Vault's Floor Security Sensor With RFID Access Using Microcontroller

Mohd Firdouz bin Bahtiar
Faculty of Electrical Engineering
Universiti Teknologi MARA, 40000 Shah Alam, Selangor
dosh_ance@yahoo.com

***Abstract* – Precious items like money, jewelry and expensive antiques are usually kept in a vault or at home. Whether it is a bank or at home, security has been the number one priority to keep each and every item safe from theft. Although, most hi-tech security systems are expensive, the fact that it actually runs on simple mechanism such as sensors for input and some interface to communicate with the consumer i.e: an LCD display, makes it probable for a low cost security sytem to be produced with the same hi-tech effects.**

A solution to these problems is to design an embedded system that provides an application of RFID for access and a photo sensor for the guarding system that runs on low power and at a lower cost to compare to the commercialize security sensor. The design is just a module to demonstrate the basic function of the floor security sytem that will be observed by the PIC16f877a microcontroller by Microchip.

The embedded system automation will be made at such a low cost but demonstrates the same functionality as the commercialize security system. This paper describe an application of RFID for access whereby the system provides security surveillance towards a certain designated ground or floor.

Users will be given the RFID smartcard for the access pass identity, the designated floor will then be armed with a source of light (laser pointer) and an LCD as indicator should any message will be given to the user. The system uses a microcontroller for the simple algorithm of the signal processing. The algorithm for the RFID access and the security sensor was performed on a commercial software to control the microcontroller and interfacing circuits.

Index Terms — **LASER, Microcontrollers, PIC16F877A, PIC application, security system, .**

1. INTRODUCTION

The number of entrepreneurs involved in commercialize security system increase every year due to the demand of security for both homes, industry and banking.

There are two types of business; a commercial and small business. For commercial purposes, usually more than 400 users can be registered unto the system whereby system can store large database for users identity storage. Small business refers to home access system usage. Somehow, these systems are usually monopolized by the commercial business too.

The importance of security has been prioritize for safety purposes. Levels of security has ben increased eventhough a home, office or a parameter has been guarded by human security guard. Commercial security equipment is designed for commercial purposes and the level of complexity of the system is very high.

In addition , high investment on equipment and devices is required. Precise manual guide and knowledgeable, skilled people are required to operate the machine.

Catering to the need of private security usage, a simpler security system is proposed to provide a cheaper but effective security access to an area that can be applied to vaults, homes, buildings or any parameter that is decided for the system to be applied to.

This controller system provides an efficient solution for exact identification of access card acknowledgement of the user.

Identity of the user can be kept into the microcontroller's memory during the code programming of the security system. Sequence of operation of the system depends on the programming development.

2. METHODOLOGY

2.1. Hardware design

This project involves the combination of hardware and software design. The processes of developing this project are divided into two main parts which are hardware and software development. The complete security system will have 2 inputs and 2 outputs to be interfaced to the microcontroller unit for signal processing.

The figure below shows the overview of the hardware design interfacing.

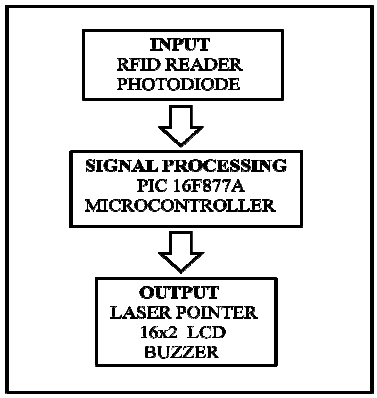

Figure 1: Design Overview

The main idea of the design is to replicate the lower part of the wall to house a laser pointer (light source), several mirrors (reflectors), a photodiode (sensor input) and a case to house the LCD (graphical output), the RFID reader (identity input) the PIC16F877A microcontroller (signal processing).

RFID reader will acquire the identity of the user for allowable access. The photodiode as the sensory subsystem will be off during the passage. Sensory subsystem is made of laser pointer for the light source of photoresistor sensory input for the microcontroller.

Control system process data that is responsible for access arming and disarming and output uses PIC16F877A microcontroller SK40B start-up-kit during the development. Features of PIC microcontroller start-up-kit can be found in the SK40B

Electronic system diagram of the security access system is shown in figure 2 with the appropriate sensors, drivers and microcontroller.

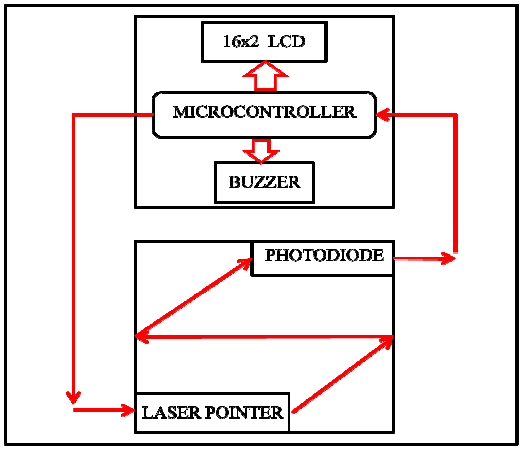

Figure 2: Complete sequence of the design

2.2 Controller

This is where all the analysis, computations, decisions are made.

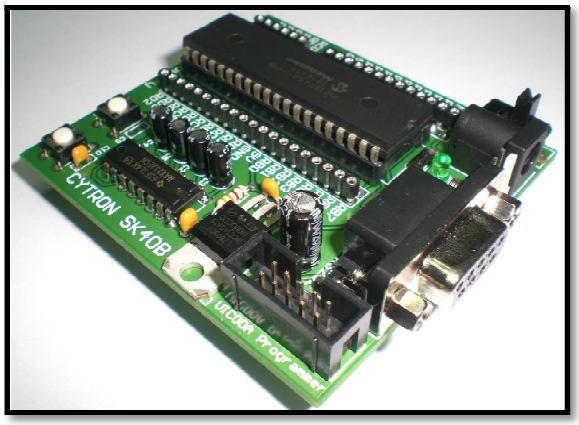

Figure 3: PIC microcontroller start-up-kit SK40B

Figure3 shows the PIC microcontroller board that is used during the development of this project. The SK40B based on PIC 16F877A, offers adequate port to interface LCD, laser pointer and sensor for the project.

In the project, port D is used as output for LCD. Port A for the RFID reader I/O port (designated port : A0,A1,A2)and input for the photodiode input circuit (designated port: A3). The LEDs are for indication as for lockdown, access allowed and intrusion alert (designated port: A5, E0 and E1 respectively). Figure 4 is the simulated schematic diagram using MPLAB's Proteus ISIS plug-in.

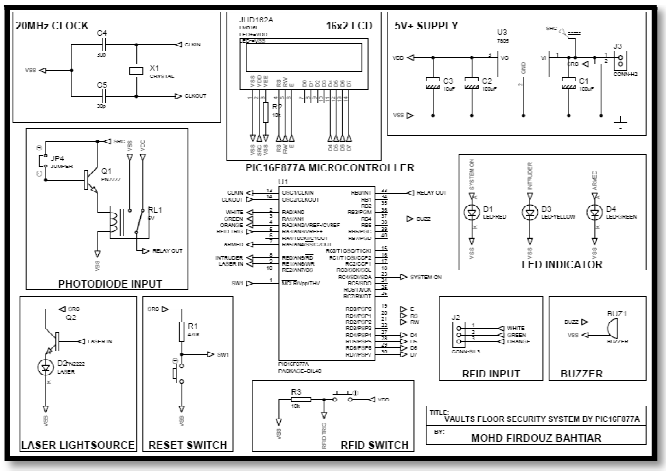

Figure 4: Schematic diagram using PROTEUS ISIS.

2.3 The WIEGAND RFID reader

Figure 5: The HID Wiegand RFID reader from BizChip

The HID (Hughes Identification Devices) Wiegand Protocol RFID (Radio Frequency Identification) reader is used together with the users identification access card. Only the designated smartcard ID owner will be allowed for access through the system.

Figure 6: The Wiegand RFID smartcard from BizChip

2.3.1 Wiegand™ Format

The term Wiegand is applied to several characteristics related to access control readers and cards. Wiegand is:
1. A specific reader-to-card interface
2. A specific binary reader-to-controller interface
3. An electronic signal carrying data
4. The standard 26-bit binary card data format
5. An electromagnetic effect
6. A card technology

“Wiegand format”, typically refer to the general concept of security card data encoding. Wiegand format, is also often understood to mean the standard 26-bit format, which is a very specific arrangement of binary card data.

Some basic facts:
• A format describes what a number means, or how a number is used. The format is not the number itself,
• The number of bits does not indicate the format except for standard 26-bit. For example, there are over 100 different 34-bit formats alone.
• Within a given bit length (34-bit, 37-bit, etc.), the size and location of each data element may change. For example:
•One 34-bit format may have an 8-bit Facility Code starting with bit #2.
•Another 34-bit Facility Code may be 12 bits starting with bit # 21.
• The capability of the access control panel will dictate what formats will and will not work.

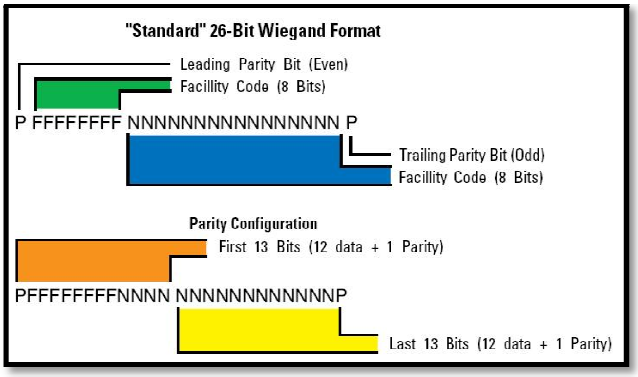

Figure 7: 26-Bit Wiegand Public Format

2.3.2 The Wiegand Reader-to-Controller Interface

An interface defines how two devices communicate with one another. Various (Hughes Identification Devices) HID readers can communicate with access
control panels using a variety of well-established, industry-standard interfaces including:
• Wiegand
• Serial (RS232, RS422, RS485)
• Clock-and-Data (Magnetic Stripe Track/2) – Also known as ABA format.

Concentrating on the Wiegand interface since it is the most prominent industry interface for card access control, the Wiegand interface consists of three conductors (wires) called Data Zero (usually green), Data One (usually white), and Data Return (usually black). All current standard HID reader types are available with a Wiegand interface. The three wires carry Wiegand data, also called the Wiegand signal.

Since the card data is binary, the reader simply receives the radio frequency (RF) data from the card, translates it from RF to Wiegand protocol and sends the complete binary string to the controller. Zeros travel on the green wire, ones on the white wire and the controller combines the two strings of characters into the original set of binary data.

The reader performs no processing or quality checking of the data. It simply receives the (RF) data from the card and converts it to Wiegand protocol for immediate transmission to the controller.

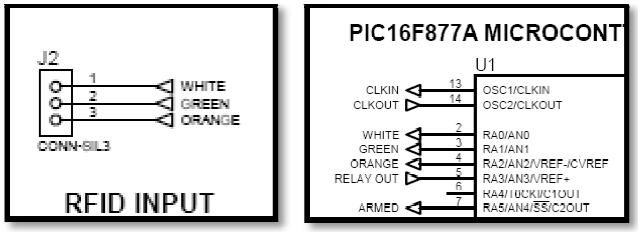

Figure 8: Designated RFID input

Many panels use hexadecimal math because it is compact, and directly represents binary.

2.4 LASER POINTER as sensor light source

A laser pointer is a small laser designed to highlight something of interest by projecting a small bright spot of coloured light onto it. Most laser pointers have low enough power that the projected beam presents a minimal hazard to eyes for incidental exposure.

Some higher powered laser pointers are faintly visible via Rayleigh scattering when viewed from the side in moderately to dimly lit conditions.

With maximum output of less than 5m Watts and at 650m the usage of the class 3A laser product in the system works as a light source after multiple reflections by mirrors. The light source will then reach on the photoresistor surface. If the light source to the photoresistor is broken, the light source will not reach the photoresistor hence giving a low input for the sensor therefore triggering the system and indicate that the security on the perimeter has been breached.

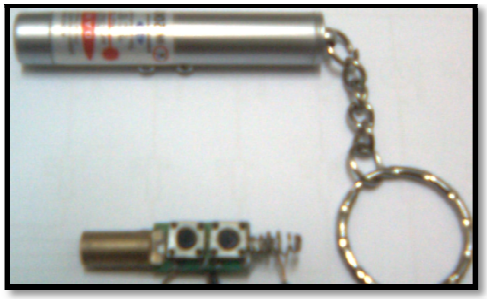

Figure 9: Laser pointers encased (top) and without case (bottom).

However, if the light source remains tight to the photoresistor surface, it will always trigger high indicating constant light source and without intrusion.

It is chosen due to the intensity of the light that makes the photoresistor's resistance to decrease hence allowing current to be supplied to the PIC as input.

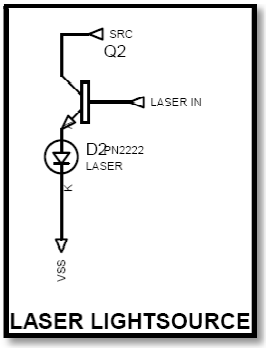

Figure 10: LASER as lightsource

2.5 Photoresistor as sensor

A photoresistor or light dependent resistor or cadmium sulfide (CdS) cell is a resistor whose resistance decreases with increasing incident light intensity. It can also be referenced as a photoconductor.

A photoresistor is made of a high resistance semiconductor. If light falling on the device is of high enough frequency, photons absorbed by the semiconductor give bound electrons enough energy to jump into the conduction band. The resulting free electron (and its hole partner) conduct electricity, thereby lowering resistance.

Photoresistors can be classified by its function and construction.

Features of photoresistors are:

1)Excellent linearity with respect to incident light
2)Low noise
3)Wide spectral response
4)Mechanically rugged
5)Compact and lightweight
6)Long life span

In the project, the photoresistor acts as a sensor as it is being exposed to the LASER when the system is being armed. This will always trigger a high input for the PIC, indicating no intrusion to the parameter.

Otherwise, when the LASER fails to reach the surface of the photodiode, this will trigger a low input for the PIC hence indicating that there is an intrusion.

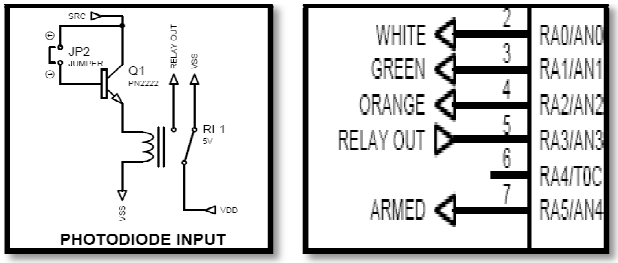

Figure 11: Input from the photodiode circuit to PIC's RA3

2.6 User Interface

The output during the operation of the system will be indicated by a 16x2 JHD162A LCD, 3 LEDs and a buzzer. The LCD interface functions as indicators for the user upon any instructions during the operation proceedings.

The LEDs will indicate the present operation status such as system running, intruder alert and alarm system is armed.

The buzzer will give an alarming sound indicating occurrence of intrusion within the parameter.

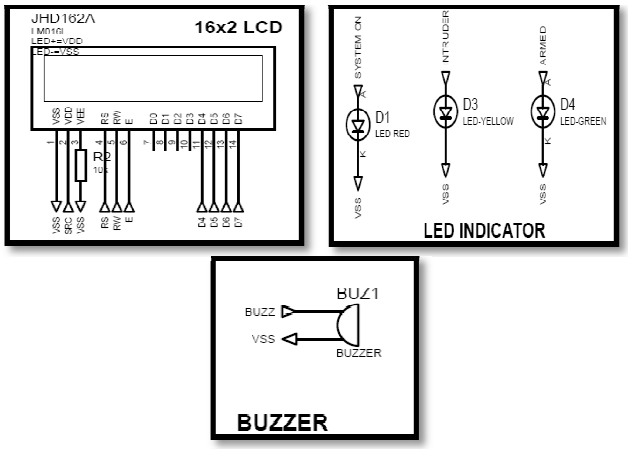

Figure 12: The interface for the user.

2.7 Hardware Housing

The parts replicate a wall to wall formation to house the laser pointer, the mirror and the photo diode.

The control box will house the main switch, PIC16F877A microcontroller, the LCD, LEDs and the RFID reader.

Figure 13: The completed housing of the security system

2.6. Software design

The programming was done in MPLAB IDE. It is a Windows Operating System (OS) software program that runs on a PC to develop applications for Microchip microcontrollers and digital signal controllers. It is called an Integrated Development Environment, or IDE, because it provides a single integrated "environment" to develop code for embedded microcontrollers.

The design of the software is based on the following flow chart requirements. Added features of functionalities were done during the development of the software through the codings in C language.

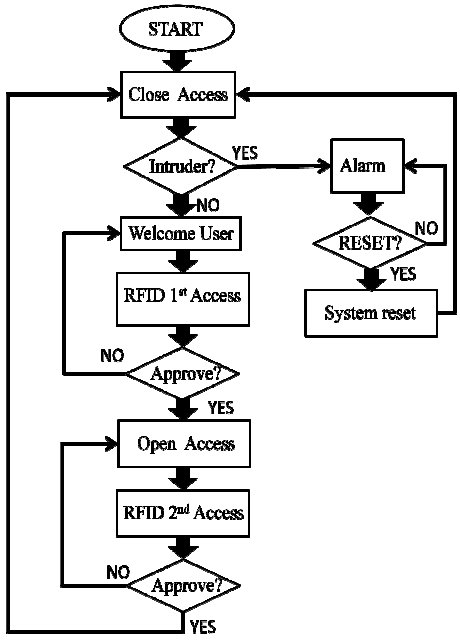

Figure 14: The flow chart of the security system

After codings in C language being done, the programs were then compiled in MPLAB IDE. It was then tested in a simulation software named Proteus ISIS for functionality test before being burnt into the PIC. A few components were replaced by switches, ports and LED to replicate the functionality of photodiode, RFID and the laser pointer respectively due to the software's limitation.

3.0 RESULTS AND DISCUSSION

3.1 Limitation on accessibility

During the development of the system, each of the components were put under test for its reliability and limitations. A few experiments had been conducted to ensure that the access part of the system (namely the RFID reader) is able to read the RFID smartcard in considerably quick time and effectively putting into considerations of the distance between the smartcard and the reader.

Due to the nature of passive RFID reader, low cost and manufacturing settings, the distance test conducted unto the RFID reader was found ineffective to read the smartcard after being put 5cm away from the reader.

The Wiegand RFID reading protocol consumes at least 0.5second to read from the passive smartcard. The reader gives an indication of 2 beeps during the reading of one passive smartcard.

This protocol allows a single card to be read during flashing. Multiple cards flashed will give confusion to the reader hence putting it into idle state.

3.2 Limitation on photo resistor

Experiments were then conducted unto the photoresistor to ensure that the input of the sensor part of the system is considerably fast to trigger the input to the PIC. It is crucial to be quick at the sensory part as this will be processed by the PIC to decide and execute for the next step in the system.

One of the tests conducted was the intensity of light absorbance through the distance versus the resistance at 0.5cm and 0.5m.

Light Type	kΩ at 0.05m	kΩ at 0.5m
White LED	0.5	∞
LASER (red)	0.9	1.2
Pendaflour	545	50.3

Figure 14: Comparison of the distance versus resistance on different types of light source.

Eventhough it was first decided that the NPN BJT will pass the input to the PIC through its emitter pin, the test conducted upon the response was found to be lagging.

Due to the built of the photoresistor, it requires time to recover to its original state. Hence, relay was put into the

sensory circuit to quicken the switching response for the PIC input.

3.3 Limitation on laser pointer as light source

Since light emits in a straight line and reflects at a 90° angle (at a medium index=1), it was decided that the laser pointer will have to be reflected by mirrors for a number of times before it hits the surface of the photo diode sensor.

During the development of the hardware, it was discovered that the light lost half of its intensity per reflection by the mirror(medium index<1). This makes the photodiode fails to trigger the BJT hence not enough to surpass the threshold voltage to trigger the PIC at 4V. Therefore, the distance from the laser pointer to travel to the photodiode was shortened by half of its original length.

As the laser pointer was mounted onto the frame, any slight changes to the angle of incident will create a great change of reflection angle. Therefore, the mounting for the laser pointer was placed with a damping material to absorb vibration that may cause the angle of incidence to change.

4. CONCLUSION

The development of the proposed Vault's Floor Security Sensor By RFID Access Using Microcontroller have been discussed and the system has reached its objective by being at a low cost production with considerable optimized functionality.

The aim of this project was to construct a prototype of a security system that is capable of performing identification on owners of smartcard, allows access upon recognition, arming the parameter with laser, detects intrusion and alert the user through visual and hearing aid.

Through thorough research and development done to accomplish the project, recommendations are proposed to improve and upgrade the performance of the security system.

Future development on the system proposed are:
1) Creating of networks between a few microcontrollers through integration (I^2C) for greater storage and addition of user identity data.

2) Networks were then connected to a Personal Computer (PC) via a General User Interface (GUI) for real time observation of access and intrusion.

3)Connecting the network with a GSM module to remotely contact the administrator of the system via Short Message Services (SMS) or call should anything go wrong when the system is left.

4) Adding a closed circuit television camera (CCTV) for real time observation during the security system operation.

REFERENCES

[1] Syed Ahson and Mohammad Ilyas. **RFID handbook : Applications, Technology, Security, and Privacy**, CRC Press, Taylor and Francis Group 2008.

[3] V. Daniel Hunt, Mike Puglia, Albert Puglia**. A guide to radio frequency identification** .John Wiley & Sons, Inc., Hoboken, New Jersey. 2007

[2][4] Finkenzeller, Klaus. **RFID handbook : fundamentals and applications in contactless smart cards and identification translated by Rachel Waddington**, 2nd edition. John Wiley & Sons, Ltd. 2003.

[5] Martin P Bates. **Programming 8-bit PIC microcontrollers in C with interactive hardware simulation**. Newness 2004.