Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Nr 51

XXVI Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE 2016

Oddział Gdański PTETiS

ANTI-THEFT LAB SECURITY SYSTEM BASED ON RFID

Bartosz MUDLAFF, Sylwia BABICZ, Janusz SMULKO

Gdańsk University of Technology, Faculty of Electronics, Telecommunication and Informatics,
tel.: +48 58 348 6368 email: sylwia.babicz@eti.pg.gda.pl

Abstract: The aim of the project is to design and create an electronic system, which can be used to protect laboratory equipment against theft. The main task of the system is to warn a person responsible for the facilities about any attempts made to steal equipment from a laboratory. In a case of an alarm situation, the system emits a sound signal (siren). The concept of the anti-theft security system based on RFID was developed on the basis of the analysis of the global market. Methods used to design each component of the system are described in detail, by presenting standards and electronic solutions applied in the developed hardware. Algorithms of the designed software embedded in each module and computer software are illustrated and explained. The method used to run and test the system is described.

Keywords: RFID, security systems, anti-theft systems.

1. INTRODUCTION

Increase in a number of large stores that offer unrestricted access to various products forces the manufacturers to develop new solutions in the area of security systems. The main requirement set for all anti-theft systems is to allow a customer to have a direct contact with the merchandise. One of the most popular anti-theft technologies used in commercial buildings is known as the Radio-Frequency Identification (RFID) [1]. Systems based on RFID use the wireless identification functionality [2, 3].

The demand for anti-theft systems is increasing not only in a case of commercial facilities. Along with the development of education and technological progress, schools and universities use more and more expensive equipment, which is directly used by students during laboratory classes. Due to the number of students, the supervising teacher does not have full control over each person and device. An anti-theft system that monitors the presence of laboratory equipment would allow the teacher to focus more on work with students. The main aim of the project was to design and create an alarm system that could protect laboratory equipment against theft. The anti-theft system based on RFID fulfills the requirement related to free access to laboratory equipment and can automatically protect it against theft at the same time. This technology [4, 5] has already been implemented in commercial facilities, but it is very expensive and inaccessible for an average user. The proposed system constitutes an alternative to such solutions [6] and retains all of their functional features.

2. RFID ALARM SYSTEM

Every RFID system is composed of three main elements: transponders, transmitter/receiver and a controller [7-9]. The transponder is a data carrier with non-volatile memory, antenna and, sometimes, with its own power source. The reader has an ability to wirelessly read (and sometimes write) information stored in the transponder. The controller, also known as the host, manages the entire system [10].

We underline, that various systems can be proposed (e.g. a single read/write device (RWD) can communicate with many protected facilities). Our considerations were limited to the solution a single RFID and single RWD. The configuration is economical in case of small protected area like the university laboratory. The lower cost and widespread availability of modules used in the presented system are the most important advantages comparing with commercial solutions. More advanced systems (like for e.g. Hybrid RFID systems [11], anti-collision systems [12-14]), would be unnecessary financial cost.

Today, numerous possibilities offered by RFID technology are reflected in the number of standards developed by industry-leading electronics companies. The most popular one, the UNIQUE standard [15], was used to design the presented system. In UNIQUE standard, the RWD (transmitter/receiver) is used only as a receiver. Because of the fact, that the main functionality of the device is getting information from transponders, it can be called a reader (Fig. 1). Such solution is usually used in simple identification systems, like e.g. teaching laboratory [16].

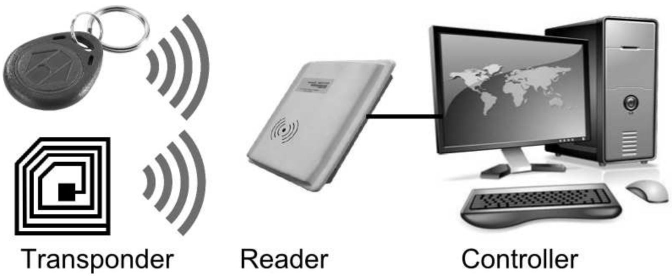

Fig. 1. Scheme of a RFID system

As an integrated tool, the alarm system needs to guarantee the following functionalities: detection of potential threats, signalization of an alarm situation and activation of other subsystems in order to allow for appropriate actions aimed at the elimination of the alarm situation. Taking the above into account, all system components were designed in accordance to their function. The basic elements of the alarm system are presented in Fig. 2. The most important part of the entire system is an alarm control panel. It collects information from the detectors, undertakes decisions about the alarm situation, activates sirens and sends messages to the property/merchandise owner. Communication between the user and the alarm control panel takes place through a manipulator.

3. CONCEPT OF THE SYSTEM

In order to determine exact technical parameters of the system and to design its operation, the following presuppositions were made:

1. target area of the system: laboratory room at a technical university;
2. system administrator: teacher, lecturer;
3. protected property: laboratory equipment;
4. operating time: long enough to ensure uninterrupted protection of items during laboratory classes.

It was assumed that the target workplace of the designed anti-theft system will be a laboratory room at a technical university, where classes with students are held. Students have free access to laboratory equipment used for their ongoing exercises. The person acting as a system manager will be a university teacher responsible for the equipment. The alarm system will protect laboratory equipment during classes, allowing for free access to them at the same time. The scheme of the system is presented in Fig. 3.

4. IMPLEMENTATION

The concept of the proposed anti-theft system requires a modular structure. The sensor is located on a laboratory station. Protected objects (like e.g. an oscilloscope or a measurement board) are placed within a range of the sensor. The sensor periodically checks the presence of the objects and reads the unique codes of their RFID transponders. After receiving a request sent from the control panel via RS-485 interface, the sensor sends information about the monitored object. The sensors are connected in a network with a bus topology compliant with a standard RS-485 interface. The sensor module consists of two components: a MP01611 reader compatible with RFID UNIQUE 125 kHz, and a logic circuit that receives the data sent by the MP01611 reader through the UART interface.

The control panel is located near the teacher's desk, at a place which is difficult to reach. The state of sensors network is periodically checked by sending requests to each sensor. Information received from the sensor (read code and RFID transponder information about the presence of the protected object) is stored in the memory unit. The control panel makes a decision about the emergency situation, e.g. absence of the protected item within the range of one of the sensors. The alarm situation is signaled via sirens and optical cameras, which register the potential thief. The user can access status information and system configuration through a personal computer (PC) application. The main block providing the system functionality is composed of a microcontroller with the integrated headquarters interfaces (VCP, RS-485). The microcontroller communicates with the control panel through the sensor network and the PC, and controls the operation of other components (e.g. camera, siren).

The PC acts as a security system keypad. The system administrator can program the operation of the control panel. Moreover, the PC creates a database of unique numbers of RFID transponders which are used to identify the protected objects. The database makes it possible for the PC application to inform the system administrator about the protected devices located within the range of the sensors. Another purpose of the application is to inform the academic staff about the cause of the alarm. This way, the teacher is able to effectively and quickly identify the stolen property and the thief. An event of theft, with its date and time, is recorded in a file. The software allows the teacher to preview the status of the protected objects, even if they are temporarily absent. PC is connected to the control panel through a USB interface configured to emulate a serial COM port (Communication Port).

The monitored facilities are marked with RFID UNIQUE flat stickers transponder. A small communication range (10 cm) enables fast and effective detection of undesired changes in positions of the objects. The transponder s' numbers may be read by the PC application.

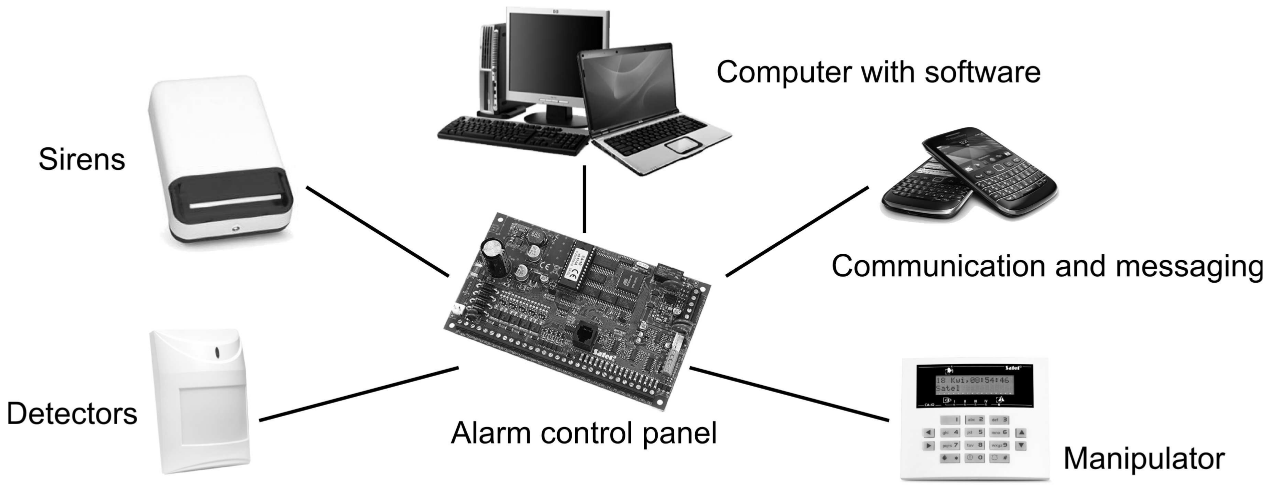

Fig. 2. Basic elements of the alarm system

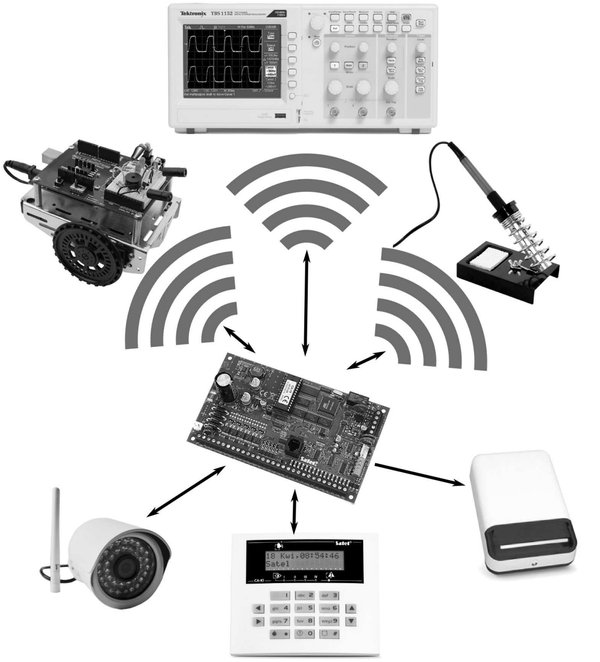

Fig. 3. Blocks of the proposed anti-theft system

The main element of the system is an ATmega162 microcontroller with an external quartz resonator of 12 MHz clock rate. The microcontroller has two independent UART interfaces used to communicate with the MP01611 reader and RS-485 network. The power supply of 5 V is provided by an L7805CV stabilizer. The system can be programmed with the use of ISP (In-System Programming).

After initialization of basic peripherals, the corresponding outputs of the microcontroller are set as inputs or outputs, both UART interfaces are initiated and a global flag allowing for the interrupts is activated. Next, the program checks if the request frame from the control panel is received. If so, the answer to the central panel is sent. The message contains a RFID number of the transponder recently registered in the detector range and the status of the protected object.

UNIQUE standard transponder s have a code length of 5 bytes. However, the MP01611 sends 12 bytes. The redundancy is caused by the fact that each byte of the unique transponder code is represented by two ASCII code digits. Moreover, the reader adds 2 additional bytes that indicate: CR (Carriage Return) and LF (Line Feed) flags. The algorithm checks if all 12 bytes are received. Next, all data are stored in a dedicated table in RAM memory. If within 0.5 s the next string with the same 12 bytes appears, it means that the protected object is still present within the reader range. After that, the system returns to a state of checking the receiving frame and the procedure is repeated infinitely.

ATmega128 microcontroller is the heart of the central panel. The implemented PCF8586 real-time clock is supplied with the battery which provides the necessary power even if the basic supply is disabled. The communication between them takes place through an I^2C (Inter-Integrated Circuit) interface. The UART interface of ATmega128 in combination with the MAX487 transceiver enables communication with detectors network. On the other hand, the communication with the PC application takes place through the FT232RL converter. The central panel is recognized by the PC as a new device connected to a serial port COM. The entire central panel module is supplied by 19 V DC.

The central panel software is started through the initialization of peripherals and both UART interfaces. Next, the algorithm checks if the flag determining a time when the request is sent to the next detector is active. If so, the central panel clears the flag, creates and sends the request frame to the next detector. If an answer from the detector is available, the second flag is activated. The flag is checked in the second step of the algorithm. The frame is received besides the main loop, by the interrupt handling of the UART interface. The data from the detector is processed and stored in RAM memory with a unique RFID number of the transponder. Moreover, the information about the presence of the transponder within the detector range is stored. If the detector does not respond in 30 ms, it means it is not available. The third flag determines the communication with the PC. In this case, the frame is also received besides the main loop, by the interrupt handling of the second UART interface. If the flag is active, the program clears it and the data from the PC are processed. The last part of the algorithm analyzes the data from all detectors and, potentially, makes a decision about an alarm.

The PC application was created in Java in Netbeans IDE virtual machine. Before initialization of the system, it is necessary to configure the connection settings between the application and the central panel. The application enables performance of alarm actions and makes it possible to define the type of situation that causes an emergency situation. Such situations include: sensor address mismatch, absence of the object or sensor or transponder mismatch. Alarm situation may be signalized by LEDs or by a buzzer. All actions are stored in a TXT log file, allowing for easy and remote monitoring of the system.

5. TESTS

The test began with reading the unique RFID numbers of transponder s. Next, the database with all transponder numbers and object names was stored in a TXT file. The central panel was configured and programmed in the PC application (Fig. 4a). Before running the monitoring part of the PC application, two transponder s were placed within the range of the proper detector. The third sensor was not connected and the alarm in this case was switched off. The detected objects were the same as monitored, so their alarm status was "OK" (Fig. 4b). Then, the first object was removed from its detector range. Moreover, a wrong object was placed within the second detector range. Both cases resulted in an alarm situation, registered by the PC application and caused the activation of the optical signaler (bulb) and siren (Fig. 4c). All operations were written down in the TXT log file (Fig. 4d). The test proved that the entire system works properly.

6. CONCLUSIONS

The paper presents a fully functional alarm system for academic laboratory. The anti-theft system monitors laboratory equipment and signals incorrect placement or absence of the monitored objects. Affordable price of the components allows for the use of the system in most academic laboratories. Such solution allows the teacher to fully focus on students and conducted classes.

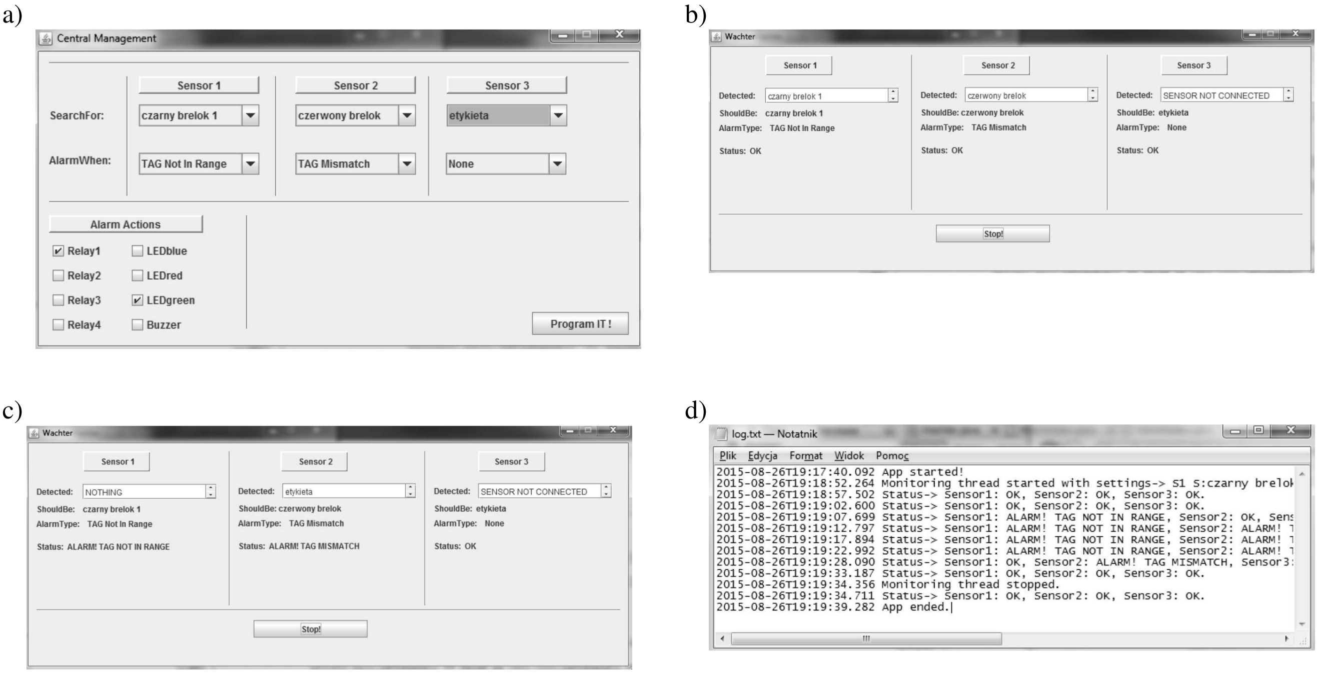

Fig. 4. View of graphical user interface in: a) programming part, monitoring part, b) non-alarm situation, c) alarm situation and d) log file.

7. REFERENCES

1. Lowe P.: Electronic anti-shoplifting system employing an RFID tag, United States Patent number 5,874,896.
2. Finkenzeller K.: RFID Handbook: Fundamentals and Applications in Contactless SmartCards, Radio Frequency Identification and Near-Field Communication, Wiley, 2010.
3. Dębowski L.: Technika RFID i jej aplikacje, Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej, No. 22, pp. 3136
4. Hunt D., Puglia A., Puglia M.: RFID: A Guide to Radio Frequency Identification, Wiley, 2007.
5. Ranasinghe D. C., Sheng Q. Z., Zeadally Sh.: Unique Radio Innovation for the 21st Century: Building Scalable and Global RFID Networks, Springer Science & Business Media, 2010.
6. Dębkowski W., Szlendak M.: System RFID kontroli dostępu do pomieszczeń. Praca dyplomowa magisterska. WETI PG, 2011.
7. Daniel M. Dobkin: The RF In RFID: Passive UHF RFID In Practice, Newnes, 2012.
8. Wójtkowicz-Kowalska M., Rebech D.: Wykorzystanie technologii RFID do zabezpieczenia zbiorów w wolnym dostępie w bibliotece Uniwersytetu Papieskiego Jana Pawła II w Krakowie, Kraków, 2013.
9. Dębowski L.: Technika RFID i jej aplikacje, Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej, Nr 22, 2006.
10. Koślacz G.: Systemy alarmowe, terminologia i klasyfikacja, Elektronika Praktyczna, nr 6/96.
11. Kozłowski K., Bizewski K., Michałek M., Kulas Ł., Nyka K.: Hybrid RFID System, 18-th Internacional Conference on Microwaves, Radar and WIRELESS Communications, 2010.
12. Shih S.-H., Sun P.-L. Yen D. C., Huang Sh.-M.: Taxonomy and survey of RFID anti-collision protocols, Computer Communications, 29, 2006.
13. Cha J.-R., Kim J.-H.: Novel Anti-collision Algorithms for Fast object identification in RFID system, Proceedings of the 2005 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.
14. Klair D. K., Chin K.-W., Raad R.: A survey and tutorial of RFID anti-collosion protocols, IEEE Communications Surveys & Tutorials, Vol. 12, No. 3, 2010.
15. EM Microelectronic- Marin SA:, EM4102 – Read only contact less identification device, data sheet, 02/2005, Rev. F., 2005.
16. Noga K.M.: Cyfrowe sterowanie z zastosowaniem układów programowalnych, Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej, Nr 40, 2014.

SYSTEM ZABEZPIECZENIA PRZED KRADZIEŻĄ POMIESZCZEŃ TECHNIKĄ RFID

Tematem podejmowanym w pracy jest projekt systemu zabezpieczenia pomieszczeń laboratoryjnych przed kradzieżą. Na podstawie analizy rynku, opracowano koncepcję systemu alarmowego z zaimplementowaną techniką RFID. W sposób szczegółowy opisano metody realizacji poszczególnych modułów systemu. Omówiono algorytmy działania oprogramowania przeznaczonego na mikrokontrolery i komputery osobiste. Przedstawiono przebieg testów działania zrealizowanego sprzętu oraz sposób obsługi oprogramowania.

Słowa kluczowe: RFID, UNIQUE, system alarmowy, system antykradzieżowy.