Development of a Microcontroller-Controlled Security Door System.

A.O. Oke[1], O.M. Olaniyi[2*], O.T. Arulogun[1], and O.M. Olaniyan[2]

[1]Department of Computer Sciences and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.
[2]Department of Computer Science and Technology, Bells University of Technology, Ota, Ogun-State, Nigeria.

[*]E-mail: olaniyimikail@bellsuniversity.org

ABSTRACT

Over the years, several security measures have been employed to combat the menace of insecurity of lives and property. This is done by preventing unauthorized entrance into buildings through entrance doors using conventional and electronic locks, discrete access code, and biometric methods such as the finger prints, thumb prints, the iris and facial recognition. In this paper, a prototyped door security system is designed to allow a privileged user to access a secure keyless door where valid smart card authentication guarantees an entry. The model consists of hardware module and software which provides a functionality to allow the door to be controlled through the authentication of smart card by the microcontroller unit.

(Keywords: access control, security, card reader, smart card, computer control)

INTRODUCTION

Security over the years has been a source of concern to organizations and companies. This has caused quite a significant amount of capital being budgeted for improvements on security systems, simply because it has been discovered that the access control system mechanism is an important part of an organisation. One of the important security systems in building security is door access control. The door access control is a physical security that assures the security of a building by limiting access to the building to specific people and by keeping records of such entries [3].

Most doors are controlled manually especially by security personel employed by the organisation, through the use of handles and locks with key to operate the locks. Examples are banks, hotels, motels and so on; some are controlled by switches while others are controlled by the biometrics technique. The idea of this technique is to enable automatic verification of identity by computer assessment of one or more behavioral and/or physiological characteristics of a person. Recently, biometric methods used for personal authentication utilize such features as the face, the voice, the hand shape, the finger print, and the iris patterns of an individual [4, 5 ,7]. Each method has its own advantages and disadvantages based on their usability and security [6, 9].

In [1] two distinct technologies in Artificial Intelligence are outlined: Artificial Neural Networks and Facial Recognition were used to develop a security door system where authorization of facial appearance of privilege users in the database is the only guarantee for entrance. In the system, the personal computer processes the face recognized by the system digital camera and compares data with privileged users in the database. The control program either sends a control signal to open the electromechanical door upon facial existence or deny entry.

Also in [3], an intelligent voice-based door access control system for building security was proposed. The proposed intelligent voice-based access control system is a performance biometric which offers an ability to provide positive verification of identity from an individual's voice characteristics to access secure locations (e.g. office, laboratory, home). In the system Perceptual Linear Prediction (PLP) coefficients features are extracted from the person voice data and then an Adaptive Network-based Fuzzy Inference Systems (ANFIS) is used to develop models of the authorized persons based on the feature extracted from the authorized person voices.

Although, these proposed models provided a novel approach to door security systems, they are dependent on the control program written on computer system and provided access control using the parallel port. The PC's parallel port is affected by cross talk and significant reduction in performance in long distance parallel transmission. Besides, computer process control systems are generally affected by high initial costs and increased dependence on maintenance [2].

In other to overcome the problems of these PC-based door acesss security control systems, this paper presents prototyped low cost, low complexity door security system designed to allow a privileged user to access a secure keyless automated door where valid smart card authentication guarantees an entry. In the proposed system an automated door is controlled with a card reader and the card reader is controlled by a control program embedded in a microcontroller unit. Implementing the system with a microcontroller will be of great value, cheaper, portable and much benefit to organizations who consistently seek a better means of door access control for their firms.

THE SYSTEM DESIGN

The system consists of a hardware module and an application program for microcontroller unit developed in Mikrobasic programming language. The hardware module comprises three stages: The card reader, the door electromechanical relay interface, the microcontroller stage and the power supply unit.

The control action is actually performed by the microcontroller. It processes the signals (requests) that are inputted from the card reader upon the insertion of the valid smart card at the entrance. The output section of the microcontroller is connected via relays for the desired operational actions. The stages involved in this design are shown in the Figure 1.

The Card Reader: A card is a small piece of plastic that holds information in a magnetic strip or microprocessor used in activities such as getting cash from the Automated Teller Machines (ATM) or making phone calls (i.e. SIM) or opening and closing of a microcontrolled based door. Based on highly optimised construction, the card readers are very compact with a discreet and cost effective design. The readers are usually made with durable plastic to withstand harsh environments. The microcontrolled door card reader is usually equipped with a two way-supervised and secured communication, for the person to gain entrance through the door and for him to exit through same door when inside.The term used to describe this is card-in and card-out.

The two-way communication between a card reader and the microcontroller is usually monitored. The Card In reader is located outside and used to enter into a building. If there are multiple doors in the room for one to gain entrance, the Card In database is incremented for all the doors in the room. Such a database list is technically known as a Muster list. The card out reader is located inside the building and used when exiting a building. In the case of multiple exit doors in a room, the card out database is incremented for all the doors in the room.The card acess system is configured to generate a list of people that have 'Carded In' to enter the building.

Upon entrance, user's name stays on the muster list until the user 'Carded Out' when leaving the building. Figure 2 is a schematic diagram of the basic principle involved. In the proposed system,the card reader is a slot where the card will be inserted by the user. On insertion of the card into the card reader, the card reader decodes the information in the card by conducting current from one end of the card to another.
The decoded signal is send to the microcontroller unit which works according to its program code specification.

Microcontroller PIC16F84A: The system is designed around PIC16f84A microcontroller. The PIC16f84A is used because it is readily available and is relatively simple to understand. The PIC implements the software based control and commands the electromechanical interface circuit to_open and/or close the door. The PORT (RB6, RB7) of the PIC was designed to send the output control signals to the door circuit through the relay switch of the electromechanical interface circuit and the PORT A (RA0 and RA1) is configured as analog input to receive voltage values that specify the state of denial and acceptance of entrance parameter form the card reader. These parameter controls produces voltage which is reduced to a maximum of 5V s.

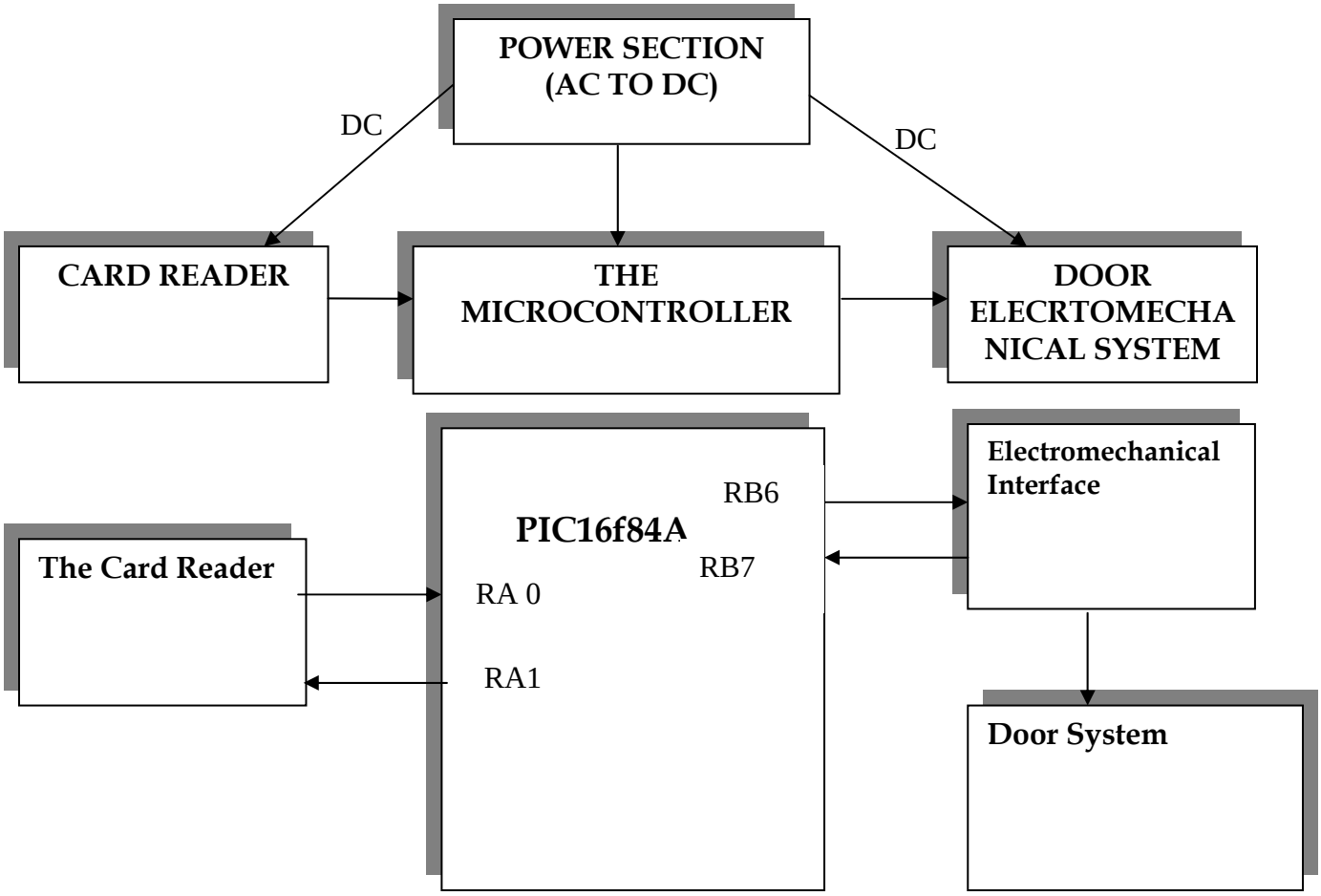

Figure 1: The Functional Block Diagram of the System.

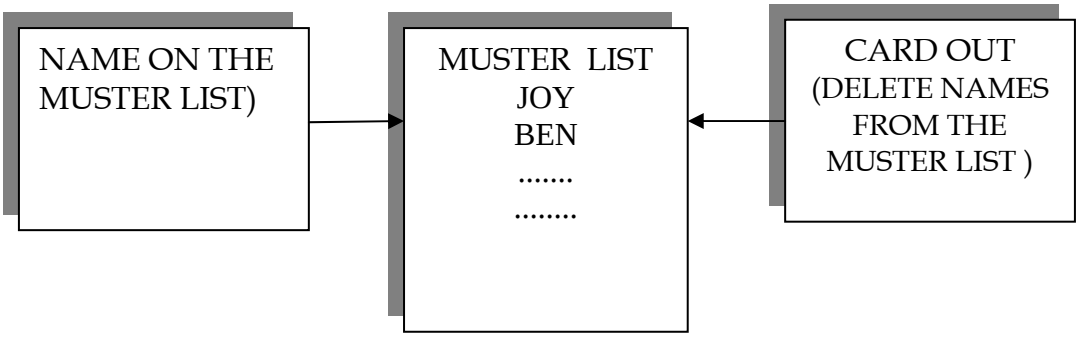

Figure 2: Muster List Card Access Configuration.

For example, if the card reader accepts valid card upon the decoding from the PIC, 5V is produced and 0V for an invalid card. The voltage is read through the PORT A of the PIC as analog input and is interpreted to mean high or low depending on the input. PORT A status is read, the status (1 or 0) determine if the electromechanical interface circuit is triggered or not (1 = YES, 0 = NO) [7, 11].

Electromechanical Door Interface Circuit: In the model, a simple 12v DC motor and Rack and Pinion motion transmission systems were used to provide translatory motion for the door to open and close upon the command of the

microcontroller unit to the relay circuitry as shown in Figure 3.

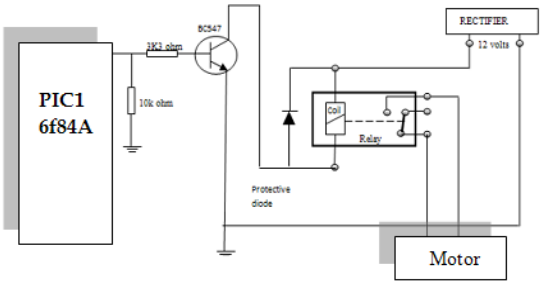

Figure 3: The Interface Circuit.

The relay circuit is responsible for performing the switching action that energizes the motion transmission systems to perform door translatory motion operations [8, 12]. The relay circuit transforms the electrical signal from the PIC into mechanical movement that performs a switching mechanism to allow the door to open or close.

THE SYSTEM CONTROL PROGRAM

The system control program can be accomplished using program written in either low level or high level language such as C, Java, mikrobasic. A compiler for a high level language helps to reduce production time. Although inline assembly is possible, the programming was done in the Mikrobasic language. The source code has been commented to facilitate any occasional future improvement and maintenance. The code written followed all the three steps of microcontroller program development that is, Compilation, Burning and Evaluation before it was transformed to the microcontroller through the programmer.A fraction code fragment for the system is given below :

Program Autodoor
Dim i as byte
Main:
TRISB = 0
TRISA = 0
PORTA =0
PORTB = 0
Eloop:
PortB.2 = 1 on green light(ready)
Delay_ms(1000)
portB.2 = 0
if PortA.2 = 1 then
PortB.4 = 1 on red light(busy)
portB.5 = 1
delay_ms(2000)
PortB.5 = 0
Delay_ms(5000)
portB.6 = 1 open door
delay_ms(5000)
PortB.6 = 0 close door
PortB.4 = 0
End if
Goto Eloop repeat
End.

THE SYSTEM OPERATION

After the system is turned on, the door indicator's light emitting diode(LED) come ON after some few seconds, indicating that the door is in the ready state. The colour for the ready state is yellow. The yellow LED continually blink to show that the card slot is ready to accept the card. The yellow colour also indicates that there is no card inserted into the card slot, hence a card can be inserted as shown in Figure 4.

When a valid card is inserted into the card slot (the reader), the LED light changes from its yellow colour to the red colour. The red colour signifies the busy state of the door.The card reader only functions when the LED is in the ready state. The PIC16F84A decodes the name on the card and compares it with specific name on its memory.The privilege user gain entrance to a restricted application area by triggering the interface circuit.

The interface circuit thererefore triggers the direct motor driven electromechanical door to slide from the left to the right, opening the door for five seconds. The door however closes after some few seconds. The number of seconds it takes the door to slide back is a function of how the microcontroller is programmed.The timing can be changed if need be by modification of the program code in the microcontroller. This is the competitive advantage of designing this proposed door access control system around PIC16f84A microcontroller unit.

However, an intruder is denied an entry upon the insertion of an invalid card.The overall system design and system operation diagram are shown in Figure 5 below.

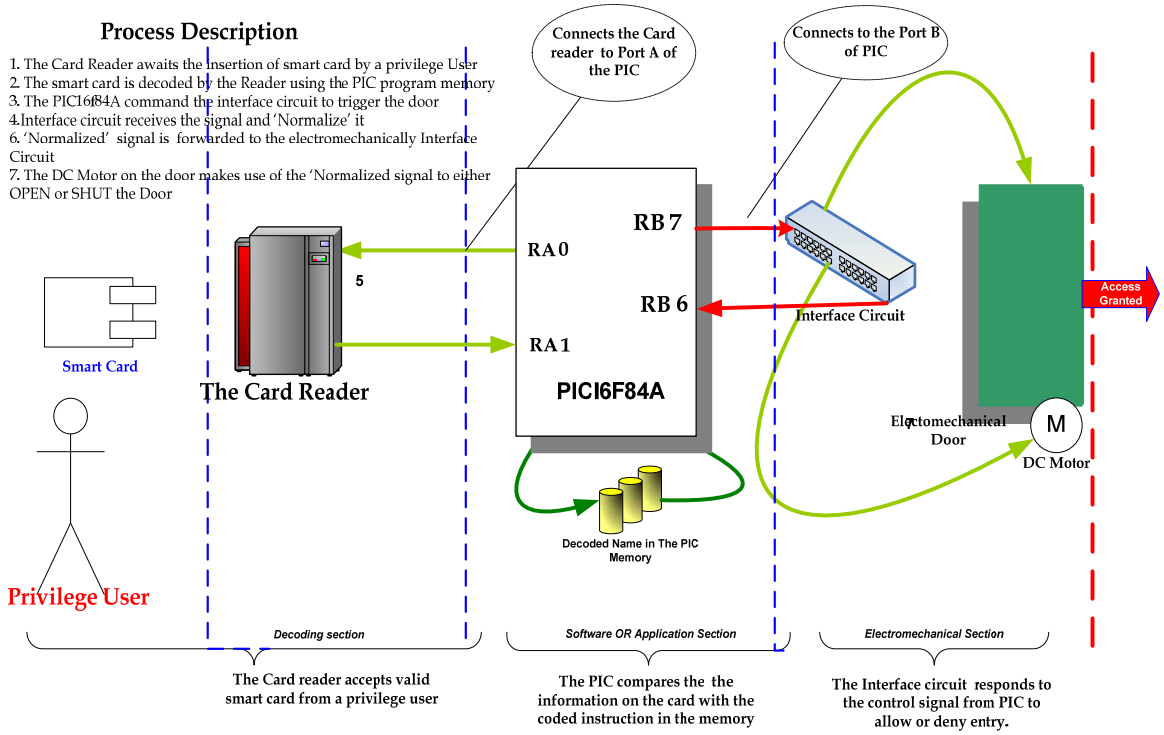

Figure 4: The Overall System Design and System Operation Diagram.

Figure 6: The Proposed Model.

CONCLUSION

This paper has successfully presented a functional, low cost and low complexity microcontroller based door access control system. The proposed security door system adopted a valid smart card to authenticate and/or deny entry to a room or building. A real-life equivalent of the prototype can be developed with minimal development costs and with relatively low operational costs for environment where high degrees of security are required like banks, military research areas, and big private investment companies.

REFERENCES

1. Omidiora, O., M. Olaniyi, and A.A. Ipadeola. 2008. "Development of Security System Using Facial Recognition". *Pacific Journal of Science and Technology*. 9(2):377-386.

2. Arulogun, O.T., E.O. Omidiora, and A.O. Owoseni. 2006. "Development of a PC Based Household Electricity Management System". *International Journal of Electrical and Telecommunication Systems Research*. 1(1):12-18.

3. Winda, W.O. and Mohammed, S. 2007. "Intelligent Voice-Based Door Access Control System Using Adaptive-Network-Based Fuzzy Inference Systems for Building Security". *Journal of Computer Science*. 3(5): 274-280.

4. Kung, S.Y., M.W. Mak, and S.H. Lin. 2004. *Biometric Authentication: Machine Learning Approach*. Prentice Hall: Englewood, NJ.

5. Osadciw, L., P. Varshney, and K. Veeramachaneni. 2002. "Improving Personal Identification Accuracy Using Multi sensor Fusion for Building Access Control Application". In: *Proceedings the Fifth International Conference for Information Fusion*. 1176- 1183.

6. Zhang, D.D. 2000. *Automated Biometrics: Technologies and Systems*. Kluwer Academic, Prentice Hall: Englewood, NJ.

7. ADSL. 2009. "All Data Sheet Library". (Retrieved March 21, 2009). http://www.alldatasheet.com.

8. Wikipedia. 2009. "Relay". (Retrieved on March 21, 2009). http://www.en.wikipedia.org.

9. Fournier, J., H. Li, S.W. Moore, R.D. Mullins, and G.S. Taylor. 2003. "Security Evaluation of Asynchronous Circuits". In: *Proceedings of Workshop on Cryptographic Hardware and Embedded Systems (CHES2003)*, LNCS Volume 2779:137 - 151.

10. Hageman, S. 2008. "PIC Development on a Shoestring". (Retrieved on May 24th ,2009). http://www.sonic.net/~shageman.

11. Microchip Technology, Inc. 2009. "PIC16F84A Data Sheet". (Retrieved May 30, 2009). http://ww1.microchip.com/downloads/en/devicedoc/39582b.pdf

12. Adoghe, A.U. and I.A. Odigwe Adoghe. 2008. "Remote Monitor and Controller System for Power Generators". *Pacific Journal of Science and Technology*. 9(2):344-350.

SUGGESTED CITATION

Oke, A.O., O.M. Olaniyi, O.T. Arulogun, and O.M. Olaniyan. 2009. "Development of a Microcontroller-Controlled Security Door System". *Pacific Journal of Science and Technology.* 10(2):398-403.

Pacific Journal of Science and Technology