



DEVELOPMENT OF AN INTEGRATED CAMPUS SECURITY ALERTING SYSTEM

A. Abdullahi^{1,*} and P. E. Orukpe²

¹ ELECTRICAL/ELECTRONIC ENGINEERING DEPARTMENT, FEDERAL POLYTECHNIC, IDAH, KOGI STATE, NIGERIA

² ELECTRICAL/ELECTRONIC ENGINEERING DEPARTMENT, UNIVERSITY OF BENIN, BENIN CITY, EDO STATE, NIGERIA

Email addresses: ¹ abuhabdullahi@yahoo.com, ² patience.orukpe@uniben.edu

ABSTRACT

Providing safe and secured environment for staff, students and visitors in colleges and university is a major task that must be achieved. With the recent level of attack on campuses by insurgents and other internal social vices, there is the need for urgent protective means of securing lives and property on campus. This work presents an integrated alerting system which uses both the Internet Protocol (IP) cameras and micro-switches for monitoring security situations thereby providing an immediate alerting signal to the security personnel. The system has the input unit, processing unit, control unit and the power supply unit as its building blocks. The design of the alerting system uses PIC16F877A Microcontroller to control and process information sent from the input unit. The processed information is sent to the output unit where it is displayed by a liquid crystal display (LCD) and an audible alarm is equally activated. It was simulated with Proteus 8, and results show improvement in security monitoring. However there is need for structural modification on the campuses for effective implementation of this design.

Keywords: Campus Security, Microcontroller, Internet Protocol Camera, Integrated system, Micro-switches.

1. INTRODUCTION

The need for effective security system on the campuses of Institution of Higher Learning in Nigeria cannot be over emphasized. Students and staff need a safe environment for academic, administrative and social activities. A standard security plan for campuses would include access control system, intrusion detection system, burglar alarm system, fire detection system, video surveillance and security communication system [1]. Campuses are dynamic environments with constant activity; as a result an effective campus security system that would address the protection and safeguarding of students, staff, visitors, faculty, property and facilities of the campus must be put in place [2].

Theft, kidnap, rape and other forms of assaults are major security challenges on campuses. Students and staff loose valuables and sometimes sustain injuries. In recent times, a new dimension of insecurity has taken over the campuses of institutions of higher learning. This is the invasion of campuses by insurgents. Lives are lost; property destroyed which include destruction of classrooms, laboratories,

libraries and hostels. With these situations of insecurity on campuses of Nigerian institutions resulting from the activities of cultists and insurgents, there is need to have an effective security system (both physical and electronic controlled) to arrest these situations [3].

The provision of an integrated alerting system that can help improve the efficiency of operation of the security personnel on the campuses of the Nigerian institutions of higher learning is an important task. An integrated system combines the functions of many stand alone security devices into a single system and significantly reduces capital expenditures and lowers facility operating costs because component devices are used in multiple ways and security officers can be trained on one system rather than many, and this makes the security staff to become more effective on the job [4-5].

Most organizations such as universities have critical positions and rooms that need to be secured. Securing a university campus could be achieved by integrating different security measures, such as the use of cameras and wireless network that is effective and of

low cost [6-7]. The wireless sensor network (WSN) consists of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutant at different locations. This system is presently being used to achieve effective security system in different applications, such as the RFID embedded debit/credit cards used in business transactions and library management [8-10].

Security challenges on the campuses of higher institution of learning are numerous; these include theft, assault, rape, fire outbreak, etc [2, 11]. These require multi-dimensional approach to effectively handle the situation. Multi-agent systems are therefore used to solve these challenges on campuses [12]. A multi-agent system (MAS) is a system composed of multiple interacting intelligent agents [4]. Different multi-agent systems have been designed to help improve security situation in different places. One of such designs is the multi-agent system based on Java Agent Development Framework (JADE)[12]. It offers a Java middle ware based on a peer-to-peer architecture with the overall aim of providing a runtime support for agents. It is used in solving complex security situations.

Locating personnel or other property during attack is a major challenge to the campus security outfit [13]. The Radio Frequency (RF) transmission has been used for personnel location systems. This system is able to locate personnel accurately in indoor and campus environment. Users wear electronic devices that provide or permit location and unique identification. In the vast majority of potential applications, the user will be aware that his/her location is being monitored. The location device must be easy to operate during day-to-day activities and emergency situations [14]. It must be water resistant, portable, rugged, non-intrusive, and economically attractive and it also needs to have an effective power source. The RF system operates optimally when integrated into the existing emergency response infrastructure of a campus.

To develop a standard security system for a campus, there must be a sound campus information system. Campus information systems are used by many universities for different purposes; these include information about academic and administrative units and staff, topographical and natural features and land use on the campus [15]. Database, maps, spatial and attribute data, analysis and queries are used to build a campus information system. In this regard, a 3D modeling of the Cukursaray (the Hollow Palace) and

its application for campus information system was designed [15]. It is a web-based campus information system and enables users to access current and visual information about the campus over the web. This would allow close monitoring of the campus.

In this work, an integrated alerting system is designed using micro-switches and IP cameras as the input units. The IP cameras capture images within the area under surveillance, while the switches (i.e. the push buttons) when depressed send signals to the microcontroller. The signals are then processed and outputs generated. An audio alarm is triggered simultaneously with visual display of the particular room under security threat. The microcontroller used to achieve this design is the PIC16F877A. It is a microcontroller from Microchip Technology in a chip type of 40-pin, 4MHZ 8KB PDIP packages [16].

The PIC16F877A microcontroller in this design operates in the master-slave configuration. The microcontroller that receives information from the input unit (i.e. switches) during intrusion or any other case of emergency in a particular room serves as the slave while the one that coordinates the activities of all the slaves is the master microcontroller. The master controller is installed in the control room. This microcontroller processes the signals and sends results to the display/alarm unit where security personnel receive this information for immediate response. The surveillance cameras on the other hand capture the images of suspected persons or objects in any security-breach situation.

The work presented in this paper is an improvement over that presented in [3] with the introduction of an alternative switch and IP camera.

2. METHODOLOGY

The method used in the design of the work presented in this paper is outlined in this section.

2.1 System Components and Operations

The system's major components are described in section 2.1.1, while the operational sequence is presented in section 2.1.2.

2.1.1 System Components

The functional components of the system are as follows:

- (i) Each room has four push buttons on the four corners of the building.
- (ii) One push-button is mounted on the foot-path through the main entrance (door) to each room.
- (iii) An alternative switch (i.e. single pole multiple throw (SPMT)) is installed in each room.

- (iv) A microcontroller is programmed to accept and process the input signal from the switches.
- (v) A surveillance camera is installed to capture all images in the building.
- (vi) A master-microcontroller is programmed to accept information from all other microcontrollers (slaves) installed in each room. It processes the received information and sends it to the output unit.

2.1.2 Operation of the System

The system's operation is carried out in the following steps:

- (i) When an attack/intrusion is sensed, a push button is pressed by the victim,
- (ii) Signal is inputted into the microcontroller (slave),
- (iii) The microcontroller (slave) accepts and processes the information,
- (iv) The message is encoded with an identity (ID),
- (v) The ID is sent to the control unit,
- (vi) The information is then transmitted to the master-microcontroller,
- (vii) The master-microcontroller decodes the information and sends results to the output unit,
- (viii) At the output unit the message is displayed and an audible alarm is activated,
- (ix) The message and alarm remain ON until a RESET is activated,
- (x) The system is then ready for another operation after a RESET is activated,
- (xi) Surveillance camera is also activated to capture images.

2.2.2 Flow Chart of the System Operation

The flow chart for the operation of the security alerting system is shown in Figure 1. It shows the signal flow from the inputs, how the information from the input is processed and how the processed information is obtained at the output unit. The IP camera is a backup system for the design. The IP camera in this design is to capture images of person/objects, store the information and displays the said information upon request. This is applicable in situation where none of the switches is activated due to absence of persons or circuit failure. The security personnel can fall back to the information captured/stored by the IP camera for further investigation.

The IP camera's operation is time-based, and as such images captured are stored with corresponding time and date. This allows easy access to any information

for a particular time in which an incident/threat occurred.

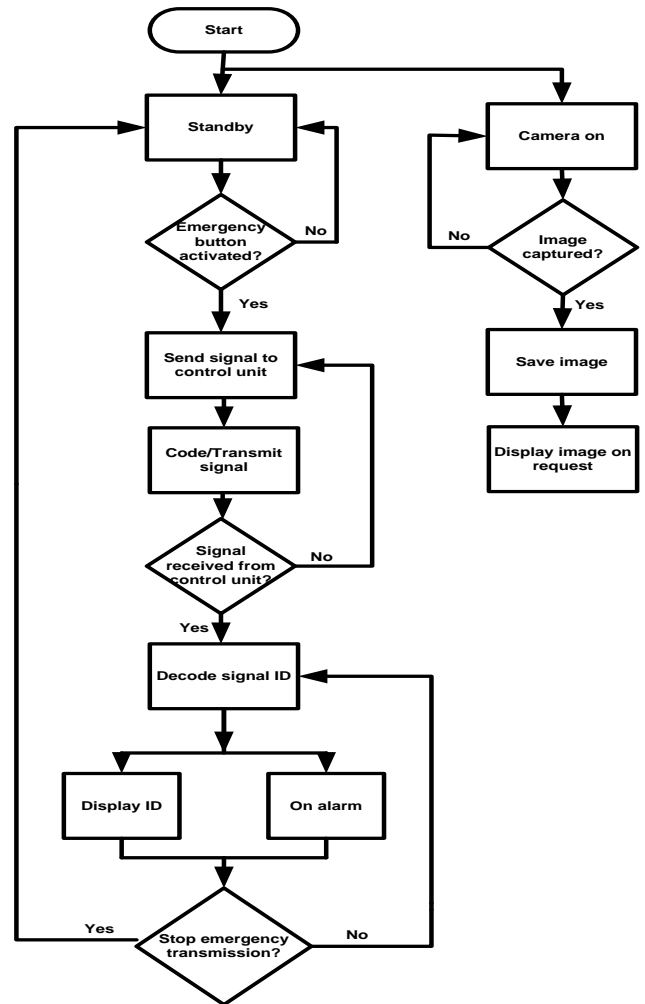


Figure 1: Flow chart of the campus security alerting system.

2.3 System Design and Implementation

The campus security alerting system was designed using the building blocks shown in Figure 2.

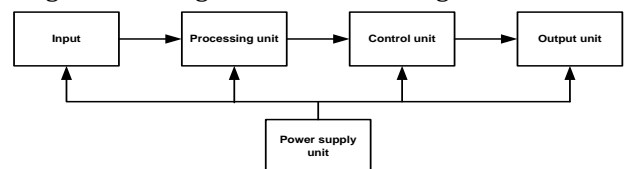


Figure 2: Block diagram of the campus security alerting system.

2.3.1: The Input Unit

The input unit consists of switches, while the IP camera is a backup for further investigation. These components send signals that trigger the operation of the other units.

2.3.1.1 The Switches

The switches used in the design are the push buttons and the single pole multiple throw (SPMT) switches.

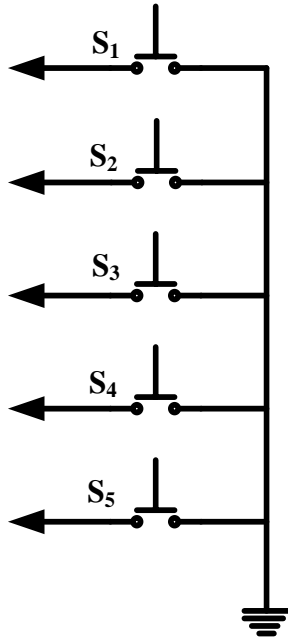


Figure 3: The input unit (Push buttons)

The push buttons are mounted on the wall in each room of the hostel/office complex. These buttons when activated send signals of logic "1" to the microcontroller (slave) indicating an emergency situation. A push button is also placed under the carpet at the entrance (foot path) to the room. The microcontroller is programmed to interpret a signal as logic "1" when such signal is sent twice sequentially at interval of one second from this button. Therefore, a double-press on the button indicates an emergency situation. These switches are very reliable in operation, especially in the case of intrusion [17].

The SPMT switch is used as an alternative switch in this design. The switch enables an emergency alert to be sent from other rooms rather than the room where security challenges exist, in a situation like fire outbreak. All switches are room coded and as such enable the system to display the particular room where an incident occurs, and in the case of an alternative switch, it displays the room of incident as

well as that of the source of information. Figure 3 shows the components of the input unit (push buttons). S_2 - S_5 are mounted on the walls while S_1 is placed at the entrance (foot path) to the room.

2.3.1.2 The IP Camera

The IP camera was used in this design to capture images within the area under surveillance. Captured images are stored, and displayed on request. This allows the security personnel to access information about any security challenge when any of the switches is not activated either due to absence of persons or circuit failure. The images are displayed on the monitor of a computer as shown in Figure 4. IP camera operations are time-based. This makes it easy to access information on a specific date and time.

IP video surveillance camera involves the use of network switches, network cameras, video management software and a computer to view, manage and store the video content. The flexibility of the IP camera makes it easy to connect many video cameras to the system. The IP camera has a resolution from 1-megapixel to 8-megapixel [18]. For this design, the Local Area Network (LAN) was used. This is to avoid exposing the system to hacking.

2.3.2 Processing Unit

This unit comprises the PIC16F877A microcontroller which is the heart of this work. Each room has a dedicated microcontroller (slave-microcontroller) that monitors the voltage at the input unit (sensor switches), processes the information and then transmits it to the control unit which is the central microcontroller (master-microcontroller) which then decodes the information sent by any of the slave-microcontrollers in any of the rooms and then sends the result to the output unit. Figure 5 represents the processing unit used in simulating security situation in a typical room (Room 1) of a building; which is similar for other rooms of interest.

Resistors R_1 - R_7 are used to limit the value of current that flows through the switches. The switches require about 5mA for operation.



Figure 4: IP Camera connection

The resistance values were determined from the relation;

$$R = \frac{V}{I} \tag{1}$$

Since $R = \frac{5V}{5mA} = 1000\Omega$, therefore, R_1 to $R_7 = 1000\Omega = 1k\Omega$. The oscillator used in this design has a frequency of 4MHz. This determines the time it will take the microcontroller to execute one line of instruction.

The time for execution is given as;

$$T = \frac{4}{F_{osc}} \tag{2}$$

where F_{osc} is the oscillation frequency. Therefore, $T = \frac{4}{4 \times 10^6} = 1\mu s$.

But frequency of operation, F_{op} is given as:

$$F_{op} = \frac{1}{4} \times F_{osc} \tag{3}$$

which implies that, $F_{op} = \frac{1}{4} \times 4000000 = 1MHz$. The crystal oscillators used in this design, Xs have operating frequencies of 4MHz, while capacitors used are of 22pF based on the data sheet [16].

2.3.3 Control Unit

The control unit coordinates the operation of the master-slave controllers. It allows up to fifteen slaves (i.e. fifteen rooms) inputs and gives a serial output through the use of a multiplexer (74154). The multiplexer gets information from each of the slave-microcontrollers that represents each room and sends the information to the master-microcontroller for decoding, and the master-controller sends the result to the output unit which comprises of the display and alarm units. Figure 6 shows the control unit.

2.3.4 Output Unit

The output unit comprises of the display and alarm units. A 2x16 Liquid Crystal Display (LCD) module display information such as device status. It possesses in it the famous HD44708 LCD controller driver. It supports 2 rows by 16 columns of character making it capable of displaying 32 ASCII characters at once on the screen and as part of the device, users need an interface to monitor the device processes.

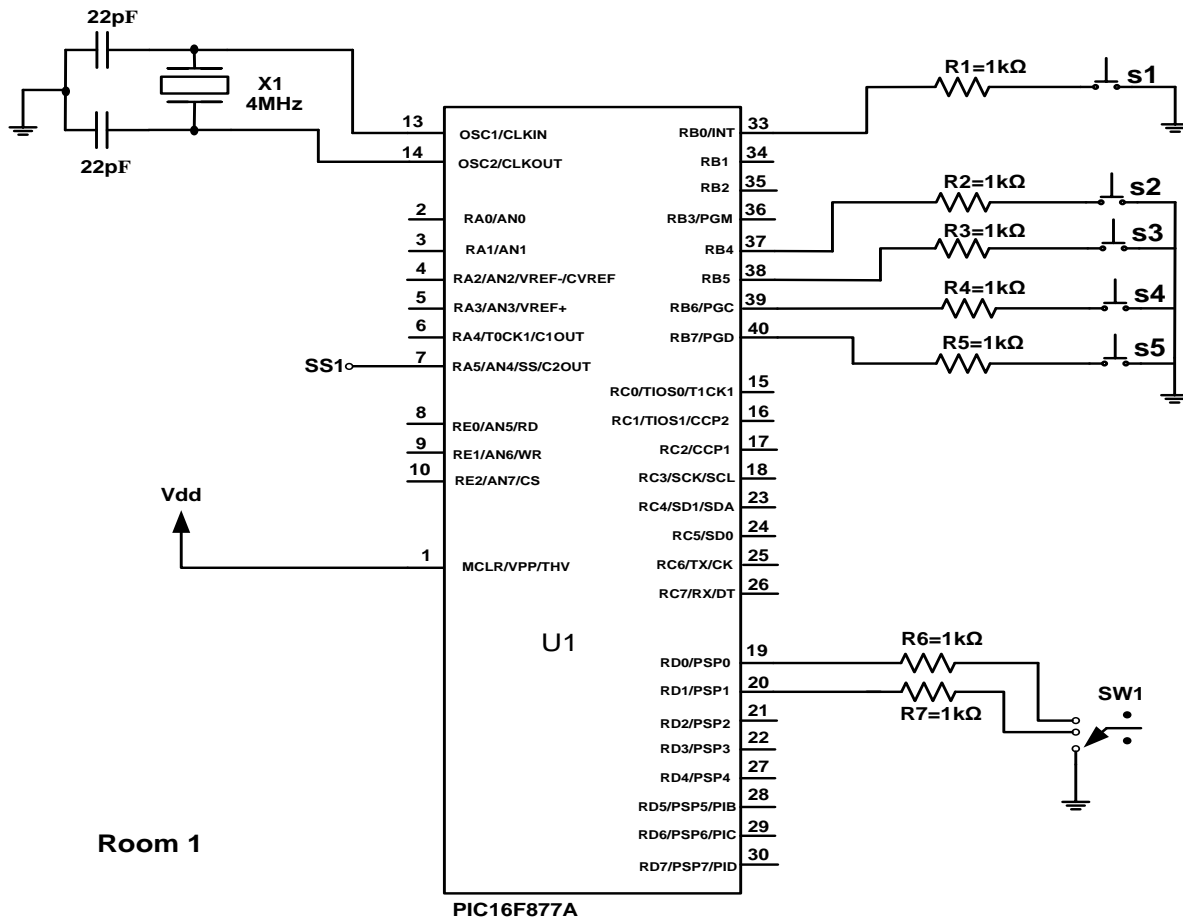


Figure 5: The Processing unit

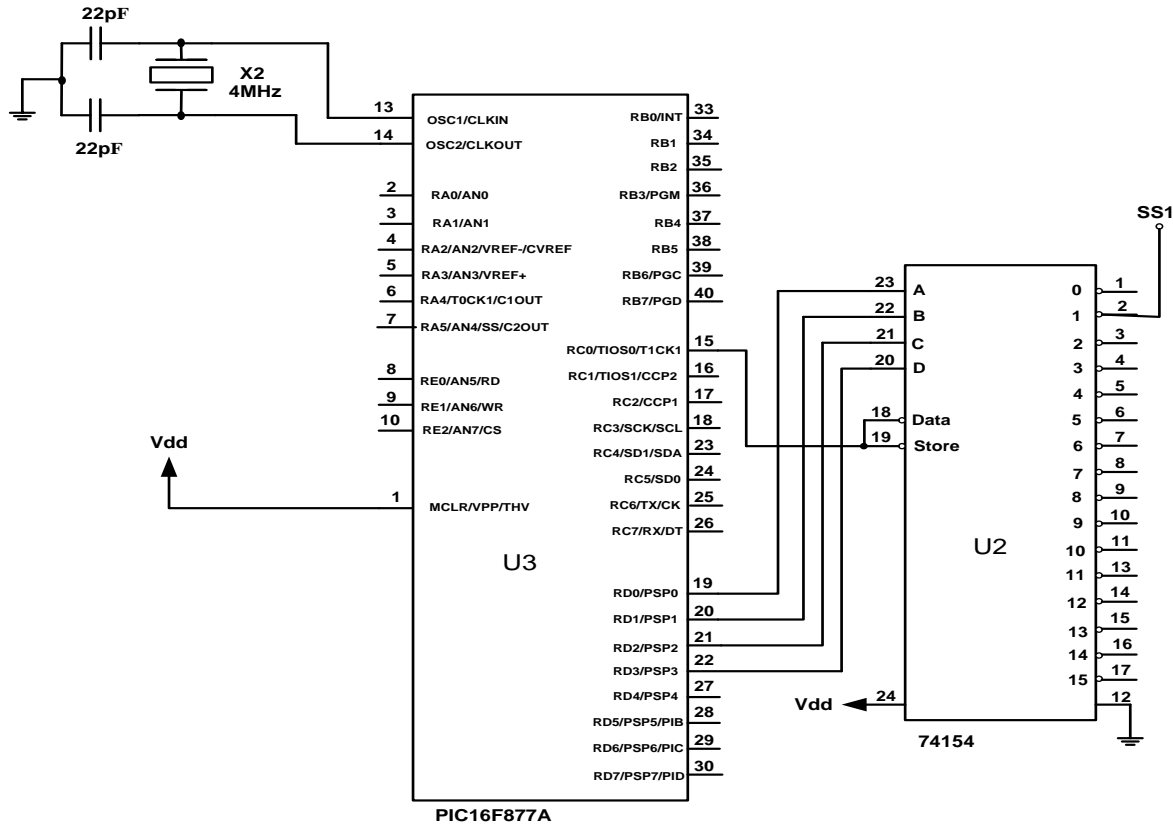


Figure 6: The Control unit

The information received from the switches is displayed on the LCD showing the particular room number under emergency situation, while the information from the camera when needed is displayed on the screen of a personal computer. If it is the alternative switch that is activated, it displays the room number of the source and the room number under attack. An alarm is also activated to give an audio alert to the security personnel. This alarm will remain in the “ON” state until a RESET is activated by the security personnel. The output unit is as shown in Figure 7.

2.3.5. The Power Supply Unit (PSU)

The power supply unit provides the required DC voltage (V_{dd}) for the circuit. The microcontroller (PIC18F877A) requires a maximum voltage of +5.5V [16]. The output unit which comprises the display and alarm units also requires a maximum voltage value of 5V. Therefore, a +5V power supply by specification is adequate to drive the alarm section and indeed the entire circuit. A 6V battery is included to keep the system in operation in case of power failure by the power utility company, for at least 8 hours before power is restored. The power supply unit includes the transformer, rectifier, filter and the voltage regulator to give the required voltage level [19].

A 220V/12V, 500mA transformer was chosen for the design. It is to provide the required voltages for both the circuit and the backup battery. The output of the transformer was rectified using diodes. For full wave rectifier design,

$$V_{max} = \sqrt{2V_{rms}} \tag{4}$$

So, $V_{max} = \sqrt{2 \times 12} = 16.97V$. The dc output voltage,

$$V_{dc} = 0.636V_{max} \tag{5}$$

Whence, $V_{dc} = 0.636 \times 16.97 = 10.79V$. The peak inverse voltage (PIV) for rectifying diode must be greater than V_{max} and the forward current must be greater than the load current (in this case, 16.97V, 500mA). Therefore, IN4001 silicon diode with PIV rating of 50V and forward current of 1A was chosen.

A capacitor was used to filter the ripples. The capacitance of the capacitor was obtained using the relation,

$$V_r = I_{rms}/2fC \tag{6}$$

In (6), V_r is the ripple voltage, f is the frequency of input voltage (50Hz), C is the capacitance of the capacitor. From (4), $V_{max} = 16.97V$, but:

$$V_r = \text{the ripple factor} \times V_{max} \tag{7}$$

Assuming a ripple factor of 14%, then, $V_r = 0.14 \times 16.97 = 2.38V$. Therefore,

$$C = I_{rms}/(2V_r f) \tag{8}$$

Equation (8) yields $C = 500 \times \frac{10^{-3}}{2 \times 2.38 \times 50} = 2.1 \times 10^{-3} = 2100\mu F$.

A standard working capacitor of $2200\mu F$, 25V was selected. The 5V regulator used is a fixed voltage regulator from the family of the 78XX series. Its output is enough to power the circuit. Figure 8 shows the power supply unit for this design.

3. SIMULATION AND DISCUSSION

On completion of the design, a sample of two rooms of a hostel was simulated using Proteus 8 software and all units functioned as stated in the system operation. Figure 9 is a scenario where security challenge occurred in room 1, and an emergency alert was sent from the same room; while scenario 2 (Figure 10) shows that security challenge in room 2 is reported from room 1. The third scenario in Figure 11 shows a situation where a security challenge in room 1 is

reported from room 2. These are displayed on the LCD. The alternative switch (used when the room with security challenge cannot be accessed) when activated displays the room number where emergency situation exists as well as the room where information is sent from. On the other hand, when any of the switches other than the alternative switch is activated, the system displays on the LCD the source of information. In the same vein, this system also accommodates situation where an alternative switch is activated simultaneously with any other switch in the room. This is possible because the switches are room-coded. Information from both sources is displayed sequentially on the LCD with the aid of the serial-shift operation of the multiplexer.

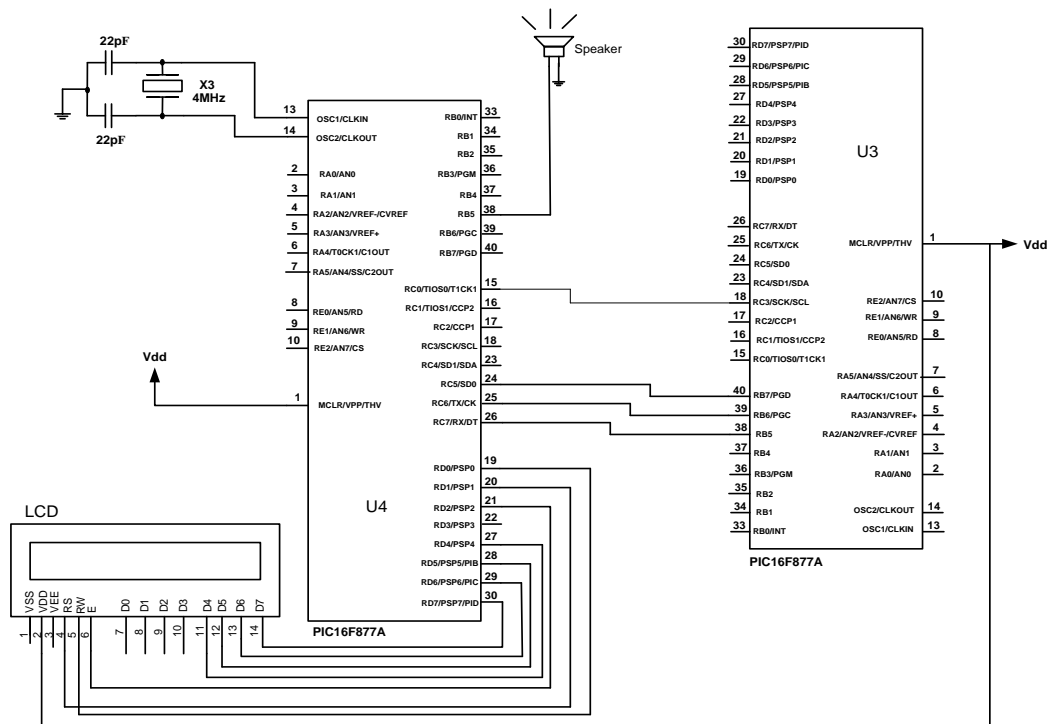


Figure 7: The output unit

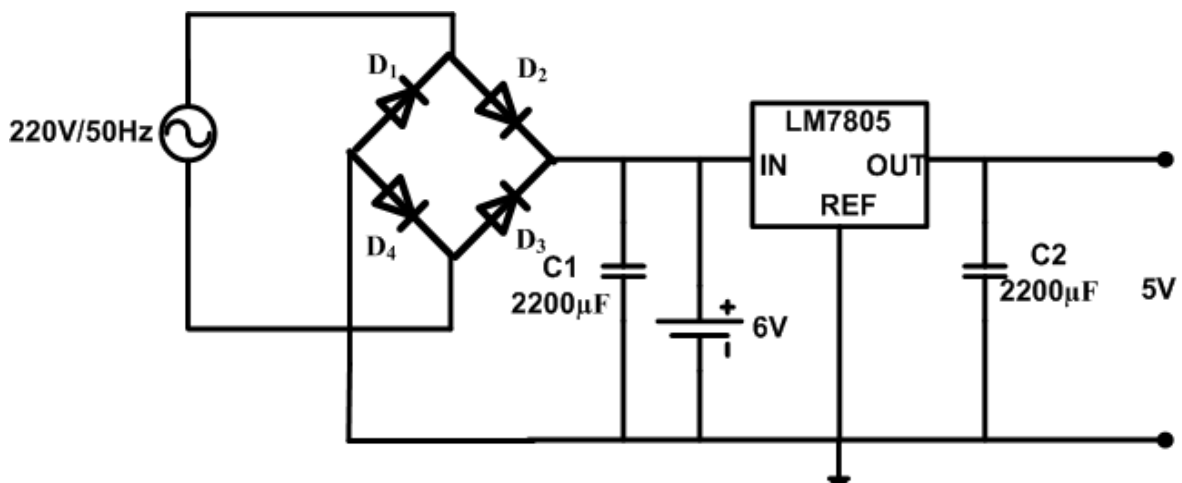


Figure 8: Power supply unit

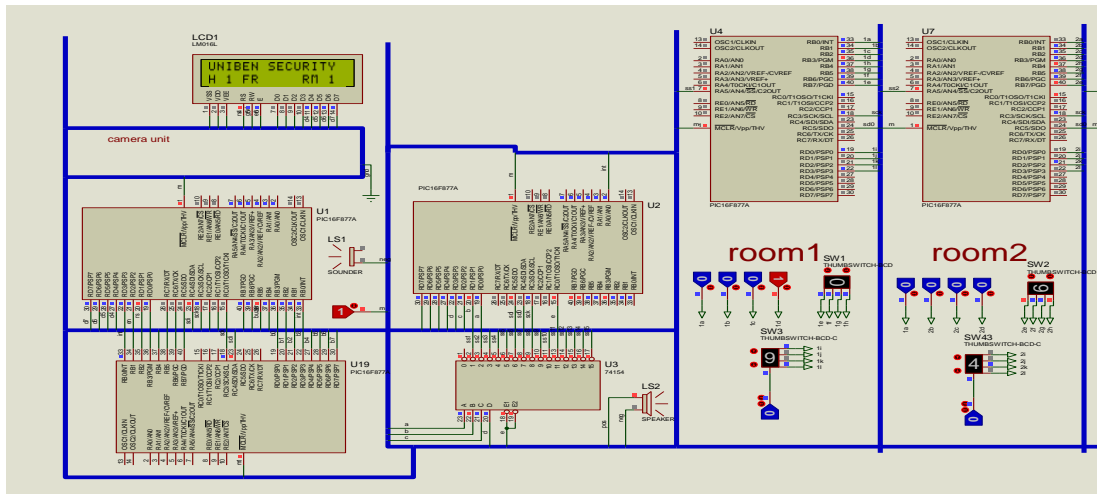


Figure 9: Scenario 1- a security challenge in room1 reported from room1

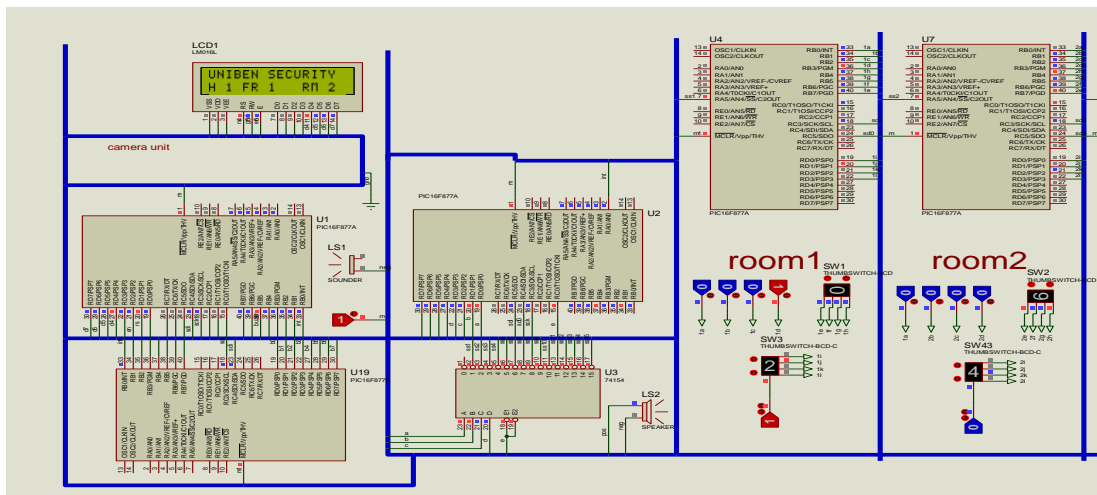


Figure 10: Scenario 2- a security challenge in room 2 reported from room 1

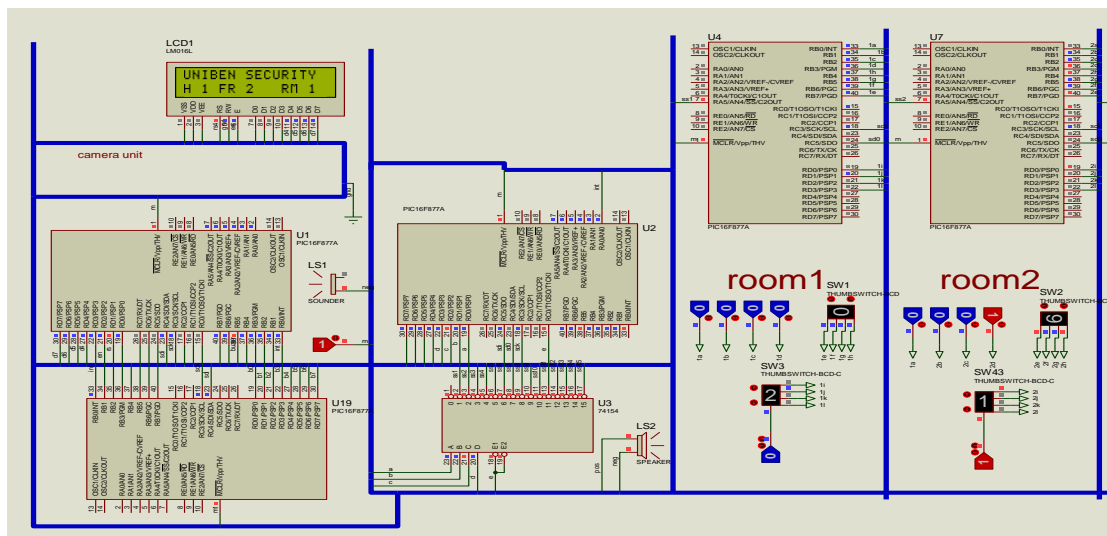


Figure 11: Scenario 3- a security challenge in room1 reported from room 2

In each case, the alarm unit is activated for audio alert. This system works simultaneously with the surveillance camera unit. The displays in LCD of

scenarios presented in Figures 9 - 11 show an improved alerting system. This system when properly installed on the campuses of Nigerian institutions of higher learning would

improve the efficiency of the security personnel on the campuses and would equally bridge the communication gap between victims and the security personnel.

4. CONCLUSION AND RECOMMENDATION FOR FUTURE RESEARCH

In this paper, a simple, efficient and cost-effective security system is designed to help improve the effectiveness of the security network on the campuses of Nigerian institutions of higher learning. It is based on the application of PIC16F877A microcontroller. It operates on the master-slave configuration of the microcontroller. A sample of two rooms of an hostel was simulated using Proteus 8 software and it showed an improved alerting system as presented in section 3. The next phase of this work is to develop a prototype of this alerting system. However, it is recommended that the structural design on campuses of Institution of Higher Learning in Nigeria be improved upon to accommodate security alerting designs. Also, Security alerting designs should include access control which will take care of unauthorized persons in certain facilities.

5. REFERENCES

- [1] Christopher S. M. "Security Master Plan and Standard for Yuba Community" www.yubacommdist.com published by the Chief of Police, Yuba Community College, April (2008).
- [2] Schneider Electric. "Creating safe campus with integrated security solutions" 2006 White Paper. www.scheider-electric.com/buildings. Accessed on 10th September, (2015).
- [3] Abdullahi, A. and Orukpe P. E. "Security Alert System for Nigerian Institutions of Higher Learning", In *Proceedings of University of Benin Annual Research Day(UBARD) Conference*, Benin City, Nigeria, pp. 684-687. (2015).
- [4] Faisal A., Zain A. A., Eslam A., Shadi A. and Ahmed T. A. "A Multi-agent based system for securing university campus", *International Journal of Recent Research Aspects*, 2(3), 2010, pp. 223-229.
- [5] Zain A. A. and Emad El-deen Al-fakhry "Towards Implementing Intelligent Security System", Master Thesis, Computer Science Department, Yarmouk University Jordan, pp.15-20. (2010).
- [6] Sandhu J. S., Agogino A. M. and Agogino. A. K. "Wireless sensor networks for commercial lighting control", www.wirelessensornetwork.com. Accessed on 10th January, 2016. (2014).
- [7] Ki Y. K. "Accident detection system using image processing and MDR", *International Journal of Computer Science and Network Security* 7 (3), pp. 35-39. (2007).
- [8] Ferrer G., Dew N. and Apte U. "When is RFID right for your service?", *International Journal of Production Economics*, Vol. 124, pp. 414-425. (2010).
- [9] Finkenzeller K. "*RFID Handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*", John Wiley and Sons Ltd., Third Edition, pp. 18,361,374. (2010).
- [10] Edwards E. O. and Orukpe P. E. "Development of a RFID based library management system and user access control", *Nigeria Journal of Technology*, Vol. 33. No. 4, pp. 574-584. (2014).
- [11] Cisco Brochure. "Campus safety: five advances in physical security for higher education", pp. 1-9. (2013).
- [12] Vila X., Schuster A. and Riera A. "Security for a multi-agent system based on Java Agent Development Framework (JADE)", *Journal of Computer and Security*, Vol.26, pp. 391-400. (2007).
- [13] Christ C. and Lavigue R. "Radio frequency-based personnel location systems", In *Proceedings of IEEE 34th Annual International Carnahan Conference on Security Technology*, Ottawa Ont.: pp 141-150. (2000).
- [14] Rappaport T. S. and Sandhu S. "Radio-wave propagation for emerging wireless personal-communication systems", *IEEE Antennas and Propagation Magazine*, Vol. 36, Issue 5, pp. 14-24. (1994).
- [15] Yildiz H. and Gumusay M. U. "3D Modeling of the Cukursary (the Hollow palace), Istanbul-Turkey and its application for campus information system". XXIIIth *International CIPA Symposium, Prague, Czech Republic*, pp. 1-6. (2011).
- [16] Microchip Technology Inc. "PIC16F87XA Datasheet, Pin Enhanced Flash Microcontrollers", (2003).
- [17] Ibrahim A. G., Oyedum O. D., Okeke S. S. N. and Adetoba A. O. "Design and Construction of a Car Immobilizer with SMS alert", *Journal of Research in National Development*, 10(3), , pp. 101-108. (2013).
- [18] Gradimirka P., Nebojsa A., Branimir J., Boris G. and Mile P., "Overview, characteristics and advantages of IP Camera video surveillance systems compared to systems with other kinds of camera". *International Journal of Engineering Science and Innovative Technology*, 2 (5), pp. 356-362. (2013).
- [19] Adewale A. A., Abdulkareem A., Agbetunyi A. F. and Dike I. "Design and Development of a Microcontroller-Based Wireless Security Access System", *International Journal of Computer Science Engineering*, 2(5), pp. 237-246. (2013).