IJCSMA
P. K. Gaikwad, International Journal of Computer Science and Mobile Applications,
Vol.1 Issue. 3, September- 2013, pg. 18-23 ISSN: 2321-8363

DEVELOPMENT OF FPGA AND GSM BASED ADVANCED DIGITAL LOCKER SYSTEM

P. K. Gaikwad

Department of Electronics, Willingdon College, Sangli, (M.S.), INDIA

pawangaikwad2003@yahoo.co.in

Abstract

This paper shows development of a highly secured system for digital lockers. In these days, door locks are technologically advanced and the password based digital lockers are available in the market. But still, it is possible to hack the lock-code and unlock the door system by any unauthorised person. That's why; the present research work has a focus to develop a more advanced system, which communicates the owner of the office or house, when any unauthorised person tries to open the code, by giving correct code as well. While closing the door of office/house, the owner has to press the key '0' available on the hex keypad and leave the system. On arrival of unexpected person and trying to open the lock using the even the known unlock code, the Global System for Mobile communication (GSM) module activates and send the short message service (SMS) to the owner; immediately after pressing any key other than the key '0'. A Field Programmable Gate Array (FPGA) based MicroBlaze processor was designed and configured to work as Universal Asynchronous Receiver/Transmitter (UART) Soft Intellectual Proprietary (IP) Core using Xilinx Core Generator.

Keywords: Digital lock; FPGA; GSM; key '0'; SMS

1. Introduction

The present paper depicts a development of an alert system; triggered on an offence to unlock the digital lock system in the door assembly. The prototype developed in this research work sends a Short Message Service (SMS) to the house or office owner's cellular mobile phone; as soon as any unauthorised person tries to unlock the digital lock. Probably, the person who open the lock, may enter the correct unlock code. Then also the alert system gets triggered and sends the SMS. It is just essential to press a '0' key, and activate the system. Latter on this, if other than zero number key is pressed, the system gets activated for SMS.

The digital door lock security designed by researcher (Mohammad Amanullah, 2013) uses a new technology, incoming number verification system which gives more protection for controlling & security system. As Conventional security system does not use any password, there was a chance to hack or break the system. In this regard they used a desire mobile number without verification which doesn't allow the door to be opened. The system was composed of the microcontroller based by using matrix keypad & Global System for Mobile Communication (GSM) network. The password was stored in Programmable Read Only Memory (PROM) so that one could change it any time. The system has a matrix keypad. When anyone enters the code in the matrix keypad, microcontroller verifies the codes. If that code is correct the device will operate and the door will be open.

A research reported by (Santosh Gautam, 2013) implements a hardware based approach of designing security system. In that project FPGA based security system was designed capable of unlocking the door once the correct code was entered from DE2 board. Finally the output of overall system was evaluated based on the display on LCD present on De2 board of Altera Company.

When the system sends the SMS to the owner itself, and he himself unlocks the system, then he will know about working of the system. The prototype developed in this research was to enhance the level of the security systems; consisting of the digital door lock units. The embedded system was technologically advanced using Field Programmable Gate Array (FPGA) implementation for Universal Asynchronous Receiver/Transmitter (UART) core, and a GSM module was interfaced with it to send a programmed SMS character string to the owner's (preloaded) mobile phone.

2. VHDL Soft IP Core Development for the Lock System

The software development of the system to implement in the FPGA was carried our using Very High Speed Integrated Circuits Hardware Description Language (VHDL). A top level entity, instantiated with key pad driver module, as given in (Design Project, 2012), and a UART core, was developed using structural modelling style of the architecture design in VHDL. The keypad driver module given in (Design Project, 2012), accepts the 8 bit data associated with the row and column on the hex keypad. Further it decodes the key and generates a four bit data-out for display controller module. A seven segment display activated by the FPGA line displays the corresponding key number; pressed on the hex-keypad. A modification to this source code was done in such a way that, whenever other than '0' key-press occurs; an output signal gets asserted high. In other words, if a key '0' of the hex keypad detects, then such signal is de-asserted low. It plays a key role to activate the UART core, and process it further to send the serial data to the GSM module.

The UART core was generated using Xilinx Core Generator with some settings of baud rate of 9600, number of data bits, 8 etc. The details of designing such a UART core using FPGA MicroBlaze Processor using Xilinx Core Generator is given by (P.K. Gaikwad, 2013). The UART core was instantiated in the top level module for the security system in this research work. The output emerging from keypad driver module was logically ANDed with the UART transmitter line 'UART_Tx'. To initialize the security system, the user was supposed to press the key '0', and leave the system to get activated and send the security SMS by GSM module; on pressing other than '0' key by any unauthorized or other person.

The lines of VHDL program shows a part of the process for keypad decoder as given in (Design Project, 2012) which was modified as shown below.

```
process(clk)
begin   if clk'event and clk = '1' then         -- 1ms
        if sclk = "00011000011010100000" then --C1
        Col<= "0111";
        sclk <= sclk+1;
                -- check row pins
        elsif sclk = "00011000011010101000" then --R1
        if Row = "0111" then
                DecodeOut <= "0001";    --1
                gsm_EN<='1';    --R2
        elsif Row = "1011" then
                DecodeOut <= "0100";    --4
                gsm_EN<='1';    --R3
                elsif Row = "1101" then
        DecodeOut <= "0111";            --7
                gsm_EN<='1';    --R4
        elsif Row = "1110" then
                DecodeOut <= "0000";    --0
                gsm_EN<='0';
        end if;
```

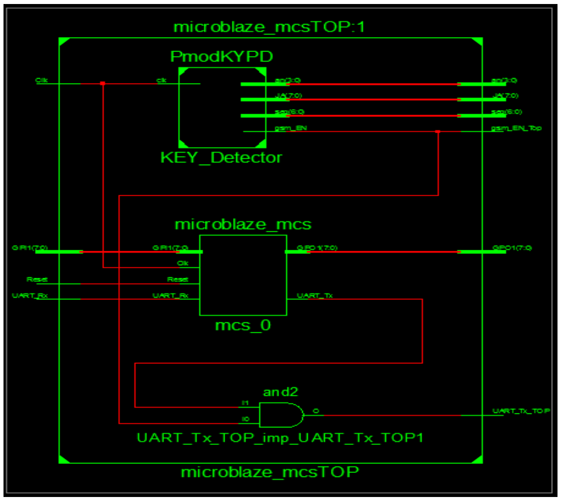


Figure 1: RTL Synthesis view of the top level module named as ‘microblaze_mcsTOP’

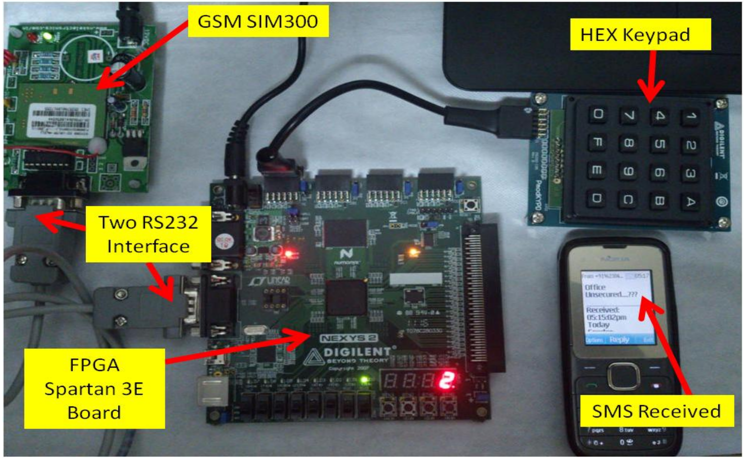


Figure 2: Hardware Implementation of the Enhanced Digital Lock System

The VHDL code shows that, when a key press of other than ‘0’ was detected, it produces logic high on the signal (‘gsm_EN’); augmented in module of key pad driver given in (Design Project, 2012). On the other hand, when a key from 1, 7 and 4, from first column of the keypad was detected pressed then it produces ‘1’ on the signal, ‘gsm_EN’. The similar process of detecting the key-press was performed for remaining keys on the hex keypad, which produce logic ‘1’ on signal named as ‘gsm_EN’.

The process of activating the UART core; embedded in the FPGA’s MicroBlaze processor resumes, only when signal ‘gsm_EN’ gets logic high on it, because the ‘UART_Tx’ signal from UART transmitter line is logically ANDed with the decoder module signal, ‘gsm_EN’. The port direction of signal ‘gsm_EN’ was therefore declared with ‘inout’ mode. Thus, the AND gate was having two inputs: one was ‘gsm_EN’ and another was the output line of UART core named as ‘UART_Tx’. The output signal of the AND gate was named as ‘UART_Tx_TOP’.

3. Synthesis of the Digital Lock System Soft IP Core

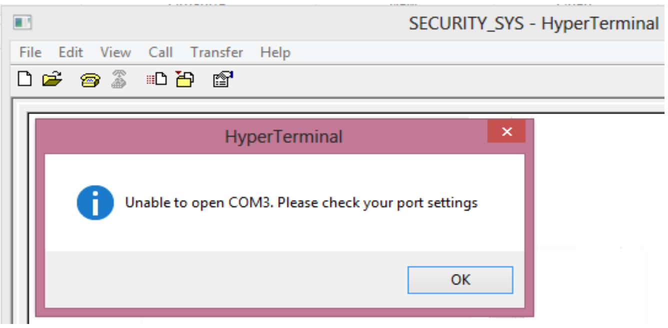
The Figure 1 shows the Register Transfer Level (RTL) view obtained after performing synthesis process for the top level module; comprising instantiated entities in it.

It shows that there are three modules namely, ‘PmodKEYPD’, ‘microblaze_mcs’ and a two input AND gate with its name, ‘and2’. The top level module contain only two VHDL entities, but the third module ‘and2’ was designed by VHDL keyword ‘and’; used in the top level soft IP core, as shown in following line of VHDL code.

UART_Tx_TOP <= gsm_EN_Top and UART_Tx_int;

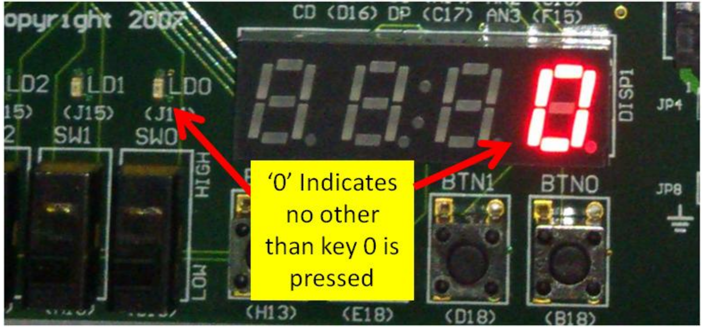
The ‘UART_Tx_int’ is an internal signal, connected to the ‘UART_Tx’ line of the UART core; implemented by the Xilinx MicroBlaze processor.

The Xilinx ISE Design flow was further performed with the process of Implementation after writing the user constraints file (.ucf). A bit file was generated; following to the successful implementation process, and it was downloaded into the PROM available on the FPGA Spartan 3E board Nexys2, developed by Digilent Inc. The interfacing details of the Nexys2 board are given in (Reference manual, 2011). The Adept software was use to download the .bit file into the onboard PROM.


SECURITY_SYS - HyperTerminal
File Edit View Call Transfer Help
HyperTerminal
OK

Unable to open COM3. Please check your port settings

Figure 3: Hyper terminal screenshot when key ‘0’ was pressed



‘0’ Indicates no other than key 0 is pressed

Figure 4: FPGA displays number ‘0’ on seven segment display and indicates logic ‘0’ on LED

4. Verification of the System at Hardware Level

The Figure 2 illustrates different hardware modules interfaced to develop the prototype system for digital lock. It consists of a GSM SIM300 module. The serial port of the GSM module was connected with the UART line of the FPGA board, Nexys2. A hex keypad consisting of 16 keys from ‘0’ to ‘F’ is also shown.

The cellular phone shown in Figure 2 displays an SMS received when the key, other than ‘0’ was pressed. The message string shown in the mobile phone display was “Office Unsecured...?”. This message was sent to the mobile from GSM module, only when key ‘2’ (other than ‘0’) was pressed.

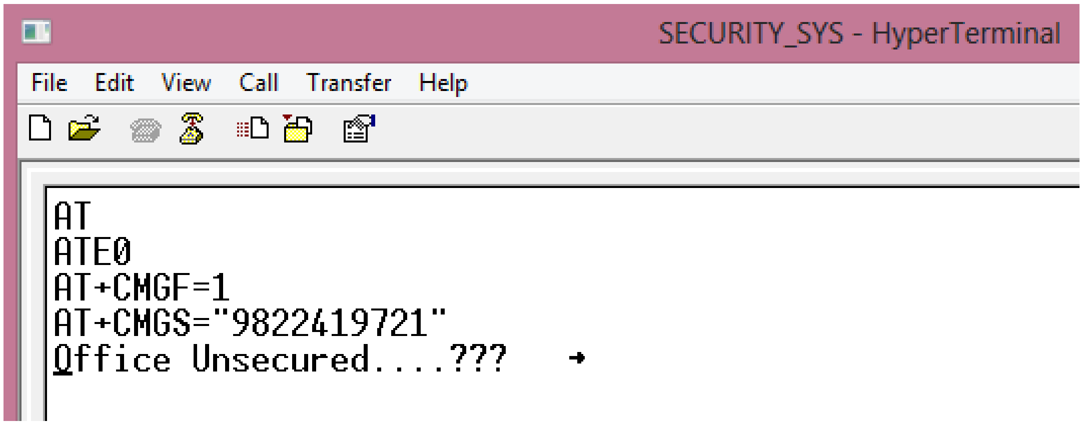
The FPGA board, Nexys2 also shows the associated key number displayed on the seven segment display. An LED was made ON, during the same process of sending the SMS; indicating visual alert of unauthorised entry in the door system. The LED port could be connected to the siren for the local level alert as well.

The digital door lock system was also tested on the hyper terminal ensure and verify it before launching in real time operation of sending the SMS. The Figure 3 depicts the hyper terminal output shown on the computer monitor, when the key ‘0’ was pressed and trying to send SMS; by reset operation on the FPGA board.

The Figure 3 shows that it is not possible to open the serial COM port, because by pressing the key ‘0’, the keypad decoder module, implemented inside the top level entity sends a logic ‘0’ and disables the ‘UART-Tx’ line of the UART core. Therefore, it was not possible to make any communication from FPGA’s UART to hyper terminal of IBM PC. In other words, the security system was now ready to detect whether any key press of other than '0' takes place or not. The same phenomenon is also shown at FPGA hardware level, simultaneously as shown in Figure 4.

The LED0 is off and a number '0' is also displayed on seven segment unit, it means that, the key '0' was pressed and the system was just waiting to monitor for the key press; other than '0'.

The Figure5 illustrates the Attention (AT) commands sent from FPGA based UART module to the hyper terminal and are displayed on computer screen. It reveals, the key other than '0' was pressed; therefore the UART output of the top level entity was routed to the hyper terminal through the serial port. The Figure 5 shows various necessary AT commands to drive the GSM SIM300 module.


SECURITY_SYS - HyperTerminal
File Edit View Call Transfer Help

```
AT
ATE0
AT+CMGF=1
AT+CMGS="9822419721"
Office Unsecured....???
```

Figure 5: AT commands and SMS string displayed on PC's hyper terminal

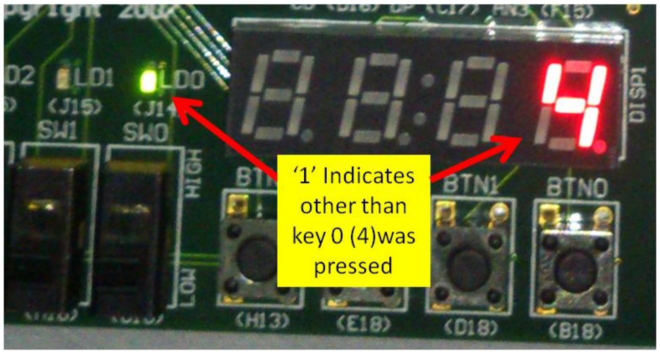


Figure 6: FPGA board displays number '4' and glows LED0 when key 4 on the hex keypad was pressed

The Figure 6 indicates that the key '4' was pressed, and tried to unlock the digital door lock security system. Even the know key was pressed; the system gets triggered to send the alert SMS.

4. Conclusion

The present paper is a development of the digital lock system, even after knowing the unlock code, the system sends an SMS to the office/house owner's mobile phone. The system has to be activated by the owner just pressing key '0' available on the hex keypad and leave it. The moment whenever an unauthorized person tries to press, even first key of the total unlock known code as well, the FPGA based UART gets activated and triggers the GSM module to send the SMS to owner's mobile phone.

References:

[1] Design Project, 2012, "PmodKYPD - 16-Button Keypad", *Digilent Inc.,* DSD-0000337, *retrieved from* http://digilentinc.com/Products/Detail.cfm?NavPath=2,401,940&Prod=PMODKYPD
[2] Mohammad Amanullah, 2013, Microcontroller Based Reprogrammable Digital Door Lock Security System by Using Keypad & GSM/CDMA Technology, *IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE),* Volume 4, Issue 6, pp. 38-42.
[3] P.K. Gaikwad, 2013, Development of FPGA MicroBlaze Processor for GSM based Heart Rate Monitoring System, *International Journal of Advanced Computer Research*, unpublished
[4] Reference manual, 2011, Digilent Nexys2 Board Refference Manual, *Digilent Inc., Pullman, WA 99163,* Doc: 502-134
[5] Santosh Gautam, 2013, FPGA: Based Security login System, *retrieved from* http://www.academia.edu/3717086/FPGA_Based_Security_login_System#

Author Profile:

P.K. Gaikwad – Dr. Pawan K. Gaikwad, born in INDIA, on August 29th, 1976, is M.Sc.-Electronic Science, from Department of Electronic Science, University of Pune, Pune(1999), Ph.D. in Electronics(2010), Diploma in VLSI Design, Pune(2000). He is a Research Guide in Electronics for the faculty of Science in Shivaji University, Kolhapur (Maharashtra), INDIA.