IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 4, Issue 6, Ver. I (Nov - Dec. 2014), PP 10-15
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

Practical Prototyping of a Home Based Microcontroller Security Outfit

Dr. Mcchester Odoh And Dr. Ihedigbo Chinedum E.
Department Of Computer Science Michael Opara University Of Agriculture, Umudike, Abia State

Abstract: *Security or the lack of it has become a world topical issue today. It is no more news that with the fast increase in technological innovations, sophistication and rise in crime has also become an issue. This has led to an increased demand for better and more secure ways to protect that which we hold precious. This paper adopted the Structure Systems Analysis and Design Methodology* ***(SSADM)*** *and prototyping with the aims of addressing the security issues. At the same time, it attempts to create a microcontroller controlled pass-worded security door embedded with alarm. The system is expected to go off and alert security personnel whenever a wrong password is inputted for three consecutive times. Based on the structural specifications, if dully implemented, would greatly improve the security condition obtainable.*

Keywords: *Practical prototyping, microcontroller, technological innovations and password.*

I. Introduction

Security is prime concern to our day-to-day life. Everyone wants to be as much as secure as to be possible. An access control system forms a vital link in a security chain [1]. In **physical security**, the term access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. Physical access control can be achieved by a human (a guard, bouncer, or receptionist), through mechanical means such as locks and keys, or through technological means such as access control systems like the mantrap. Within these environments, physical key management may also be employed as a means of further managing and monitoring access to mechanically keyed areas or access to certain small assets, [2].

Physical access control is a matter of whom, where, and when. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. Historically this was partially accomplished through keys and locks. When a door is locked only someone with a key can enter through the door depending on how the lock is configured. Mechanical locks and keys do not allow restriction of the key holder to specific times or dates. Mechanical locks and keys do not provide records of the key used on any specific door and the keys can be easily copied or transferred to an unauthorized person. When a mechanical key is lost or the key holder is no longer authorized to use the protected area, the locks must be re-keyed.

Electronic access control uses computers to solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. The electronic access control system grants access based on the credential presented, When access is granted, the door is unlocked for a predetermined time and the transaction is recorded, [3]. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked.

The microcontroller based digital lock presented here is an access control system that allows only authorized person’s access restricted areas. As a simple example, to lock our mobile phone keypad, a security code of at least four digits must be entered. Security access system is an important aspect of any system. Security access control is the act of ensuring that an authenticated user accesses only what they are authorized to and no more [4].

II. Literature Review

Access Control System Operation

When a credential is presented to a reader, the reader sends the credential’s information, usually a number, to a control panel, a highly reliable processor. The control panel compares the credential's number to an access control list, grants or denies the presented request, and sends a transaction log to a database. When access is denied based on the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as an LCD (liquid crystal display) for displaying information or a flashing red LED for an access denied and a flashing green LED for an access granted, [5].

The above description illustrates a single factor transaction. Credentials can be passed around, thus subverting the access control list. For example, Alice has access rights to the server room but Bob does not. Alice either gives Bob her credential or Bob takes it; he now has access to the server room. To prevent this, two-factor authentication can be used. In a two factor transaction, the presented credential and a second factor are needed for access to be granted; another factor can be a PIN, a second credential, operator intervention, or a biometric input, [6].

There are three types (factors) of authenticating information:

- something the user knows, e.g. a password, pass-phrase or PIN
- something the user has, such as smart card
- Something the user is, such as fingerprint, verified by biometric measurement.

Passwords are a common means of verifying a user's identity before access is given to information systems [7]. In addition, a fourth factor of authentication is now recognized: someone you know, where another person who knows you can provide a human element of authentication in situations where systems have been set up to allow for such scenarios. For example, a user may have their password, but have forgotten their smart card. In such a scenario, if the user is known to designated cohorts, the cohorts may provide their smart card and password in combination with the extant factor of the user in question and thus provide two factors for the user with missing credential, and three factors overall to allow access.

Credential

A credential is a physical/tangible object, a piece of knowledge, or a facet of a person's physical being, that enables an individual access to a given physical facility or computer-based information system [8]. Typically, credentials can be something you know (such as number or PIN), something you have (such as an access badge), something you are (such as a biometric feature) or some combination of these items. The typical credential is an access card, key fob, or other key. There are many card technologies including magnetic stripe, bar code, Wiegand, 125 kHz proximity, 26 bit card-swipe, contact smart cards, and contactless smart cards [9]. Also available are key-fobs which are more compact than ID cards and attach to a key ring. Typical biometric technologies include fingerprint, facial recognition, iris recognition, retinal scan, voice, and hand geometry, [10].

Access Control System Components

An access control point, which can be a door, turnstile, parking gate, elevator, or other physical barrier where granting access can be electronically controlled. In our case the access point is a door. An electronic access control door can contain several elements. At its most basic there is a stand-alone electric lock. The lock is unlocked by an operator with a switch. To automate this, operator intervention is replaced by a reader. The reader could be a keypad where a code is entered, it could be a card reader, or it could be a biometric reader. Readers do not usually make an access decision but send a card number to an access control panel that verifies the number against an access list. To monitor the door position a magnetic door switch is used. In concept the door switch is not unlike those on refrigerators or car doors. Generally only entry is controlled and exit is uncontrolled. In cases where exit is also controlled a second reader is used on the opposite side of the door.

In cases where exit is not controlled, free exit, a device called a request-to-exit (RTE) is used. Request-to-exit devices can be a push-button or a motion detector. When the button is pushed or the motion detector detects motion at the door, the door alarm is temporarily ignored while the door is opened. Exiting a door without having to electrically unlock the door is called mechanical free egress. This is an important safety feature. In cases where the lock must be electrically unlocked on exit, the request-to-exit device also unlocks the door [1].

In computer security, access control includes authentication, authorization and audit. It also includes measures such as physical devices, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, and monitoring by humans and automated systems. Authorization is the act of determining the level of access that an authorized user has to behavior and data. This section explores the issues surrounding authorization, there is often more to it than meets the eye, and then explores various database and object-oriented implementation strategies and their implications, [8].

III. Methodology

The prototyping methodology is applied in the development of this project. Prototyping is the process of building a model of a system. It is a model of a system, built to show off certain features or to get a working model before refining other parts of the design or just to evaluate the feasibility of the system development. A systems prototype is a working system model built to test ideas and assumptions about the proposed system. Prototyping is an iterative process that is part of the analysis phase of the system development life cycle. It helps the analyst develop an initial set of system requirements. In electronics, prototyping means building an actual circuit to a design to verify that it works, and to provide a physical platform for debugging it, if it does not work. Prototyping sometimes converts intangible specifications into a tangible but limited working model of the desired information system.

High Level Model

The high level model of a newly proposed entails basically the decomposition process, focused on the flow of control in the entire modules of the system.

There are basically two (2) high level modeling techniques namely:

- Top-down technique
- Bottom-down technique

The top-down modeling technique will be adopted in illustrating the flow system; it shows the program structure of the proposed solution represented in a top-down design module specification.

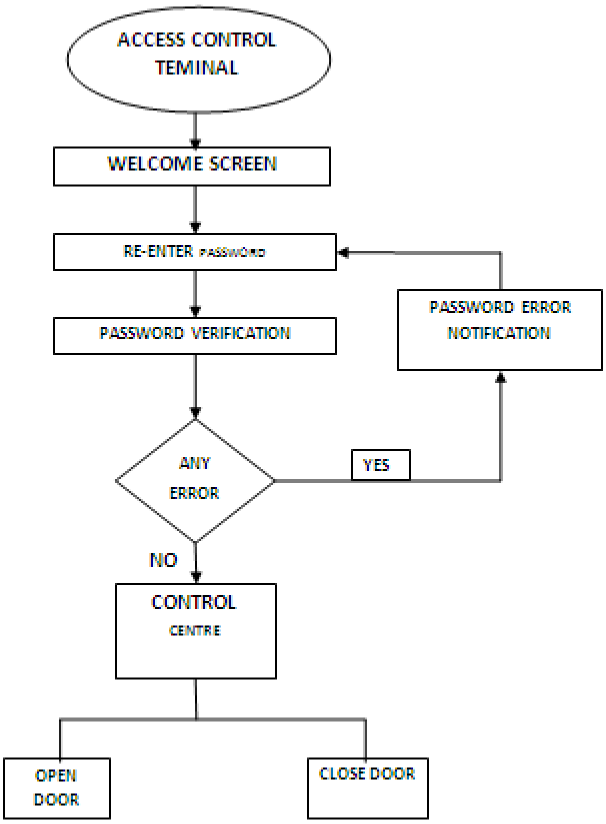

Figure 1: High level model of the proposed system

IV. Results:

System Design Calculations

Power Supply Unit

In any electronic design, the power supply unit is usually of paramount importance as the power needed for the overall functionality of the device depends on it. The required voltage and current is provided by this unit. Generally, electronic devices make use of direct current (DC) voltage as against the Alternating current (AC) voltage supplied by the energy company (PHCN). This AC supplied by the energy company is stepped down and then converted to the DC level required by the device. In this project, the following is required for this design:

- 240/12v Transformer
- Bridge rectifier
- Capacitor
- Voltage regulator

Transformer

A transformer is a device consisting of two closely coupled coils (called primary and secondary) [3]. An AC voltage applied to the primary appears across the secondary with a voltage multiplication proportional to the turn ratio of the transformer and a current multiplication inversely proportional to the turn ratio. It either steps up or steps down the AC voltage. It equally isolates the electronic device from actual connection to the AC power.

Figure 2. A typical step down transformer

Analysis on transformer parameters

Specifications:
V_{out} = 12v
Load current = 500mA
Calculating for turns of coil
$\frac{\mathrm{Ep}}{\mathrm{Es}} = \frac{\mathrm{Np}}{\mathrm{Ns}} = \mathrm{a}$……………………..........4.1
Where
Ep = primary voltage
Es = secondary voltage
Np = number of primary turns
Ns = number of secondary turns
A = turns ratio
but Ep = 240v
Es = 12v
240/12 = 20
Recall, $\frac{\mathrm{Ep}}{\mathrm{Es}} = \frac{\mathrm{Np}}{\mathrm{Ns}} = 20$
Np = 20Ns.

Therefore, the turn’s ratio of the primary to the secondary coil is given as 20:1.

Taking into consideration the voltage drop across two diodes of the full wave bridge rectifier at any instance, the actual output voltage of the transformer will be the sum of the required voltage and the voltage drop across the two diodes. This is given as:
12 + (0.6×2) = 13.2v.
Therefore, the peak minimum voltage of the transformer should be at least 13.2v but the transformer voltage is usually expressed as its root mean square (rms) value. This is given as:
$\mathrm{Vrms} = \frac{\mathrm{Vmax}}{\sqrt{2}}$……………………4.2
$\mathrm{Vrms} = \frac{13.2}{\sqrt{2}}$ = 9.33v.

Bridge rectifier

Rectification involves the conversion of an alternating current (AC) to direct current (DC). One such electronic component used to achieve this is the Diode. There are two kinds of rectification; half wave and full wave rectification. The full wave rectification was employed in this project. It involves the arrangement of four diodes to form a bridge.

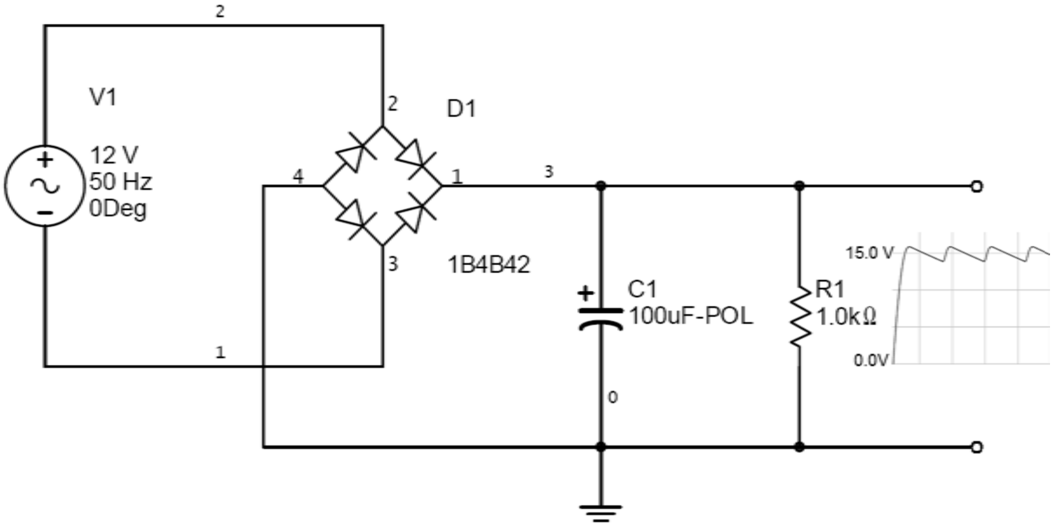

Fig 3: Full wave rectification

Software algorithm

Software algorithm refers to the step by step approach to be taken to arrive at the control program. In this project, the software algorithm began with flow-chart and finally the assembly language program, which is converted to its machine code (HEX file) and written to the microcontroller’s internal ROM for the appropriate controlling of the device.

A flow-chart represents the pattern of a system’s operation. It gives the designer an appropriate picture of the system’s performance pattern. Below is the flowchart of the microcontroller based password controlled security door system.

Data Dictionary

Table 1: Data dictionary

S/N	INSTRUCTION SET	MEANING
1	CALL	Call
2	JMP	Jump to an address
3	START	Begin program
4	MOV	Move to memory location
5	CJNE	Compare and jump if not equal
6	SETB	Set bit
7	LJMP	Long jump
8	CLR	Clear
9	INC	Increment
10	RET	Return from sub-routine
11	DJNZ	Decrement and jump if not zero
12	END	End of program

V. Summary And Conclusion

The simulation and prototyping of a microcontroller password security door with alarm system was successfully implemented. We were able to design, model and simulate a security access system that accepts password from authorized personnel to allow them gain entrance into a restricted place. When a wrong password is inputted thrice the system activates an alarm system which alerts the attention of the security. The system is basically controlled by a microcontroller which was developed with Assembly language. Conclusively, I wish to reinstate that security is a priority in the world today as the world is bedeviled with the problem of information theft, identity theft, and other forms of theft. Every technology available to us today should be deployed into enhancing the safety and sanctity of humanity, and this has been the objective of this project. Also with little alteration and innovation, it can also be deployed into offices such as the Dean of Student’s Affairs office, the Registrar’s office, the Bursary, and even lecturer’s individual offices.

References

[1]. Augarten, Stan (1983). The Most Widely Used Computer on a Chip: The TMS 1000. New Havenand New York: Ticknor & Fields. pp. 5. ISBN 0-89919-195-9.

[2]. Beck, Leland L. (1996). "2". System Software: An Introduction to Systems Programming. Addison Wesley.

[3]. Buah FK (1969). The Ancient World, A new History for Schools and Colleges. Book 1, 2nd Edition. London and Basingstoke: Macmillian Education Limited.

[4]. Dorf, Richard C.; Svoboda, James A. (2001). Introduction to Electric Circuits (5th ed.), pp. 64-65. New York: John Wiley and Sons, Inc.. ISBN 0-471-38689-8.

[5]. Federal Financial Institutions Examination Council (2008). "Authentication in an Internet Banking Environment". Retrieved 2012-07-24.

[6]. Heath, Steve (2003). Embedded systems design. EDN series for design engineers (2 ed.). Newnes. pp. 14. ISBN 9780750655460

[7]. J. Banks, J. Carson, B. Nelson, D. Nicol (2001). Discrete- Event system simulation. Prentice Hall. P.3. ISBN 0-13-088702-1.

[8]. H. Harter, Paul Y. Lin, Essentials of electric circuits, pp. 96–97, Reston Publishing Company, 1982 ISBN 0-8359-1767-3.

[9]. Sokolowski, J.A., Banks, C.M. (2009). Principles of Modeling and simulation. Hoboken, NJ: Wiley. P.6. ISBN 978-0-470-28943-3.

[10]. West Churchman the design of Inquiring systems: Basic Concepts of Systems and Organization.Basic Books, New York, 1971, SBN 465-01608-1