Turkish Journal of Science & Technology
Volume 8(1), 15-21, 2013

A Tutorial and an Application of SM130 RFID Module and Mifare Contactless Smart Memory Card

Ö. Fatih KEÇECİOĞLU , Mustafa ŞEKKELİ , Metin SALİHMUHSİN
Department of Electrical and Electronics, Faculty of Engineering, Kahramanmaras Sutcu Imam University, K.Maras, Turkey
msalihmuhsin@ksu.edu.tr

(Geliş/Received: 22.05.2012; Kabul/Accepted: 08.08.2012)

Abstract: In this study, we have developed a driving circuit based on a PIC 18F4520 microcontroller to control overall operation of an RFID tagging system. Our system utilizes a SonMicro SM130 RFID transmitter/receiver module in order to read manufacturing ID of a Mifare 1K contactless smart memory card. An RF antenna is used to perform data communication between the module and the tag. A graphical LCD is utilized to prompt messages to the user as well as display information received from the module. Our system successfully worked and manufacturing ID of the Mifare 1K memory card was displayed on the screen of the graphical LCD.

Keywords: SM130 RFID Module, Mifare RFID Tag, PIC 18F4520 Microcontroller

SM130 RFID Modülünün Mifare Temassız Akıllı Hafıza Kartları ile Kullanımı ve Uygulaması

Özet: Bu çalışmada bir RFID barkod sisteminin çalışmasını kontrol etmek üzere PIC 18F4520 kullanılarak bir sürücü devresi tasarlanmıştır. Sistemimiz SonMicro SM130 RFID alıcı/verici modülünü kullanarak bir Mifare 1K temassız akıllı RFID barkodunun fabrika seri numarasını okuyarak ekranda göstermektedir. Alıcı/verici modülü ile barkod arasında veri alışverişini sağlamak için bir RF anten kullanılmıştır. Kullanıcıya yönelik mesajlar ve barkoddan okunan bilgilerin gösterimi için bir adet grafik LCD kullanılmıştır. Geliştirmiş olduğumuz sistem başarılı bir şekilde çalışmış ve Mifare 1K RFID barkodunun fabrika seri numarası okunarak grafik LCD ekranında gösterilmiştir.

Anahtar Kelimeler: SM130 RFID Modülü, Mifare RFID Barkodu, PIC 18F4520 Mikrodenetleyicisi

1. Introduction

RFID (Radio Frequency Identification) is a technology that allows performing remotely storage or retrieval of data from a chip which is known as a tag. Although its history goes back to 1950, it has been increasingly used in variety of fields after 1990ies. Nowadays, RFID systems have enormous amount of applications ranging from supply chain management of supermarkets to personal ID systems such as ID cards and passports [6-8].

In general, an RFID system consists of a transmitter/receiver module, an antenna and a tag. The transmitter/receiver module communicates with the tag through the antenna in order to perform desired operations. There are many studies conducted on RFID systems. Below, we will summarize couples of them which are related to our work.

Wu et all. gave a good survey on current RFID applications [1]. Their paper started with a brief history of invention of these systems and gave a comparison in between usage of barcode and RFID. Then, they had mentioned current RFID technologies and some applications of these systems. Examples of RFID applications they had mentioned were supply chain management with RFID tags in supermarkets, facilitation of RFID systems in toll systems at highways or parking lots, ticketing with RFID tags at exhibition or stadiums, security and identification systems in which RFID systems embedded inside ID cards or passports.

Cole et all. illustrated a good tutorial on various RFID tagging systems followed by a brief overview of electromagnetic compatibility constraints imposed by some countries [2]. Then they gave a good survey on effects of various noise sources in detection of passive tags by RFID readers.

Pope et all. described an 13.56 MHz RFID system they have developed [3]. They first explained briefly differences between near field and far field RFID systems. Then, they gave operating characteristics of their RFID system which they called ISD model C. They explained noise immunity of their 13.56 MHz system over RFID systems in LF band. Then, they gave 2 applications of their system: Drilling identification system for oil and gas wells and air cargo tracking system.

Hori et all. proposed a multi sensing-range method for position estimation of passive RFID tags [4]. Their method was based on using 3 different transmission powers for an RFID reader to search passive tags. These sensing ranges were called long, middle and short ranges. Their method was applied as follows: A mobile robot is provided with an RFID reader. The reader had 3 different transmission powers as mentioned above. The robot first searched for a tag with the long range power. If a tag was detected, its position was then refined with usage of middle and short sensing range transmission powers. They illustrated effectiveness of their method through computer simulations.

2. Method

Our goal in this study is to implement an RFID system that is capable of sensing RFID tags remotely. A microcontroller based control circuit is developed to control overall operation of the system and process incoming/outgoing information. Microchip PIC 18F4520 micro controller is used to establish the control circuit. The block diagram of the circuit is given the Figure 1.

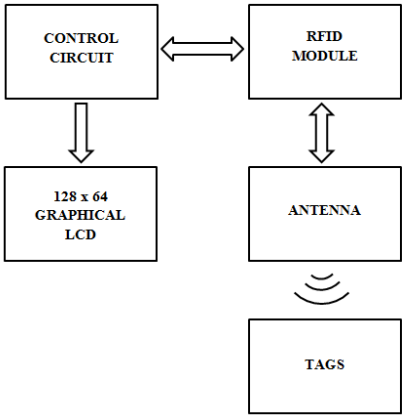

Figure 1. The Block diagram of the RFID system.

We have used SonMicro SM130 RFID receiver/transmitter module in our application [5]. The module consists of a transmitter and a receiver. There is an antenna which is connected to the module separately and performs propagation of commands from module to the tag and receiving of information from the tag by the module in terms of electromagnetic waves. The transmitter/receiver unit has 2 watt power and hence the communication between the module and the tag can be successfully performed remotely up to a distance of 10-15 cm in between them. Commands sent from module to the tag are coded in terms of electromagnetic waves by the transmitter unit. These commands are received by the RFID tag and processed in order to perform operations required by the command. Then, the tag returns a response of the command to the module in terms of coded electromagnetic waves. This response is encrypted as well. The RFID receiver unit receives the response, decrypts it, and then decodes it in order to extract the information sent from the tag. The received data is then sent to

the control unit by the module through one of two serial communication procedures: UART or I2C.

The SM130 RFID module operates at 13.56 MHz base frequency. It provides contactless data communication up to 106 Kbit/s with RFID tags through an appropriate antenna. The data communication is done in a secure and encrypted format which makes the RFID module suitable applications where secure access and fast data transfer is needed. The module supports Mifare 1K, 4K and ultra-light memory contactless smart memory tags. For our application we have utilized Mifare 1K memory tag. SM130 module has 23 commands to control its operations and perform read/write and other necessary operations on RFID tags. The list all commands is given in the [5].

Mifare 1K tags operate at frequency of 13.56 MHz. They are known as passive tags since there is no battery needed to operate the tag. They can be classified as many bits and read/write tags. The 1k memory they contain is a non-volatile memory [2]. A Mifare 1K contactless smart memory card (tag) consists of 3 main sections and it's own antenna unit [5]. The antenna consists of a few turns and connected directly to the tag. The three sections are an RF-Interface, a digital control unit and an EEPROM unit. The Figure 2 shows a block diagram of the tag.

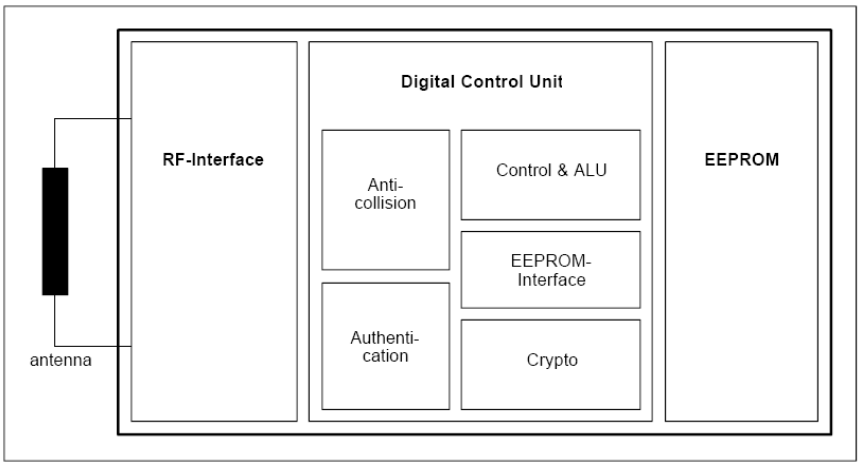

Figure 2. The block diagram of the Mifare 1K tag.

In the above figure, the RF-Interface section consists of a voltage regulator, a clock generator, a power on reset utility, a rectifier and a modulator/demodulator unit. The commands sent from SM130 module is demodulated by the demodulator unit of the tag before it has been processed. Similarly any data read operation from the tag could be made after the data has been modulated by the modulator unit of the RF interface.

The digital control unit is responsible to implement commands received from the RFID module. It consist of Arithmetic Logic Unit (ALU) and Control unit, an EEPROM interface an anti-collision unit, an Authentication unit and a Crypto unit. The anti-collision unit is used to differentiate one tag from another when there are several tags around the module which has to be processed simultaneously (one at a time). The authentication unit enforces the usage of a set of keys in order to access any sector in the EEPROM area. Each sector has a set of 2 unique keys known as key A and key B. The control and ALU unit performs control and arithmetic operations on data blocks such as increment or decrement a value stored in the EEPROM. The crypto unit encrypts data which are read from the tag by read operations and hence allows a secure data exchange between the tag and the module.

A Mifare 1K RFID tag's memory is organized in terms of sectors and blocks. It has 16 sectors. Each sector has 4 data blocks namely: data block0, data block1, data block2, data block3. Each data block contains 16 bytes of available space. Data block 0, 1, and 2 of each sector are used to read data from the tag, write data into the tag or as a value block. A value block is defined as a 4 byte signed integer of which its value can be incremented or decremented by the module. Value block feature of the tag is used for electronic purse applications. Data block3 of each sector is called sector trailer. The sector trailer is used to hold access conditions and keys in order to perform any operation on the related sector. Without providing access bits and a correct key, neither data can be written into that sector nor can a read operation be performed on it. Sector 0 of the tag has an exception. Data block0 of the sector 0 is called manufacturer block and holds a unique 4 byte serial number of the tag. This data block is read only and cannot be overwritten. The Figure 3 shows memory organization of the Mifare 1K contactless smart card as explained above.

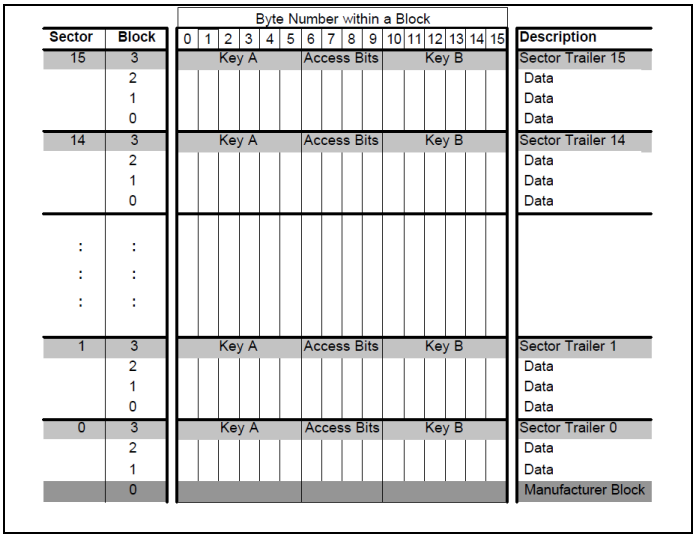

Figure 3. Memory organization of a Mifare 1K tag.

There are 3 steps which are needed to access a block of memory in the tag. The first step is that the tag has to be selected with the tag select command. At the second step, the module has to send a proper key to the tag for the sector to be processed. Proper values of the key choices are: keyA, keyB or keyA/keyB (keyA or keyB). This process is called authentication. At the third step, desired operations can be made on the authenticated sector. It is important to note that only the memory blocks in the authenticated sector can be accessed. Furthermore, if a block of memory is set to have read access with keyA and write access with keyA/keyB, then providing keyB to the tag will only allow a write operation to be made. An attempt to perform a read or a write operation without providing a proper key will cause the tab to halt. Flow chart in the Figure 4 outlines the procedure to access a memory block of a Mifare 1K tag.

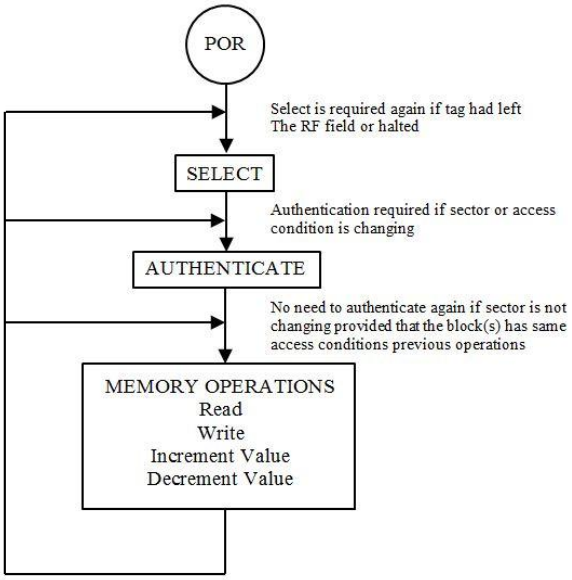

Figure 4. The procedure to access a memory block of the Mifare 1K tag.

We have developed a driving circuit based on PIC 18F4520 microcontroller in order to control and operate overall operation of the SM130 module. The driving circuit communicates with RFID module through UART serial communication protocol. A program is written in the assembly language of the PIC 18F4520 in order to perform all operations of the RFID system. There is a graphical LCD connected to the PIC 18F4520 which has 64 rows and 128 columns. The LCD is used to prompt messages to users as well as display any information sent from the module. The schematic of the driving circuit is given in the Figure 5.

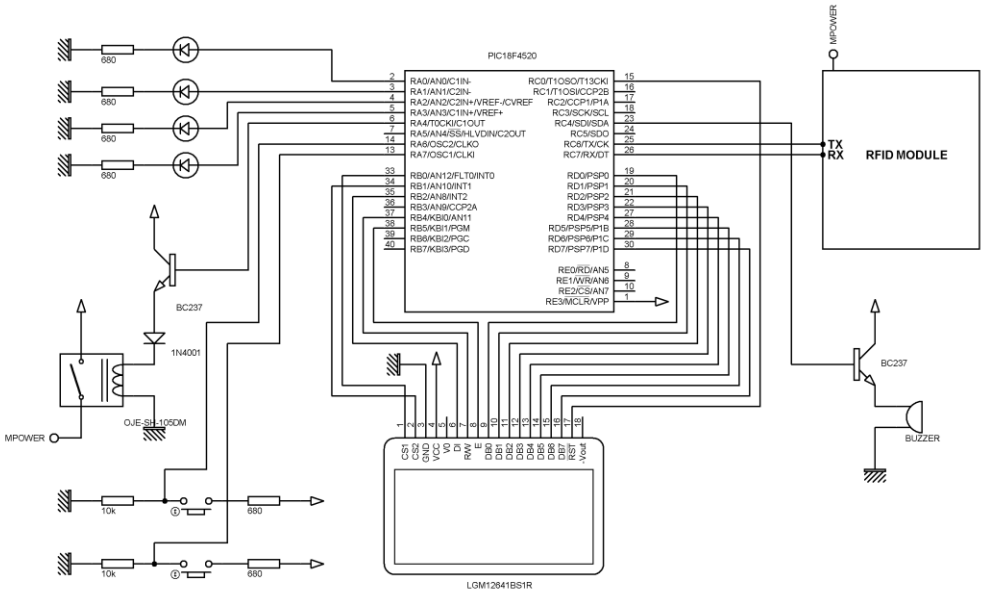

Figure 5. The Schematic of the RFID system.

3. Results

We have developed an operated the RFID system which consists of the driving circuit, the SM130 module, the antenna and the RFID tag successfully. The system is able to perform identification of a Mifare 1K tag and read manufacturer ID of it. The system works as follow:

1- The user is prompt to press a button in order to read the manufacturer ID of a Mifare 1K tag.

2- When the user presses the button, the control circuit of the system sends commands for an initialization and tag select procedures to the SM 130 module. The module performs the required operations on the tag and sends back the manufacturer ID of the tag. The module then sends this information to the control circuit. The PIC 18F4520 microcontroller based control circuit displays the manufacturer ID on the graphical LCD. In order to perform another read operation on a tag, the user has to press the same button used to initiate the above process again.

For any operation to be made on the tag successfully, the tag has to be placed around the antenna for a distance of less than 15 cm. Photos of the system during operation are given in the Figure 6.

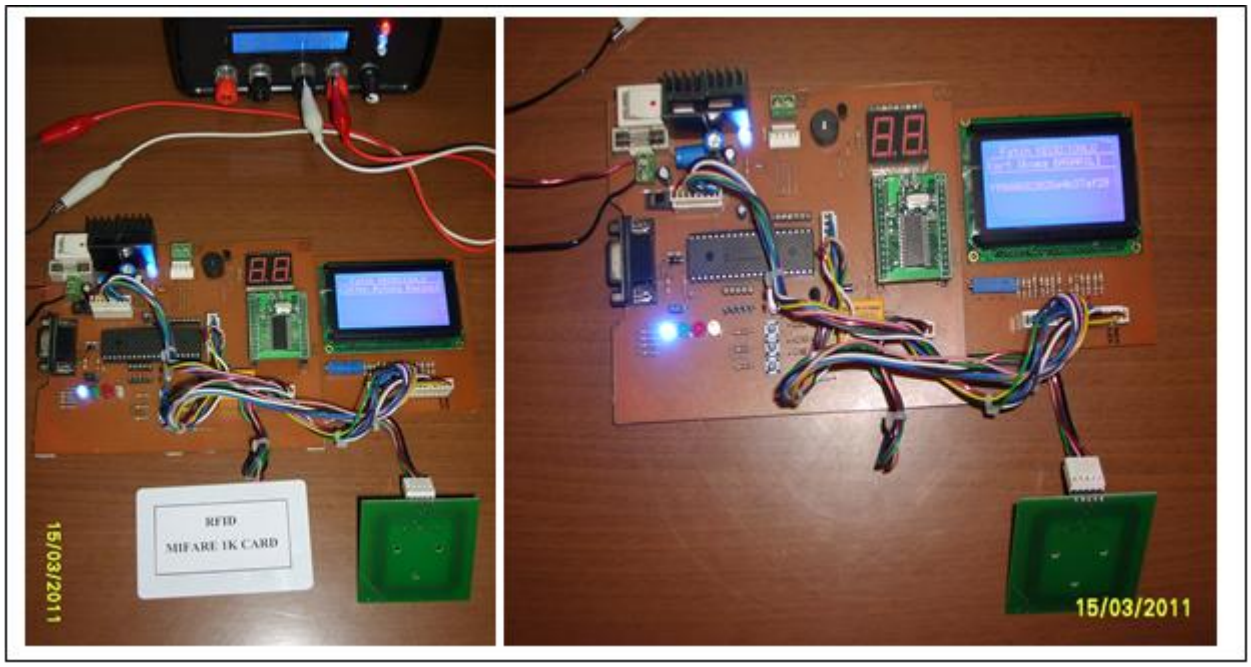

Figure 6. Two photos of the RFID system while it's in operation.

4. Conclusion

We have developed a PIC 18F452 based system which uses a SM 130 RFID transmitter/receiver module and an RF antenna and performs reading of manufacturer ID of a Mifare 1K tag. The information read is then displayed on a graphical LCD. Our system successfully reads and displays the manufacturing ID of the tag. In the future works, we will utilize read/write and other operations of SM130 module on the tag and use the RFID system we have developed in an application.

5. References

1. Wu, D., Wing, W.Y.NG., Yeung, D.S., Ding, H. (2009). A Brief Survey on Current RFID Applications. IEEE Proceedings of Eight International Conference on Machine Learning and Cybernetics, Baoding, 2330-2335.
2. Cole, P.H., Hall, D.M., Loukine, M.Y., Werner, C. (1995). Fundamental Constraints of RFID

Tagging Systems. Third Annual Wireless Symposium, Santa Clara, California, 294-303.

3. Pope, G.S., Loukine, M.Y., Hall, D.M., Cole, P. H. (1997). Innovative Systems Design for 13.56 MHz RFID. Wireless and Portable Design Conference, Burlington, Massachusetts, 240-245.
4. Hori, T., Wada, T., Ota, Y., Uchitomi, N., Mutsuura, K., Okada, H. (2008). A Multi-Sensing-Range Method for Position Estimation of Passive RFID Tags. IEEE International Conference on Wireless and Mobile Computing, Networking & Communications, 208-214.
5. SM130 module and Mifare 1K tag Technical Documentations by Sonmicro Electronics at http://www.sonmicro.com/en/downloads/Mifare/ds_SM130.pdf , last access date by us at 27/07/2011.
6. Finkenzeller, K. (2003). RFIF Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition, John Wiley and Sons Inc., New York.
7. Chawla, V., Ha, D. S. (2007). An Overview of Passive RFID, IEEE Communication Magazine, Volume 45, Issue 9, Pages 11-17.
8. Gao, Y., Yang, D., Ning, W. (2010). RFID Application in Tire Manufacturing Logistics International Conference on Advanced Management ScienceVol 3, Pages 109-112.