Usage of a Microcontroller in Security Access Control Onboard Ships

Mohamad Fikri bin Abdul Hamid,[a,]
Daniel Dian, [b,]
Christopher Rully anak Andrew Alek,[c]

Email: [a] fikri_aet@yahoo.com, [b] dian_epiphone@yahoo.com, [c] crully@gmail.com

ABSTRACT

Security onboard vessels has always been an important part of life at sea. This has been made more so in the events of 11 September 2001 in New York City, New York, USA. The aim for this paper is to show that with simple electronics like PIC16F84A microcontroller, and a little bit of coding knowhow, the access to sensitive areas onboard a vessel will be closely monitored and controlled by the vessel's officer in charge of security. Of course, this system doesn't fully replace basic human intervention. This paper will show a highly simplified system, designed and simulated using the software Proteus, and its designed code that can be expanded, written in PIC C Compiler. This paper does not, however, show a fully working physical model, as the availability of components and time to build up a working physical model is scarce. However, this simulated system can be scaled up and tested first in simulator software, before it can be built up physically and tested on a bench, before installed onboard a real vessel.

KEY WORDS: *ISPS Code, PIC16F84A microcontroller, Access Card, Crew/Visitor Access Control*

NOMENCLATURE

PLC	Programmable Logic Controller
IMO	International Maritime Organization
STAFF	Ship Crew
VISITOR	Visiting Personnel
RFID	Radio Frequency Identification
SELECTOR	Room Selector
CARD	Access Card
LCD	Access Display LCD
Lock	Motor/Solenoid for Door Lock

1.0 INTRODUCTION

The shipping industry is known to be a highly regulated industry with a great number of rules and regulation created and enforced to produce an industry that is not only safe, but also able to adjust itself to the times. One of the most important regulations that impacts the global maritime/shipping industry is the ISPS Code. Also known as the International Ship and Port Facility Security Code, it is a now essential maritime regulation for the global safety and security of ships, ports, cargo and crew.

1.1 Why Security?

The state of global safety and security has always affected the way all industries do its business. However, due to the terrorist attack during 11 September on the World Trade Center Twin Towers in New York in 2001, it was found that ship security, was found to be inadequate. Before those terror attacks, and before the ISPS code was introduced, the shipping industry and IMO's primary focus was safety of the ship and lives of its crew at sea[1]. In response to the terror attacks and the lack of security awareness among seafarers, IMO has created the ISPS Code, which was implemented on 1st July 2004.

1.2 Aims of ISPS Code in Vessel's Day to Day Operations

- To monitor the activities of people and cargo operation
- To detect the different security threats onboard vessels and in port and implement measures as per the situation
- To provide a security level to the ship and derive various duties and functions at the different security level
- To build and implement roles and responsibilities for onboard officers to tackle maritime security at

the international level

- To provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels
- To find the shortcomings in the ship security and port security plan and measures to improve them

2.0 CURRENT SITUATION ONBOARD VESSELS

2.1 How is access and security currently monitored onboard

Currently, ISPS Code requires vessels to have personnel to gather, assess and distribute security-related information to appropriate contracting government agencies[1]. This means, that there has to be personnel to receive and understand the information, and other personnel to implement the security protocols onboard the vessels. These protocols are, but not restricted to,

- Prevent unauthorized entry into the vessel at any time
- Prevent the passage of unauthorized weapons and other devices that could potentially be dangerous to a vessel and her crew, and,
- To implement a proper security plan onboard each vessel.
- To prevent unauthorized entry into designated security areas.

While the first three protocols above are unfortunately only able to be implemented by qualified personnel, the last protocol can be implemented via automation through the use of access control cards.

2.2 Proposed System of Access Control

Access control is one of the security protocols that can be modernized and automated through electronic means [5][6]. Of course, this is still to be tested in a real situation, but this paper, and its proposed system, hopes to give the industry, that is already struggling with lack of manpower due to minimized manning onboard vessels, a means to still keep security at a high level onboard, without the need to sacrifice manpower that could be used elsewhere onboard.

3.0 METHODOLOGY

A PLC based control panel, based on the PIC16F84A microchip, would be responsible for granting and denying entry to a few sensitive security areas of the ship. These areas are the Wheelhouse, Engine Control Room, Cargo Control Room, Engine Room, Smoking Room and Mess Room. From these areas, only the Smoking and Mess Rooms are where visitors are allowed access, while ship crews are allowed access to all areas of the vessel. However, sometimes, visiting personnel are onboard the vessel to do maintenance or repairs to machineries or to meet the vessel's Master, so they may be required to go to a meeting room, but accompanied with a security personnel, usually an AB.

3.1 Components

The system proposed by this paper is a simple system with access control only to 5 designated areas. Therefore, the components required by this system is minimal. It consists of:

1. PIC16F84A 18-pin EEPROM 8-bit microcontroller. Refer to Figure 1.
2. LM016L 2X16 Character LCD
3. Servo/Stepper Motor for Door Lock Mechanism
4. Green and Red LED to signified Entry Granted or Denied
5. Selector switch

These components are chosen as they provide the most basic for the security system mentioned in this paper.

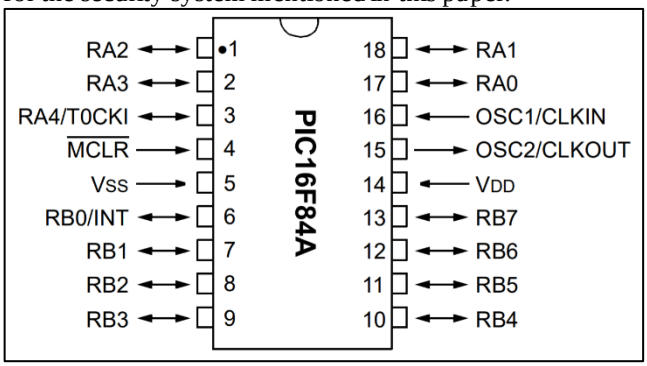

Figure 1: PIC16F84A Microcontroller with Pin Assignments

3.2 Operation of the system

The concept for the system is as follows:

- When personnel come onboard a ship, he/she and their luggage will be searched and verified to be given permission to be onboard.
- That personnel will be given an access card along with a security declaration form that has to be filled and signed. This access card will hold either a code for STAFF, which signifies that personnel to be ship crew that has signed on, or VISITOR, which signifies that personnel to be outside personnel, onboard for maintenance or meeting with ship crew.
- With the access card, the personnel coming onboard will be able to either have full access of the whole vessel, if he/she is a ship crew, or have access restricted to messroom and smoking room only while onboard the ship.
- Each time a person accesses an area he/she will be required to use his/her access card to open the door. This is the automation of the security access system.

Below, in Table 1, is the logic of the operation of the system.

INPUT					OUTPUT			
Selector	Card	A0	A1	A3	ENTRY	D1	D2	MOTOR
Bridge	STAFF	1	0	1	YES	YES	NO	YES
	VISITOR	0	1		NO	NO	YES	NO
Engine Control Room	STAFF	1	0	1	YES	YES	NO	YES
	VISITOR	0	1		NO	NO	YES	NO
Engine Room	STAFF	1	0	1	YES	YES	NO	YES
	VISITOR	0	1		NO	NO	YES	NO
Cargo Control Room	STAFF	1	0	1	YES	YES	NO	YES
	VISITOR	0	1		NO	NO	YES	NO
Smoking Room	STAFF	1	0	1	YES	YES	NO	YES
	VISITOR	0	1		YES	YES	NO	YES
Mess Room	STAFF	1	0	1	YES	YES	NO	YES
	VISITOR	0	1		YES	YES	NO	YES

Table 1: Truth Table

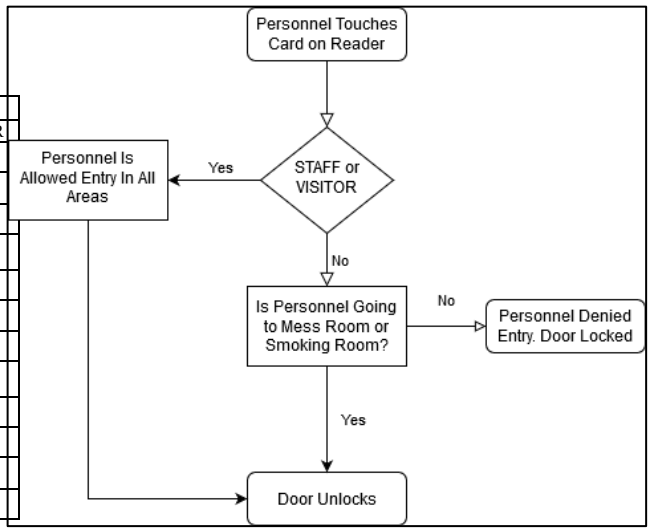

Figure 2: Flowchart of the system

3.3 PIC16F84A Microcontroller

The whole system is controlled by a single PIC16F84A microcontroller. Based on the PIC16x84 family of PLC and introduced in 1998, the 8-bit microcontroller, produced by Microchip Technology, is an improved version of the original PIC16C84, which was introduced in 1993[2]. The PIC16F84A comes with 68 bytes of RAM, compared to the 36 bytes the PIC16C84 had. The PIC16F84A also had 64 bytes of EEPROM and a single timer and has a clock speed of up to 20MHz[3]. For the purpose of this paper, this microcontroller is simulated in the software Proteus 8.

3.4 Software and Coding

The program code for the system is composed, edited, compiled and programmed using the "CCS C Compiler" software. This compiler allows for the quick and easy programming and error checking of the code before a hex file is produced to be uploaded into the simulated microcontroller within Proteus 8. This whole system is then tested in Proteus in simulation to check if the microcontroller, components and coding do as it is expected to do.

3.5 System Flow

Figure 2 below, details the logical system flowchart of the proposed access control system.

3.7 Circuit Schematics

The circuit given below is a part by part schematic diagram of the circuit from Proteus 8

Input Circuits:

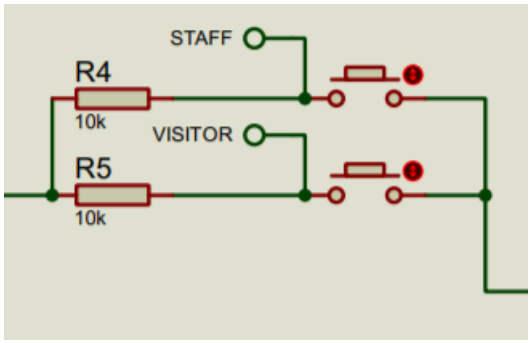

Figure 3: Staff or Visitor Card Input

Due to lack of programming knowledge, the access card input is replaced with 2 push button normally open switches. In real application, this will ideally be replaced with an RFID reader and card, with location identifier, to allow the system to work as intended.

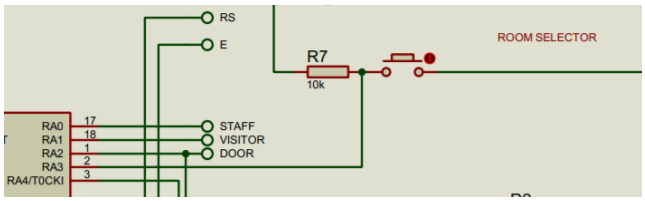

Figure 4: Area Selector Input

As with the previous Staff/Visitor input circuit, the expertise to create a program that knows the location of

where the access card is used, is lacking. Therefore, as a basic workaround, a push button normally open switch is used to cycle between locations where the access is required.

Output Circuit:

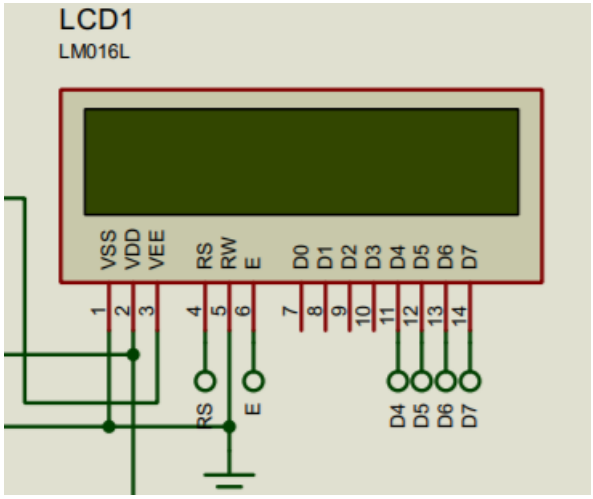

Figure 5: LCD Connection

The circuit for the LCD uses mostly the B Port of the PIC16F84A microcontroller. This allows for a single microcontroller to be used to control not only the door access logic, but also to control the LM016L LCD screen, outputting statements of location and whether entry is granted or denied, along with LED indication of Green for Entry Granted, or Red for Entry Denied.

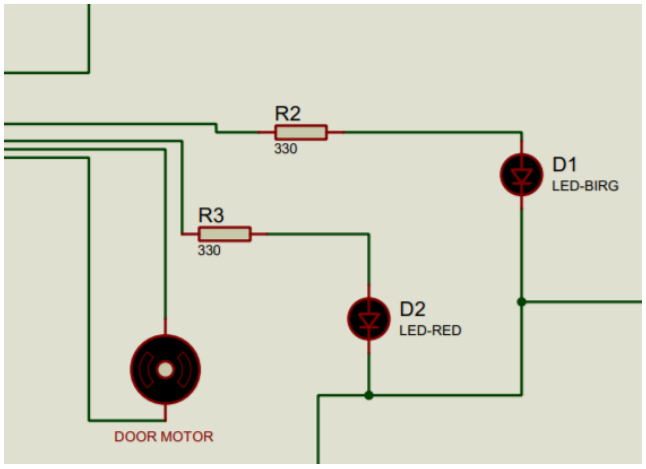

Figure 6: D1 (Green LED), D2 (Red LED) and Door Lock Motor Circuits

As per the above LCD control circuit, the LED Circuit is just a basic visual indicator as to whether personnel are granted or denied entry to a location. This circuit also includes the door motor, which would preferably be either a stepper or a servo motor, that would open or close a latch that locks the door.

Overall:

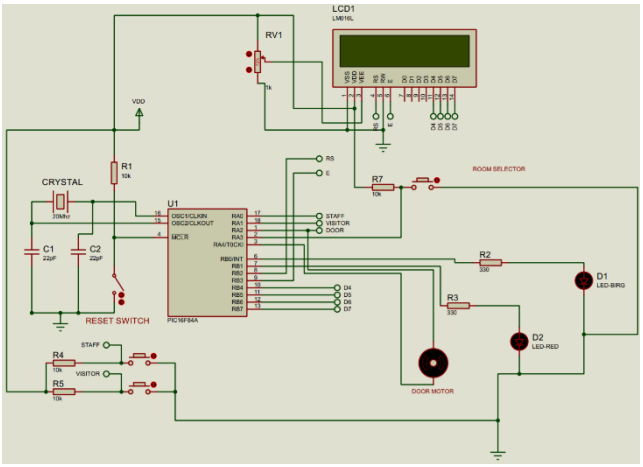

Figure 7: Overall System Schematic

4.0 SIMULATION AND TESTING

The circuit above was created in the software Proteus 8. Circuit components were chosen from the library of available components and lines were used for connections. Some connections were intentionally broken up to show each system easily and also to minimize incorrect connection due to confusion of crossed lines. The program was written and later compiled using the software CCS C Compiler. The program was tested for errors before a hex file was compiled. This compiled hex file was later loaded into the PIC Microcontroller in Proteus 8. It was then tested to see if the system works as intended. It was found to work as intended, given the limitations of coding ability.

4.0 RECOMMENDATIONS FOR FUTURE REVISIONS

In this paper, the author has discussed and presented the reasons why an automated door access system is a useful addition to the automation systems onboard. Given the low price of the microcontroller and other components used to produce the system, it is the author's hope that this can be refined and one day, implemented onboard ships as a tool to not only reduce the burden on ship crew that has to do operational duties, and also security duties, especially when the ship is calling a port for loading/discharging. However, due to the lack of ability from the author, the system showed here is currently lacking the functionality that the author has set out to achieve. However, with a programmer that has good skills and ability could be able to code the system that

fulfils all the functionality that was originally planned for it.

5.0 CONCLUSIONS

This proposed system, if created and implemented in full, will allow, for the already minimized crew onboard due to high vessel automation, a layer of security that until now is enforced manually using manpower. Of course, the system that is discussed in this paper, can be vastly improved as the level of ability of the author is basic at best. With an RFID card and reader and good coding and programming ability, the system can be improved to the point where security of the vessel's restricted areas can be left to automation, relieving at least 1 ship crew per duty from security duties. Of course, this system does not replace human judgement and security should never be taken for granted.

ACKNOWLEDGEMENTS

The authors would like to convey a great appreciation to Malaysian Maritime Academy (ALAM) and its lecturer, Mr. Ramesh Babu Amathalai, for their support into this project paper and article.

REFERENCES

[1] International Maritime Organization, ISPS Code (2003 Edition), London: IMO Publications, 2003.

[2] Microchip Technology, "PIC16F84A - Microcontrollers and Processors," Microchip Technology, [Online]. Available: https://www.microchip.com/wwwproducts/en/PIC16F84A. [Accessed 16 September 2020].

[3] Microchip Technology Inc., "PIC16F84A Data Sheet," [Online]. Available: https://ww1.microchip.com/downloads/en/devicedoc/35007b.pdf. [Accessed 16 September 2020].

[4] Datasheetspdf.com, "LM016L Datasheet | Hitachi Semiconductor - Datasheetspdf.com," 2014. [Online]. Available: https://datasheetspdf.com/datasheet/LM016L.html. [Accessed 16 September 2020].

[5] E. C. J. Nwankwo Prince. N and Nsionu Ifeanyi. I, "Design and Implementation of Microcontroller Based Security Door System (Using Mobile Phone & Computer Set)," *Journal of Automation and Control Engineering*, vol. 1, no. 1, pp. 65-69, 2013.

[6] M. Amanullah, "Microcontroller Based Reprogrammable Digital Door Lock Security System by Using Keypad & GSM/CDMA Technology," *IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)*, vol. 4, no. 6, pp. 38-42, 2013.