenna were considered.

During the wireless network development process Texas Instrument Packet Sniffer was used. It helped monitoring the network traffic. The device was connected to computer with dedicated software installed.

Different families of PLC were available during the development process. Most of the work was done with a help of GE VersaMax Micro IC200UDR020 controllers. 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. All of the controllers were featured with build-in serial port with MODBUS RTU support. Expansion modules makes it possible to connect the devices to two different networks.

7. The network

A priority during the integration of wireless network and PLC based network was to make it universal. It means, that the same methodology could be applied for PLC from different manufacturers and different classes. First result of such approach was exclusion of less popular protocols like Genius or DeviceNet. They are implemented only in more advanced controllers or require sold separately extensions. In contrary, Modbus RTU protocol is available even in most simple solutions. It is also supported by many other industrial automation devices like inverters or human interface devices. Therefore, only one network is needed for communication even in very

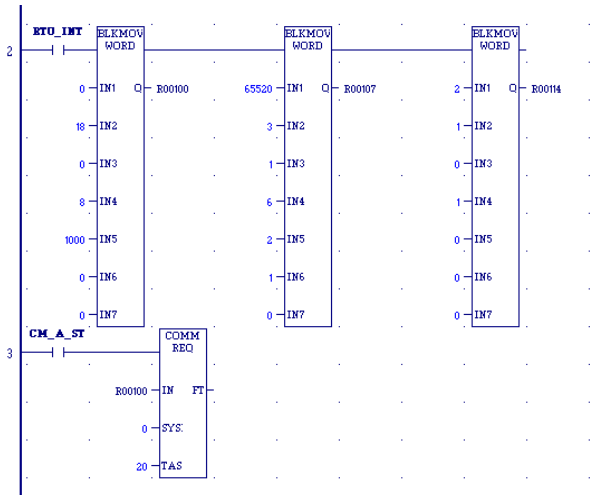

Fig.3. Modbus inicialisation in GE Proficy Machine Edition

complex applications.

The disadvantage of Modbus protocol is the lack of real-time operation support. Therefore, it is not recommended in applications where the controller response time is critical. Nevertheless, a solution comes from serial I/O functionality. Most of the controllers are featured with an option to write 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. First input variable of the function block determines the communication protocol and current activity. Other two are linked with the used hardware and describe address of the communication module and port. The same block is used to establish Modbus RTU and custom serial communication. As a result, used ladder program design methodology is the same for both considered protocols.

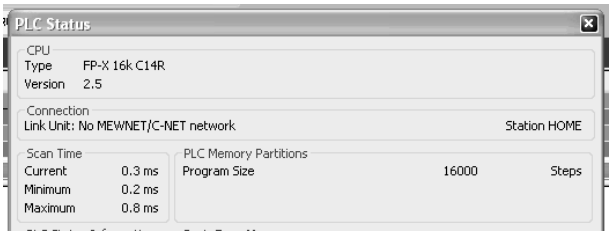

Fig.4. Run parameters (scan time) for Panasonic FP-X C14R PLC

One of the PLC features also can be used as a time restricting feature. Scan time of the PLC program can be monitored and in some applications fixed. 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 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. On the figure XX scan times for a working simple program are shown.

Interrupts are not to be forgotten when defined time response is considered. Their mechanism is similar to this known from microcontrollers so there is no need for further description. Execution of mentioned earlier COMM_REQ blocks from the

interrupts is another mean of controlling network time constraints.

8. Conclusions

Industrial automation systems can take advantage of real-time wireless sensor networks based on IEEE 802.15.4 standard. Industrial solutions designers can make use of vast selection of tools available in modern PLCs. Communication protocols utilizing PLC built-in serial port can be based on standard ladder language blocks. With the mentioned above solutions it may be possible to provide automation system designers with a powerful tools which will broaden the range of real-time wireless networks applications.

Bibliography

[1] H. Zhou; F. Zhang; J. Liu; F. Zhang: A Real-Time Monitoring and Controlling System for Grain Storage with ZigBee Sensor Network, IEEE Conference Publications, E-ISBN : 978-1-4244-3693-4

[2] 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

[3] Bartosz Pękosławski, Piotr Krasiński, Andrzej Napieralski: Power Processing Circuits for Wireless Sensor Nodes Utilizing Energy Harvested from Mechanical Vibrations, Proceedings of MIXDES 2011 conference.

[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, 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.

[6] 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.

[7] 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.

Author:

MSc. Piotr Krasiński
Łódź University of Technology
Department of Microelectronics
and Computer Science
ul. Wólczańska 221/223