International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 521-538 www.ijaem.net ISSN: 2395-5252

Design and Simulation of Microcontroller Based Radio Frequency Identification (RFID) Lock System

Hussaini, S. S.[1], Lawal, A. M.[2], Sambo, A. M.[3], Muhammad, I. S.[4], Adamu, A. A.[5]
[1,2,3]Mechanical Engineering Department, Abubakar Tatari Ali Polytechnic, Wuntin Dada, Bauchi, Nigeria
[4,5]Welding and Fabrication Engineering Department, Abubakar Tatari Ali Polytechnic, Wuntin Dada, Bauchi, Nigeria
Corresponding author: Hussaini

Date of Submission: 26-07-2020 Date of Acceptance: 05-08-2020

ABSTRACT: First step towards safety was Lock and key system. Security protocol used on this device was "Single key for a single lock". This type of safety mechanism does offer security against theft, but can easily be exploited with duplicated keys. Several lock systems which ranges from simple electronic to intelligent lock system were developed, though with limitations. This research presents the Development of a Prototype RFID-Mobile communication Based Lock system aimed at addressing some of these limitations. The device was designed to detect Radio Frequency Identification (RFID) Tag brought near the RFID reader by interrogating and comparing it with what is stored in the program memory. If the data matches, a 4-digit code will be generated using linear congruential generator (LCG) technique and sent to the card holder using short mail services (SMS) via mobile communication system. The generated code will be entered through the keypad to gain entrance. The LCD displays the respective information. The device was achieved by designing the circuit using Proteus software. Using Mikro C software the control program of the device was written and builds up; the hex file generated was linked to the designed circuit for simulation. The microcontroller was programmed, the printed circuit board (PCB) was made, the components were neatly arranged and the parts were assembled. The prototype of the device was finally created. The result obtained includes: simulation result and a prototype of the device with improve reliability. With the reliability measures, the severance and the occurrence of fault decrease by 16.4% and 50% respectively. And detection increase by 11%. The RPN also reduces by 68% which was analyzed using failure mode effect and criticality analysis (FMECA).

KEYWORDS: RFID, Simulation, Lock system, Microcontroller, Buzzer.

I. INTRODUCTION

Over the years, control systems were put in place to prevent access by unauthorized persons. They are called locks on doors (Omijeh and Ajabuego, 2013). Lock and key system was the first step towards security."Single key for a single lock" became the safety protocol utilized by this gadget. This sort of safety mechanism does offer a few safety towards theft, however it can be exploited through duplication of keys (Fathima et al., 2015).

The best option considered was the Electromagnetic lock.But it has similar limitations including low break-in force, and need uninterrupted power supply to sustain the locked state, consumed more power. Solenoid, though with some limitation, now becomes preferable instrument for automatic door locking as they can save energy up to 50 percent or more (Sivarao, 2012). These aforementioned limitations and challenges necessitate the need for a lock system to possess some level of automation.

Radio Frequency Identification (RFID) – mobile communication-based lock system was developed to add to the security of restricted area.RFID gadget makes use of radio waves to transfer data from electronic tag, known as RFID tag or label, connected to an object, via a reader for the motive of figuring out and monitoring the object (Yuh-Wenet al., 2011).

Addition of mobile communication system increased the reliability of the security device. According to Qualcomm, 2014 there are about 7 billion mobile connection, almost as many as the people on earth. The research also forecast about 25 billion interconnected devices by the year 2020.The most famous second-generation mobile communication gadget is the Global System for Mobile Communication (GSM) (Sinclair, 2001). It makes use of variation of Time Division Multiple

Access (TDMA) and is the most broadly used of the two virtual wi-fi telephony technologies (Code Division Multiple access, CDMA, and TDMA). GSM digitizes and compresses data, then sends it down a channel with different streams of user data in its own instances slot. It operates at either 900 MHz or 1800MHz frequency band (Joshua et al., 2013).

The lock system function as thus: The RFID reader reads the ID number from passive Tag and sends it to the microcontroller, if the ID number is valid then microcontroller generates and sends 4-digit codes to the authenticated person mobile number using Short Mail Services (SMS), then the authenticated person enters the codes in the keypad. If the generated and entered codes matched then the lock will be opened otherwise the microcontroller activates the buzzer and it will be remains in locked position.

2.0 MATERIALS AND METHODS

2.1 Structure of the Lock System

The device has several component parts of which is the RFID system, the GSM module, password (keypad) and alarming mechanism (buzzer), as shown in Figure 1.

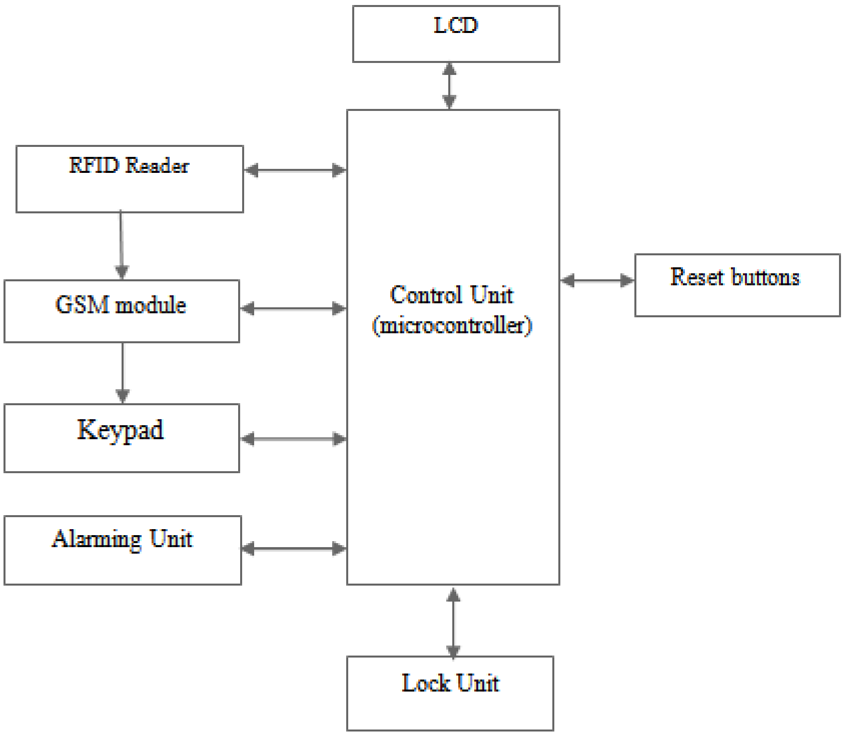

Figure 1: Block Diagram of the Lock system

Each of these parts is used for three basic component of access control (identification, authentication and confirmation) and latter was additional security feature for notification. Other components of the lock system are microcontroller and liquid crystal display (LCD). The Software that will be used is Micro C and Proteus which are used to write the codes (and load it into the microcontroller) and for simulation respectively.

The Microcontroller coordinates the operation of the system while the GSM Module Send 4-digits code generated by the microcontroller to the person after the tag has been read successfully. The Buzzer notify any closer person any attempted intruder, LCD guides the user in the operation of the system. The Key Pad will be used to enter the code after text message containing code is send to GSM of authorized user. The RFID reader reads the ID number from passive Tag and sends it to the microcontroller for confirmation, the complete circuit diagram is shown in Figure 2.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 521-538 www.ijaem.net ISSN: 2395-5252

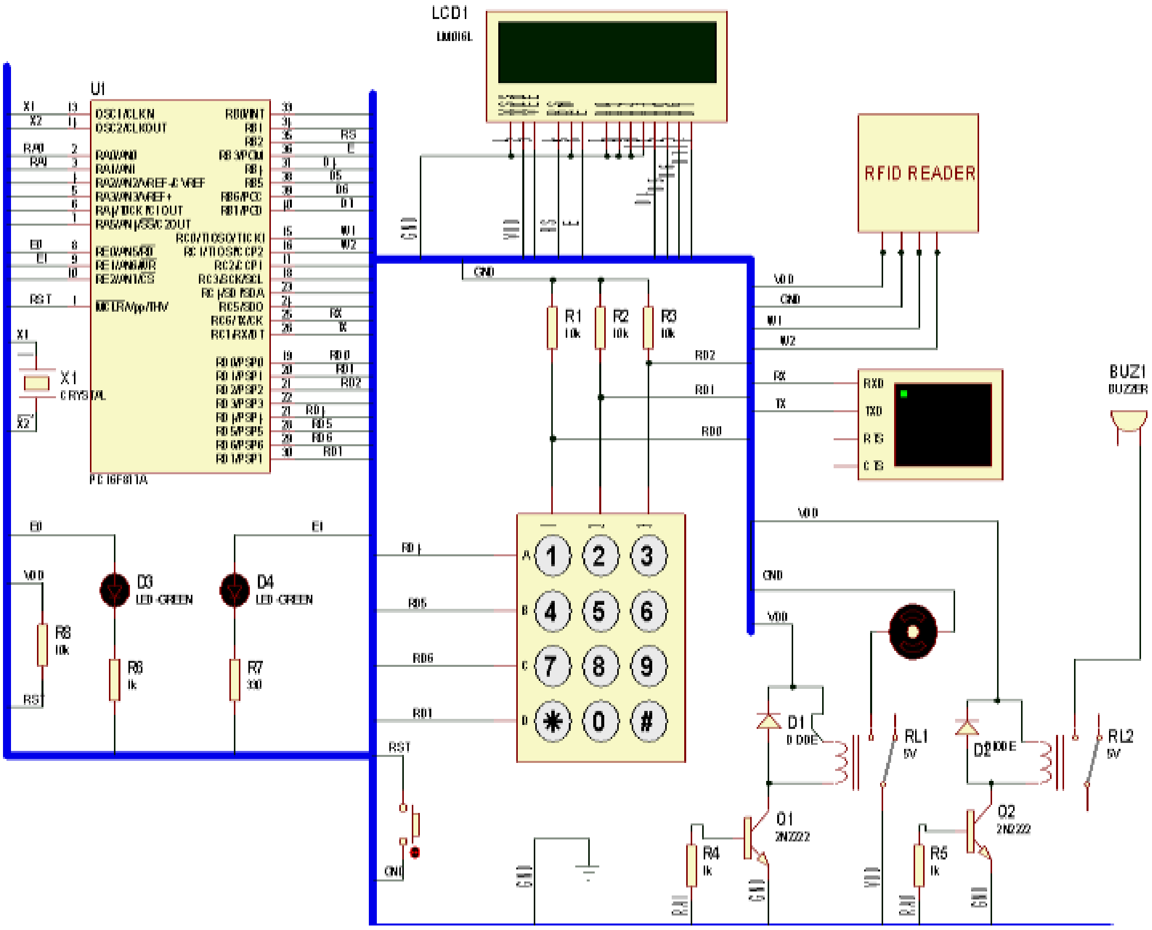

Figure 2: Complete Circuit Diagram

2.2 The Software

The Micro C software was used to write the codes and load it into the microcontroller, software known as Proteus was used to simulate the program part by part. When the program written in Micro C was built up, it generates series of ‘one’ and ‘zero’ known as ‘hex file’. The circuit drawn with Proteus software is linked to this hex file generated for simulation. There are sequences of steps aimed at programming the device to carry out the desired function, these steps and the desired output are illustrated in flow chart as shown in Figure 3.

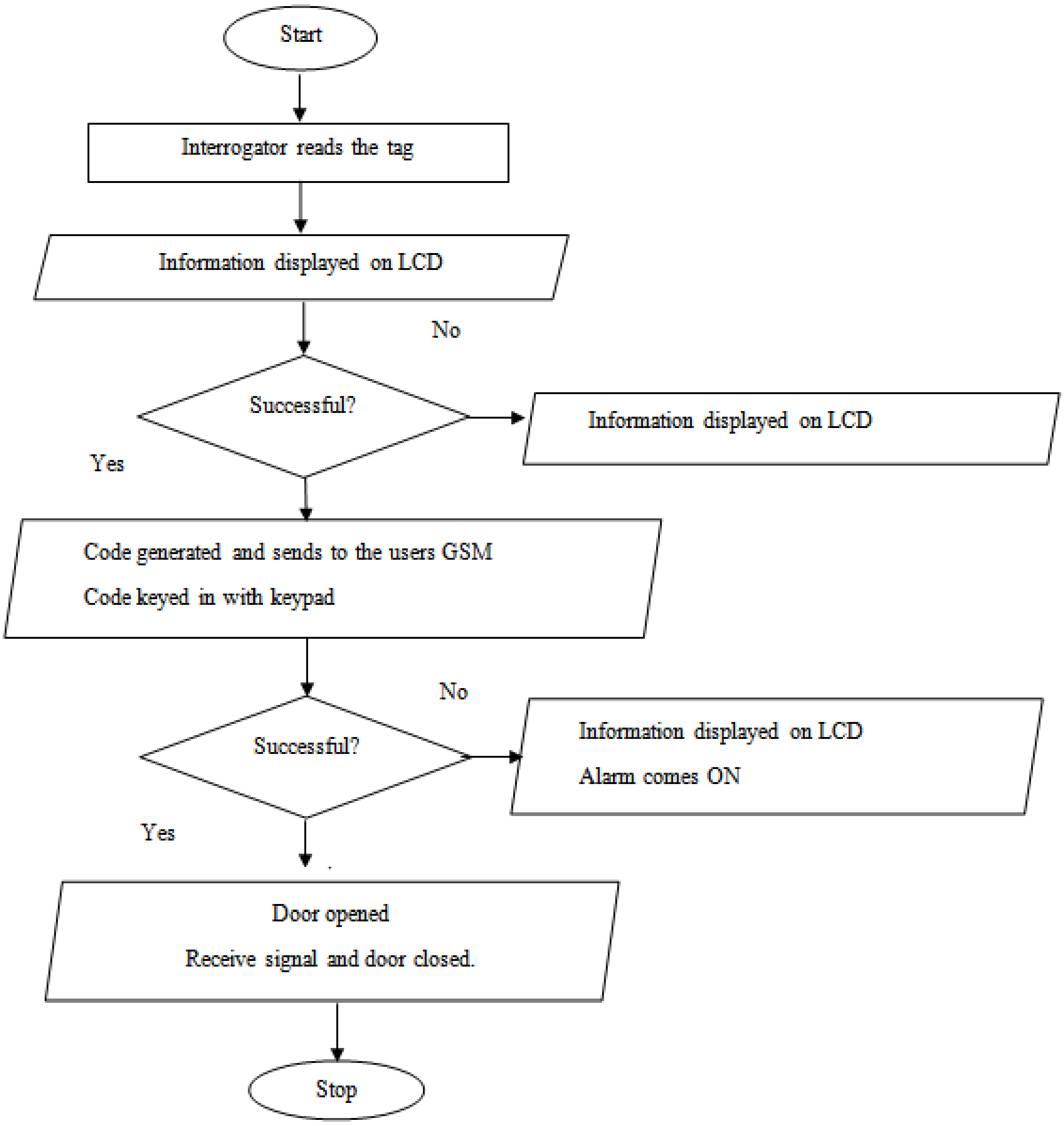

Figure 3: Flow Chart Illustrating Programming Procedure

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 521-538 www.ijaem.net ISSN: 2395-5252

2.3 Failure Mode, Effect and Criticality (FMECA)

Failure Mode and Effects Analysis (FMEA) is a proactive process aimed to examine a system, design, process and service for feasible approaches wherein failuremay occur (Sellappan and Palanikumar, 2013). An FMECA is generated from an FMEA by including a criticality figure of merit. These analyses are carried out for reliability, safety, and supportability information. The FMECA model is typically used and is suitable for hazard control.

2.3.1 Terminologies

The following terms are defined according to Akbari et al., (2013).

(i) Failure: termination of the ability of an item to perform a required function.
(ii) Failure mode: manner in which an item fails.
(iii) Failure reason and/or mechanism: reason or series of reasons that begin a process (mechanism) that ends in a failure mode over a given time. The most likely causes of the failure mode are listed under "Possible failure causes".
(iv) Failure effects: outcome of a failure mode during operation, function or status of the item.
(v) Severity: refers to the stop impact of a device failure.The higher the consequence, the more the cost of severity can be assigned to the effect.
(vi) Occurrence: refers to the frequency that a root purpose is probable to occur, defined in a qualitative way. That is not in the form of a period of time but rather in terms such as remote or occasional.
(vii) Detection: this means the chance of detecting a root reason earlier than a failure can occur.
(viii) Risk precedence Number (RPN): The Risk Priority Number is defined as the product of the Severity (S), Occurrence (O), and Detection (D) ranking. It is a degree of layout risk and the ranking levels are in a scale from 1 to1000 (Tejaskumar and Mihir, 2014).

$$\mathrm{RPN} = \mathrm{S} \times \mathrm{O} \times \mathrm{D}$$

Severity (S), Occurrence (O), and Detection (D) codes are shown in Tables 1, 2 and 3 respectively.

2.3.2 Design Failure Mode, Effect and Criticality Analysis

In order to increase the reliability of the system, the potential effect of fault, occurrence and possible detection were diligently studied. Depending on the degree, numbers were allotted and subsequently, the risk priority number was obtained for each unit. Been a series system (a failure of a unit result into failure of the system), necessary actions were taken to reduce the RPN.

2.4 Development of the Lock System

The development of the lock system was achieved by development of the component parts such as the microcontroller system, the printed circuit board (PCB), the RFID system, the GSM system, the keypad and the mechanical system.

2.4. 1 Development of Microcontroller System

The unit is implemented using a PIC microcontroller (PIC 16f877a) and some complimentary components whose choices are based on specifications by the manufacturer on the data sheet. These components include a crystal oscillator of rating 8 MHz, a 10k$\boldsymbol{\Omega}$ pull-up resistor and two stabilizing capacitors.Resonant frequency of RC oscillator relies on voltage rate, resistance R, capacitance C and working temperature (Abdulazeez, 2010).

2.4. 2 Development of Printed Circuit Board (PCB)

The circuit was designed using Proteus software; the printed circuit board (PCB) layout was simulated to ascertain the possible arrangement of the component. Several adjustments were made so that terminal sockets are closer to the edge and some are made to be as free as possible. As shown in Plate I, the LCD terminal socket (extreme right) was at the edge and other terminal sockets were free for connection.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 521-538 www.ijaem.net ISSN: 2395-5252

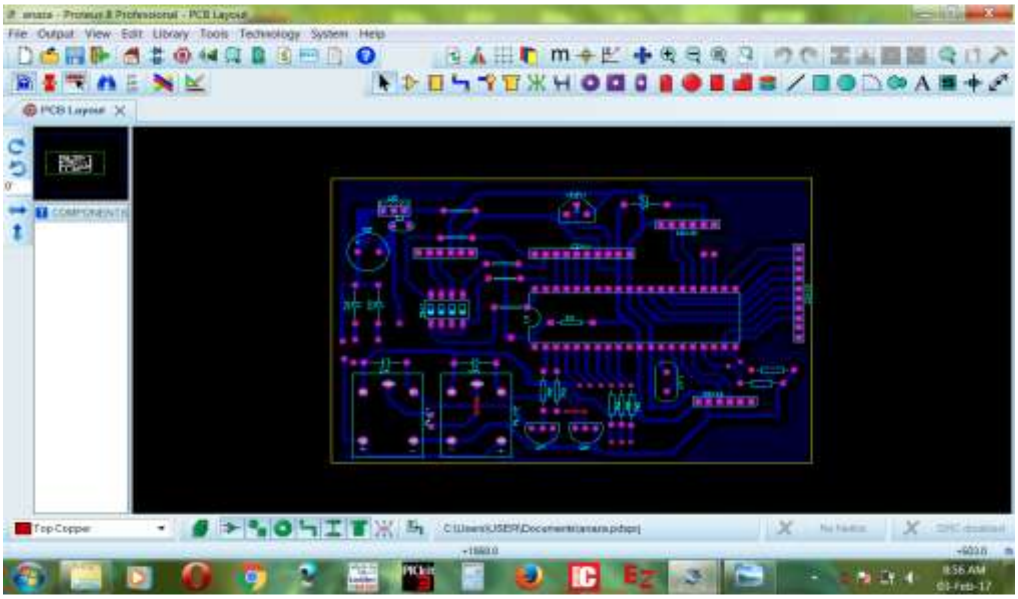

Plate I: screenshot of PCB Layout (wiring)

Adjustments were also made on the position of the relays to be at edge to give access to the connection to the motor as shown (Plate II) in the 3D solid Necessary dimension of the board was obtained for planning of parts assembling. Necessary adjustment was made to take of fastening of the board to the casing. The simulation result of 3-D view was satisfactory as shown in Plate II.

It was printed on a transparent material; the circuit was transferred to the copper clad by placing the circuit printed on transparent on the copper clad. Pressing iron regulated to temperature of about 75^0C was then moved over it to transfer the ink to the clad. Cold water was poured over it to lower the temperature and the transparent material was removed gently.

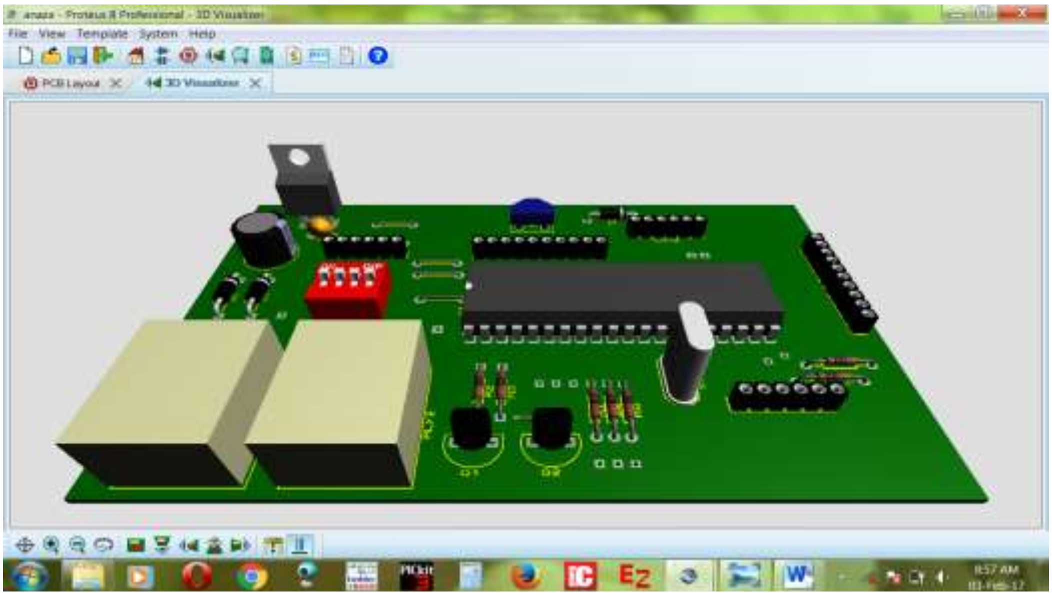

Plate II: 3-D View of the Circuit

Ferric chloride (FeCl2) was diluted to prepare a solution of FeCl2. FeCl2 was the chemical used to etch out unwanted parts (not covered with ink). Copper clad containing the printed circuit was gently immersed inside the solution. It was monitored for about 10 to 15 minutes to ascertain the level of etching. The copper clad was removed and washed inside water; hence the printed circuit board (PCB) was

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 521-538 www.ijaem.net ISSN: 2395-5252

obtained. Holes were drilled at the mounting places of the component with the aid of drilling machine

2.4.3 Development of Passive Component, RFID, GSM and Keypad System

During the developmental stage of the device, provisions were made on the PCB to accommodate the female sockets. Abiding by the pin out configuration, adequate female sockets were made on the board, male socket to an end of optical cord and the other ends to RFID reader, the GSM module and the Keypad system respectively. The connecting cords were made dismountable using sockets for flexibility and ease in troubleshooting. The components are neatly arranged on the board and soldered.

2.4.4 Developments of Casing and the Mechanical System

During the construction of the casing the dimension of the board, the RFID reader, the keypad, the GSM module etc were the basic factor considered in casing dimension and openings. The RFID reader and the keypad were arranged to be on the front of the device (prototype). Provision for reset switches was made on the front. An opening was also created where a prototype of the door will be placed.

The door (mechanical system) was also positioned in the front which is a combination of pulley, gear system, plates of plastic material, and a DC motor. The DC motor is activated by a signal from the microcontroller. It can rotate in both forward and reversed direction with the aid of relays which direct the flow of current to achieve any desired rotation.

III. RESULTS AND DISCUSSIONS

3.1 Result of Failure Mode Effect and Criticality Analysis (FMECA)

The FMECA of each unit that make up the system was analysed. For the power supply unit, battery backup was used as a backup which changes severance from 7.75 to 2 (as shown in Table 1) occurrence from 4 to 2, detection from 6.25 to 2, and risk priority number (RPN) from 236.25 to 8.

Table 1: FMECA of Power Supply Unit

Parts of power supply unit	Failure Mode	Effects (s) of Failure	Risk rating						Actions Taken	Revised risk			
			S	Cause(s) of Failure	O	Fault Detection	D	RPN		S	O	D	RPN
electrical Power supply from mains	Failure of power from mains	loss of power supply to the entire system	8	Load shedding fault, system maintenance	8	Extremely Unlikely	10	640	Battery backup, . Indicator for main power supply	2	2	2	8
Transformer	open circuit, short circuit	loss of power supply to the entire system	8	Manufacturer defect, over loading, ageing	2	Design controls have an even chances	5	80		2	2	2	8
Rectifier	open circuit, short circuit	loss of power supply to the entire system	8	Manufacturer defect, over loading, ageing	3	Design controls have an even chances	5	120		2	2	2	8

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 521-538 www.ijaem.net ISSN: 2395-5252

Voltage regulator and other component	open circuit, short circuit, Output struck, input struck,	Unfiltered and unregulated power supply	7	Manufacturer defect, over loading, ageing	3	Design controls have an even chances	5	105		2	2	2	8
	Average		7.8		4		6.3	236		2	2	2	8

It thus reduces the severance if failure occurs and possible occurrence by 74% and 50% respectively. The likelihood of failure detection increases by 68%. Subsequently the risk priority number (RPN) reduces by 97% as shown in Figure 4.

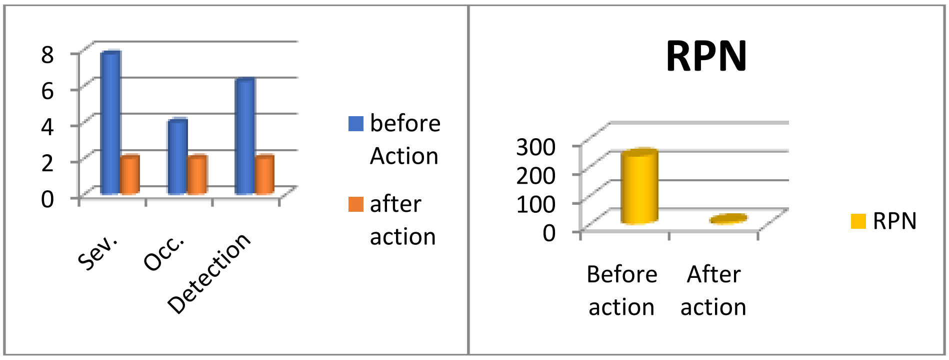

Figure 4: FMECA of Power Supply Unit

In the microcontroller unit, component earthing, careful selection of microcontroller was the action taken which changes only occurrence from 4 to1 and risk priority number (RPN) from 320 to 80 as shown in table 2.

Table 2: FMECA of Microcontroller Unit

Name of Unit/function	Failure Mode	Effects(s) of Failure	Risk rating						Actions Taken	Revised risk			
			S	Cause(s) of Failure	O	Fault Detection	D	RPN		S	O	D	RPN
Microcontroller / Interlink the units and house the software	Output struck, input struck, drift of frequency	Leads to entire system failure	8	Manufacturer defect, static charges	4	Extremely Unlikely	10	320	Component earthing	8	1	10	80

It thus reduces only the possible occurrence of failure by 75% while the severance and detection if failure occurs remains unchanged. The risk priority number (RPN) also reduces by 75% as shown in Figure 5.

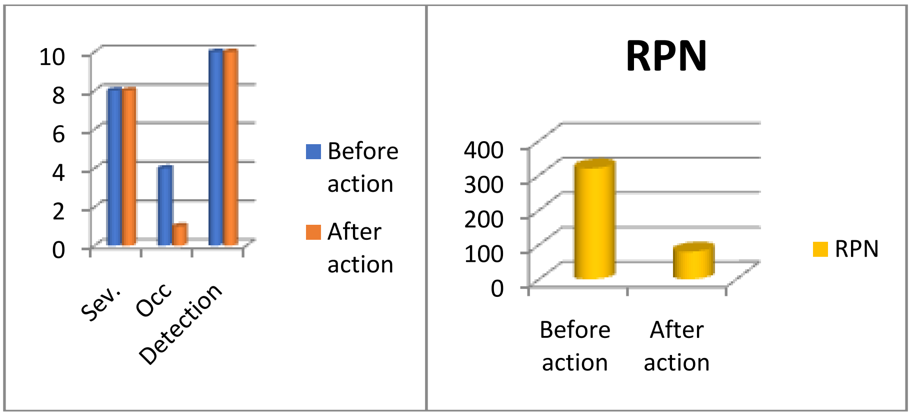

Figure 5: FMECA of Microcontroller Unit

To increase the reliability of the system, hardware redundancy, effective design and code reviews were the measures taken to increase the reliability of the software which changes the severance from 8 to 5 occurrences from 4 to 2 and Risk Priority Number (RPN) from 288 to 90 as shown in table 3.

Table 3: FMECA of Software

Name of Unit/function	Failure Mode	Effects(s) of Failure	Risk rating						Actions Taken	Revised risk			
			S	Cause(s) of Failure	O	Fault Detection	D	RPN		S	O	D	RPN
Software (Mikro C) / Responsible	Data related (Ann, 2010)	System failure	8	Software designer defect	4	Very Low Likelihood	9	288	hardware redundancy, effective	5	2	9	90
control of the entire system	Event related(Ann, 2010)	System failure	8	Software designer defect	4	Very Low Likelihood	9	288	e design and code reviews	5	2	9	90
	Average		8		4		9	288		5	2	9	90

This reduces the severance if failure occurs in the software by 37.5%, possible occurrence by 50% but the likelihood detection of such failure remains unchanged.Subsequently the Risk Priority Number (RPN) reduces by 68.75% as shown in figure 6.

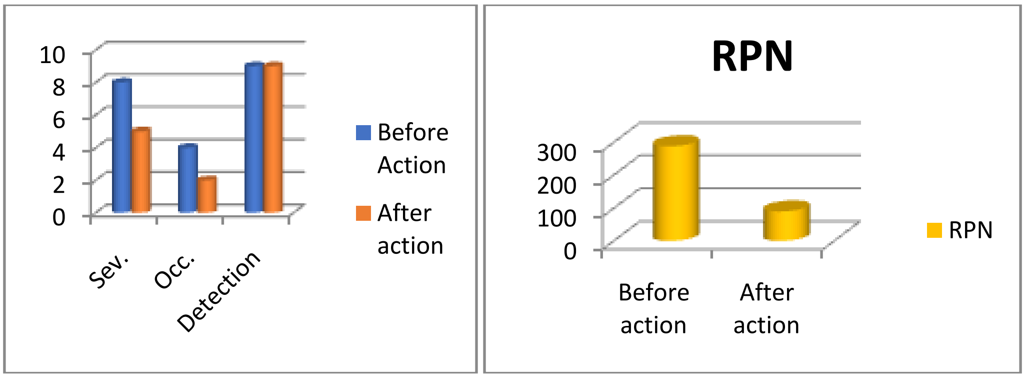

Figure 6: FMECA of Software

For the RFID system: Physical, Virus attack, cloning and eavesdropping were the possible causes of failure. The RFID system (Tag and Reader) kept hidden which changes only occurrence from 5.5 to 1.5 and Risk Priority Number (RPN) from 156 to 44 as shown in Table 4.

Table 4: Failure Mode Effect and Criticality Analysis (FMECA) of RFID System

RFID system	Failure Mode	Effects (s) of Failure	Risk rating						Actions Taken	Revised risk			
			S	Cause(s) of Failure	O	Fault Detection	D	RPN		S	O	D	RPN
Tag failure.	Output struck, drift of frequency	System failure	8	Physical, Virus attack,	5	High Likelihood	3	120	Kept hidden	8	1	3	24
Failure of reader	input struck, drift of frequency	System failure	8	Physical, Virus attack, cloning, eavesdropping	6	Moderately High Likelihood	4	192		8	2	4	6 4
	Average		8		5.5		3.5	156		8	1.5	3.5	44

It thus reduces the possible occurrence of failure by ~73% while the severance if it occurs and likelihood of detection remains unchanged. The Risk Priority Number (RPN) reduces by ~72% as shown in Figure 7.

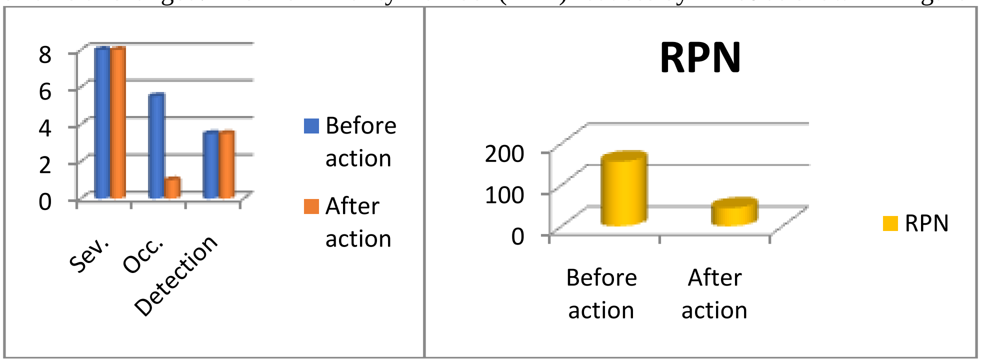

Figure 7: FMECA of RFID System

For the GSM module unit: Bad network, complete network failure and Manufacture defect, will be the likely causes of failure. Careful selection was adopted to avert the latter and a light emitting diode (LED) to indicate when a command is given to the GSM module. These changes the occurrence from 3.5 to 3.0 detection from 3.0 to 1.0 and Risk Priority Number (RPN) from 63 to 18 as shown in Table 5.

Table 5: FMECA of GSM Module Unit

GSM module	Failure Mode	Effects (s) of Failure	Risk rating						Actions Taken	Revised risk			
			S	Cause(s) of Failure	O	Fault Detection	D	RPN		S	O	D	RPN
Communication network	Network failure	System failure	5	Bad network, complete network failure	5	High Likelihood	3	75	indicator	5	5	1	75

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 521-538 www.ijaem.net ISSN: 2395-5252

GSM Module	Output struck, input struck, drift of frequency	System failure	7	Manufacture defect,	2	High Likelihood	3	42	Careful selection	7	1	1	21
	Average		6		3.5		3	63		6	3	1	18

Thus, reduce the possible occurrence of failure by ~43%. The likelihood of detection increases by 67% while the severance remains unchanged. The risk priority number (RPN) also reduces by ~76% as shown in Figure 8.

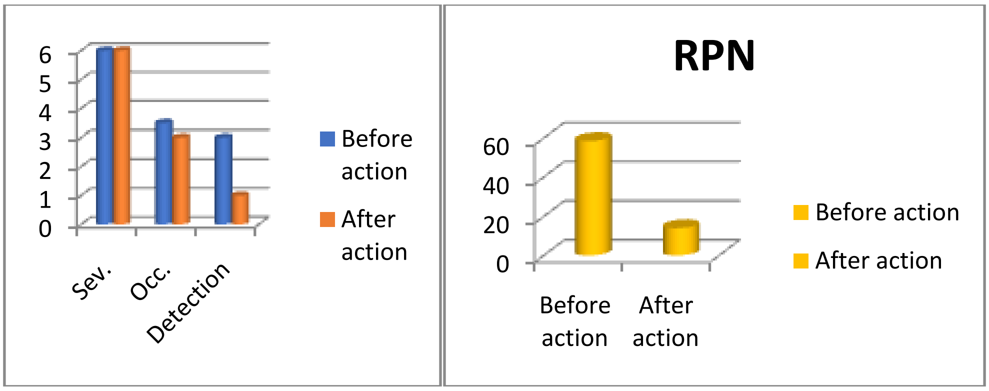

Figure 8: FMECA of GSM Module Unit

To reduce the failure rate of the system, careful selection of keypad was the measure taken in the keypad unit which changes the occurrence from 3 to 2 and Risk Priority Number (RPN) from 96 to 64 as shown in table 6.

Table 6: FMECA of Keypad Unit

Name of Unit/function	Failure Mode	Effects (s) of Failure	Risk rating						Actions Taken	Revised risk			
			S	Cause(s) of Failure	O	Fault Detection	D	RPN		S	O	D	RPN
Key pad / provide access to key-in the password.	Open circuit, short circuit	System failure	8	Manufacturer defect, ageing	3	Moderately High Likelihood	4	96	Careful selection	8	2	4	64

This reduces the possible occurrence of failure of the unit by ~33% but the severance if failure occurred and likely detection of such failure remain unchanged. Subsequently the Risk Priority Number (RPN) also reduces by 33% as shown in Figure 9.

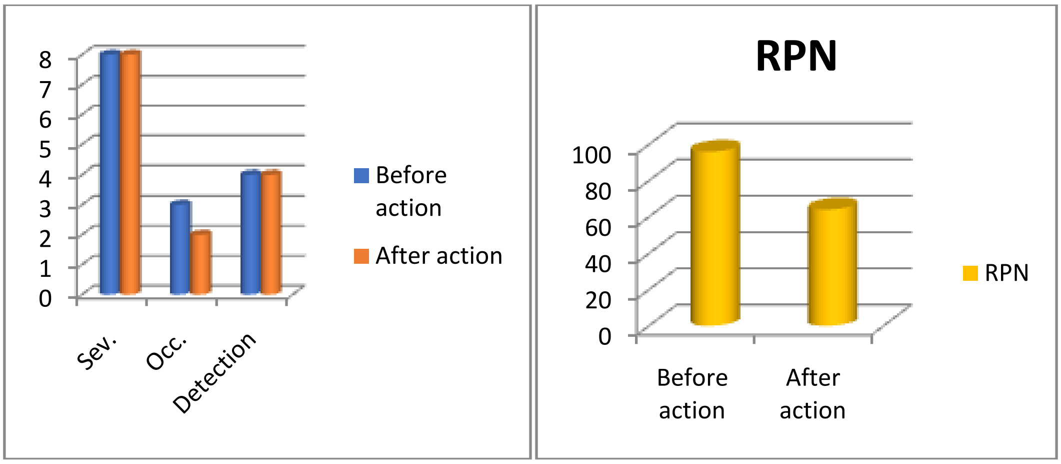

Figure 9: FMECA of Keypad Unit

High starting torques, Misalignment of teeth and worn out due to friction were predicted to be likely cause of failure. Lubrication is adopted to avert these which change the occurrence from 5 to 3 and risk priority number (RPN) from 120 to 72 as shown in Table 7.

Table 7: FMECA of Lock Unit

Name of Unit/function	Failure Mode	Effects(s) of Failure	Risk rating						Actions Taken	Revised risk			
			S	Cause(s) of Failure	O	Fault Detection	D	RPN		S	O	D	RPN
The lock or motor /opens or lock the system	Winding Failure In short Mode	System failure	8	Low starting torque, Misalignment of teeth, worn out	5	High Likelihood	3	120	Current limit circuit introduced. Redundant motor and redundant winding to be introduced.	8	3	3	72

Thus, rate of occurrence of fault is expected to reduce by 40%. The RPN also reduces by 40% as shown in Figure 10.

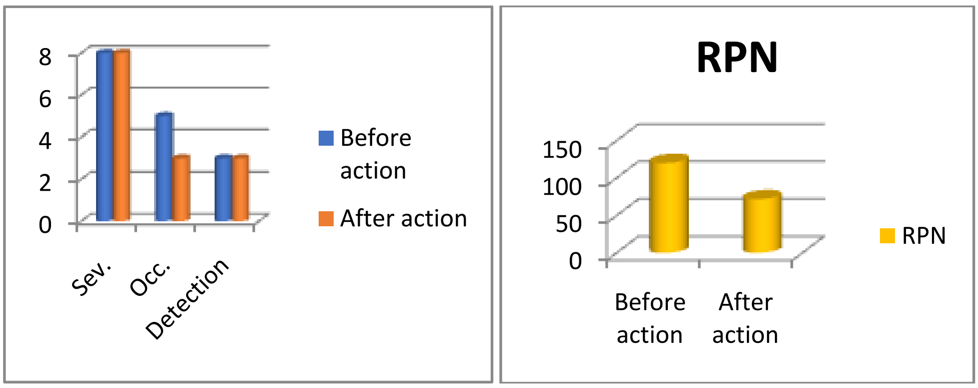

Figure 10: FMECA of Lock System

With all the measures taken to increase the reliability of the system, the severance changes from 7.69 to 6.43, occurrence from 4.14 to 2.07, detection from 5.54 to 4.93 and Risk Priority Number (RPN) 182.11 to 58 as shown in Table 8.

Table 8: FMECA of the Lock System

Name of system	Risk rating				Revised risk			
	S	O	D	RPN	S	O	D	RPN
Lock system	7.69	4.14	5.54	182.11	6.43	2.07	4.93	58

Thus, the severance of the system due to failure reduces by ~16.4 and the possible occurrence by 50%. The likely detection of such failure increase by ~11%. The RPN also reduces by ~ 68% as shown in Figure 11.

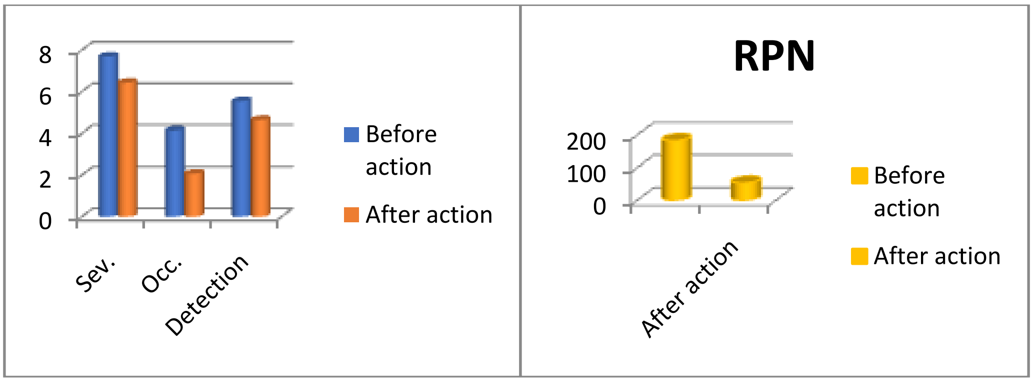

Figure 11: FMECA of the System

3.2 Development and Testing

During the construction stage of the device, the testing of device was also carried out concurrently. Plate III shows the internal structure of the device under construction.The RFID reader and the keypad are organized to be at the front of the prototype (device). The connecting cords are dismountable using sockets as shown in Plate VIII. The components are neatly arranged on the board, provision for reset switches was made on the front. An opening was also created were a prototype of the door will be placed as shown (Plate III).

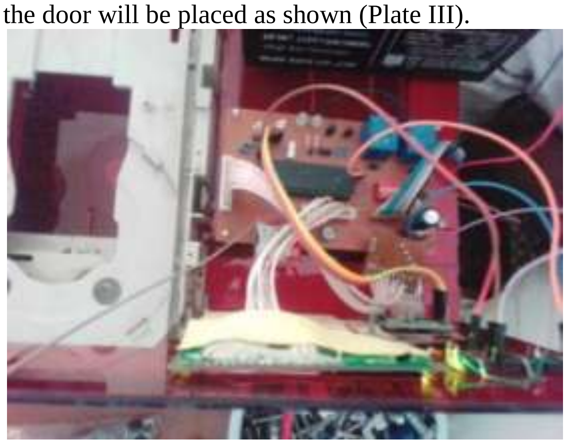

Plate III: The Internal Structure of the Device

Testing of the device begin by testing the code generating capability of the microcontroller. The microcontroller was programmed to display any code generated on the LCD to check the code generation routine. As shown in Plate IV, 2740 was the code generated and it was displayed as programmed.The checking out end result become satisfactory.

Plate IV: Testing of Code Generation

Testing of the response of the device if a right code was entered was also carried out. As

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 521-538 www.ijaem.net ISSN: 2395-5252

shown in plate V, the microcontroller was programmed to display both generated and entered codes. The generated code was 8279, the code was entered and DC motor was actuated which symbolize the opening of the door. It was successful.

Plate V: Entering of Right Code in Progress

One of the drawbacks of this device is its reliability on GSM network provider for its peration. In Nigeria, they do fail in their responsibilities. There are possibilities that in this device, the GSM module may delay to send the generated codes due to network failure or not sending at all. To localize the fault (due to network failure) if generated code is not received, the microcontroller was programmed to turn ON an LED if the command has been given to the GSM module. It was tested as shown in Plate VI and the result was satisfactory.

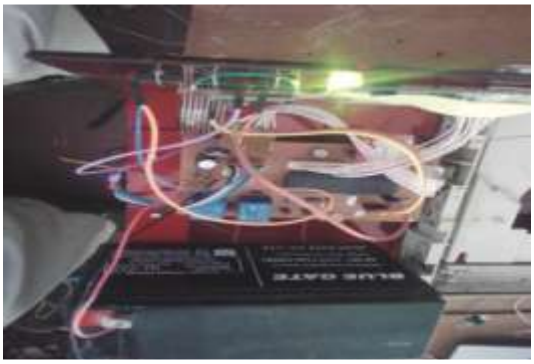

Plate VI: The LED Turn ON

3.3 **Complete Software Program of Device in Mikro C language**

```
// LCD module connections
sbit LCD_RS at RB2_bit;
sbit LCD_EN at RB3_bit;
sbit LCD_D4 at RB4_bit;
sbit LCD_D5 at RB5_bit;
sbit LCD_D6 at RB6_bit;
sbit LCD_D7 at RB7_bit;

sbitLCD_RS_Direction at TRISB2_bit;
sbitLCD_EN_Direction at TRISB3_bit;
sbit LCD_D4_Direction at TRISB4_bit;
sbit LCD_D5_Direction at TRISB5_bit;
sbit LCD_D6_Direction at TRISB6_bit;
sbit LCD_D7_Direction at TRISB7_bit;
char txt1[]= "RFID Tag Reader";
char txt2[]=  "Okon P.";
char txt3[] ="ENTER CODE";
char txt4[] ="Ag.U.";
 //char txt5[] ="wrong password";
  //char txt6[] ="reset and try ";
char message0[]=" WAIT FOR CODE" ;

// End LCD module connections
unsigned short kp,kp0,reject, cnt, oldstate = 0,res;
 // Keypad module connections
char  keypadPort at PORTD;
// End Keypad module connections
  // unsigned int CD1;
unsigned  int random;
int j ;
  // int mode;
unsignedint convert2;
unsignedint convert1;
   //char txtc [3] ;
char txtc2 [6];
char txt[5];
chardat[26];
char SC[4];
unsignedint k;
count    ;
int i;
void SMS1()
   {PORTA.F5=0;
  // delay_ms(30);

uart1_write_text("AT+CMGS=\"+2349024785438\
"\r\n");
delay_ms(30);
   uart1_write_text(txt);
delay_ms(300);
   uart1_write(0x1A);   // sends control-z, required
to end sms session
delay_ms(500); // wait
  // }
```

```
 // void SMS2()
 // {
  PORTA.F5=0;
delay_ms(2000);

uart1_write_text("AT+CMGS=\"+2348179732321\
"\r\n");
delay_ms(30);
  uart1_write_text(txt);
delay_ms(300);
  uart1_write(0x1A); // sends control-z, required to
end sms session
delay_ms(30);
  PORTA.F5=0;
 }
void comp()
 {
if ((SC[0]==txt[2]))
{ if ((SC[1]==txt[3]))
{ if ((SC[2]==txt[4]))
{ if ((SC[3]==txt[5]))

        {

reject=1;

        }
else
        { }
        }
reject=1+reject;
      }
reject=1+reject;

    }
reject=1+reject;

 //void act2()
if(reject<4)
     {
     //PORTA.F0=0;PORTA.F1=0;   //locked vault
     PORTE.F1=1;
     }
 }
void act()
 {
if(reject==4)
    {
    PORTA.F0=1; //relay
    PORTA.F1=1; //relay
delay_ms(3000);
   PORTA.F0=0; //relay
    PORTA.F1=0; //relay
    }
 }
```

```
void RANGEN()
{
random= rand()%8999+1000;
random=(random-TMR1H ) ;
  //random=1234 ;
intToStr(random,txt);          // Convert  to string
  //Lcd_out(1,1,txt);

 }

void key2()
 {
do {
kp = 0; // Reset key code variable
do  // kp = Keypad_Key_Press();  // Store key code
in kp variable
kp = Keypad_Key_Click();// Store key code in kp
variable
while (!kp); // Prepare value for output, transform
key to it's ASCII value
switch (kp)
   {
case  1: kp = 49; break; // 1        // Uncomment this
block for keypad4x4
case  2: kp = 50; break; // 2
case  3: kp = 51; break; // 3
case  4: kp = 65; break; // A
case  5: kp = 52; break; // 4
case  6: kp = 53; break; // 5
case  7: kp = 54; break; // 6
case  8: kp = 66; break; // B
case  9: kp = 55; break; // 7
case 10: kp = 56; break; // 8
case 11: kp = 57; break; // 9
case 12: kp = 67; break; // C
case 13: kp = 42; break; // *
case 14: kp = 48; break; // 0
case 15: kp = 35; break; // #
case 16: kp = 68; break; // D
      }
if (kp==42)
    {
     PORTA.F0=0;PORTA.F1=0;   //locked vault
     PORTE.F1=0;
     //Lcd_out(1, 5,"rtrt");    // =password error
break;
     }
 }
while (1);
  }
void key()
 {
do {
kp = 0; // Reset key code variable
do   // kp = Keypad_
Key_Press();// Store key code in kp variable
```

```
kp = Keypad_Key_Click();// Store key code in kp variable
while (!kp); // Prepare value for output, transform key to it's ASCII value
switch (kp)
  {
case  1: kp = 49; break; // 1   // Uncomment this block for keypad4x4
case  2: kp = 50; break; // 2
case  3: kp = 51; break; // 3
case  4: kp = 65; break; // A
case  5: kp = 52; break; // 4
case  6: kp = 53; break; // 5
case  7: kp = 54; break; // 6
case  8: kp = 66; break; // B
case  9: kp = 55; break; // 7
case 10: kp = 56; break; // 8
case 11: kp = 57; break; // 9
case 12: kp = 67; break; // C
case 13: kp = 42; break; // *
case 14: kp = 48; break; // 0
case 15: kp = 35; break; // #
case 16: kp = 68; break; // D
     }

    SC[j]=kp;
Lcd_chr(2, j+1, (SC[j])); // Print key ASCII value on LCD
j++;
if (j>3)
   {
break;
    }
 }
while (1);
 }
void main()
{
 //char i,rfid[13] = "12345678121";
  PORTA.F0=0;      // vault
   PORTA.F1=0;    // vault
   PORTE.F1=0;   //alarm
  TRISC.F0=1;
  TRISC.F1=1;
  TRISC.F2=1;
  TRISC.F5=0;
  TRISC.F4=0;
  TRISC.F3=0;
  PORTC.F3=0;
  PORTC.F5=0;
  PORTC.F4=0;
  TRISA=0;
     PORTA.F0=0;      // vault
   PORTA.F1=0;    // vault
   PORTE.F1=0;   //alarm
    TRISE.F1=0;
  PORTC.F0=0;
  PORTC.F1=0;
  OPTION_REG = 0x70;
Lcd_Init();                   // Initialize LCD
Lcd_Cmd(_LCD_CLEAR);                   // Clear display
Lcd_Cmd(_LCD_CURSOR_OFF);          // Cursor off
Lcd_Out(1,1,txt1);    // Write text in first row
Keypad_Init();                     // Initialize Keypad
  UART1_Init(9600);
cnt = 0;
  j=0;
count=0;
   T1CON.F0 = 1;
reject=0;
   PORTA.F2=0;
   PORTA.F0=0;     // vault
   PORTA.F1=0;    // vault
   PORTE.F1=0;   //alarm
while(1)
 {
     //PORTA.F1=1;
     //PORTA.F5=1;

  //PORTE.F1=0;   //alarm
 UART1_Init(9600);  // Initialize connectivity
delay_ms(500);  // wait for modem to boot up, disable this line if you power the
//modem first before the mcu
 uart1_write_text("AT\r\n"); // allow autobauding
delay_ms(500);
 UART1_Write_Text("AT+CMGF=1;\r\n");
// text format
delay_ms(300);

//UART1_Write_Text("ATD+XXXXXXXXXXXXXX;\r\n");  // call the given phone number
 // delay_ms(1000);
 PORTA.F5=1;
reject=0;
i=0;
 j=0;
while(i<26)
//repeat the loop until all 26 bit data are sent (start from 0 to 25)
{      PORTC.F3=0;
while((PORTC.F0==1)&&(PORTC.F1==1));
//wait while data0 and data1 remain at high logic level (no changes at data0 and data1)
if((PORTC.F0==0)&&(PORTC.F1==1))
//if data0 changes (data0 is active low)
                              {
dat[i]=0;                          //save that the bit received is 0
```

```
while((PORTC.F0==0)&&(PORTC.F1==1));
//wait for data stream finish sending from RFID tag again (data0 or data1 will back to high logic)
                }
else
if((PORTC.F0==1)&&(PORTC.F1==0))
//if data1 received is 0 (data1 is active low)
                {
dat[i]=1;                   //save that the bit received is 1
while((PORTC.F0==1)&&(PORTC.F1==0));
//wait for data stream finish sending from RFID tag again (data0 or data1 will back to high logic)
                }
i++;
//i+1
            }

              //no data stream received from RFID tag
i=0;                        //clear i

for(i=1;i<9;i++)                    //loop for data[0]-data[7]
            {
            convert1=(convert1<<1)|dat[i+1];
//shift current data and combine with previous data, store data in convert1
            }

for(i=0;i<16;i++)                   //loop for data[8]-data[25]
            {
            convert2=(convert2<<1)|dat[i+9];
//shift current data and combine with previous data, store data in convert2
            }
intToStr(convert2,txtc2);

Lcd_Cmd(_LCD_CLEAR);
if((txtc2[0] == ' ')&&(txtc2[1] == ' ')&& (txtc2[2] == '5')
&&(txtc2[3] == '8')&& (txtc2[4] == '1')&& (txtc2[5] == '4')&&(count<1))
        {
Lcd_Cmd(_LCD_CLEAR);
Lcd_Out(1, 5,txt2);   // ="Ag.U.";
Lcd_Out(2, 1,message0);
delay_ms(1000);
Lcd_Cmd(_LCD_CLEAR);
RANGEN();
SMS1();
key();
comp();
act();
delay_ms(3000);
key2();
        }

        // else
 ////////////////////////////////////////

if((txtc2[0] == ' ')&&(txtc2[1] == '2')&& (txtc2[2] == '9')
&&(txtc2[3] == '7')&& (txtc2[4] == '5')&& (txtc2[5] == '6')&&(count<1))
      {
Lcd_Cmd(_LCD_CLEAR);
Lcd_Out(1, 5,txt4);   // ="Ag.U.";
Lcd_Out(2, 1,message0);
delay_ms(1000);
Lcd_Cmd(_LCD_CLEAR);
RANGEN();
SMS1();
key();
comp();
act();
delay_ms(3000);
key2();
      }
      }
  }
```

IV. CONCLUSION

In conclusion, prototype of a security lock system has been designed and developed by following design procedure. The proteus software was used to design the circuit. Writing of codes and building up of program was done using Mikro C software. The drawn circuit in Proteus software was linked to the hex file generated in Mikro C and simulated.

In order to increase the reliability of the system, the potential effect of fault, occurrence and possible detection were diligently studied. Depending on the degree, numbers were allotted and subsequently, the risk priority number was obtained for each unit. Been a series system (a failure of a unit result into failure of the system), necessary action was taken to reduce the failure rate. This leads to reduction in the risk priority number (RPN).

Printed Circuit Board (PCB) layout and the solid view were designed using proteus software. The PCB layout was printed out and transferred to copper clad by means of heat. With the application of etching chemical, Printed circuit board (PCB) was made. The components were neatly arranged and the various component part of the device was tested independently. The entire device was tested, casing was made and other basic components of the system were assembled. And

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 521-538 www.ijaem.net ISSN: 2395-5252

finally, a prototype of the security device was created.

REFERENCES

[1]. Abdulazeez, M. S. A (2010). Design and implementation of a Microcontroller basedDigital information Display (DID) with keypad as input. Unpublished B.Engproject of Department of Electrical/ Electronic Engineering, Abubakar Tafawa Balewa University, Bauchi - Nigeria pp. 10

[2]. Akbari, M., Khazaee, P., Sabetghadam, I. and Karimifard, P. (2013).Failure Modes andEffects

[3]. Analysis (FMEA) for Power Transformers.28th international powersystem conference Tehran Iran.

[4]. Fathima, G., Divya, A., Jaya, S. and Manjushree, R.

[5]. (2015).Intelligent Secure System for Vehicles. International Journal for Scientific Research &Development(IJSRD).**(3)**2,438442.www.ijsrd.com.

[6]. Joshua, B.J., Aryalekshmi, S.R., Deepika, S., Kezia, G. and Maria, J. J. P.(2013).Intellectual Bank Safekeeping System.International journal of innovation in engineering and technology.**(2)**2, 321-326

[7]. Omijeh, B.O. and Ajabuego, G.O. (2013).Design Analysis of a Security Lock System using Pass-Code and Smart-Card. IOSR Journal of Electronics andCommunicationEngineering(IOSRJECE).**(4)**6,64-72. www.iosrjournals.org

[8]. Omorogiuwa, E., and Elechi, P. (2014).GSM Based

[9]. Intelligent Home Security System for Intrusion Detection. International Journal of Engineering andTechnology, **(4)**10, 595-605.

[10]. Qualcomm, (2014). The Evolution of Mobile Technologies:1Gto2Gto3Gto4GLTE.www.qualcomm.wireless

[11]. Sellappan,N. and Palanikumar, K. (2013).Modified Prioritization Methodology for Risk Priority Number in Failure Mode and Effects Analysis.International Journal ofApplied Science and Technology.**(3)**4, 27-36

[12]. Sinclair, I. (2001). Document on Cellular System CDMA and GSM.pp.1-10

[13]. Sivarao, S. (2012). Critical Review of Electro –Mechanical Door Locking System andProposal towards Development of Innovative Super Energy Saving Door LockingSystem.International Journal of Engineering and Innovative Technology (IJEIT).**(2)**5, 201-207.

[14]. Tejaskumar, S. P. and Mihir, T. P (2014). A Case

[15]. Study: A Process FMEA Tool toEnhance Quality and Efficiency of Manufacturing Industry. BonfringInternational Journal of Industrial Engineering and ManagementScience.Volume **(4)**3, 145-152

[16]. Yuh-Wen, C., David, C. Y. and Dong-Her, S. (2011). Importance- Performance Analysis for the

[17]. Adoption of Radio Frequency Identification Technology.Journal ofInformation Technology Management. Volume**(12)**2, 30-40.

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 02 Issue: 01 DOI: 10.35629/5252

www.ijaem.net
Email id: ijaem.paper@gmail.com