

An Approach for Security Systems Using seeUsee

Santhosh Damodaran

*Department of Electrical and Electronics Engineering
SNS College of Technology, Coimbatore, Tamil Nadu, India*

Gowtham Veluchamy

*Department of Electrical and Electronics Engineering
SNS College of Technology, Coimbatore, Tamil Nadu, India*

Pradeep Rajan

*Assistant Professor, Department of Electrical and Electronics Engineering
SNS College of Technology, Coimbatore, Tamil Nadu, India*

Abstract- Secure Each and Everything you see" acronym is seeUsee, First of all the idea is about combining all the security into a single device called seeUsee . We have so many security devices which is specially made for specific targets like automobile , housing , computer , safety lockers , Tracking systems but there is no such device for all together. Bringing out the Technical feasibility along with Commercial viability is the main aim of this seeUsee.

Keywords – seeUsee , Security Systems

I. INTRODUCTION

The point which gave birth to this idea is that the property wanted to be safe and the Proprietor wanted to know every second whether it is safe or not and the Proprietor need to get the alert if it is stolen not others surrounding the property because the Proprietor care much about the object than others If , The Proprietor get an alert even when he is 100's of Km away he can take some action or he can send some reliable person to go have a look at it , and like concentrating on many security items for different things is not reliable , Bringing all the security checks under one device and everything to be secure and safe , this thought brought out to think about seeUsee.

The rest of the paper is organized as follows. II. Idea III. Basic Operation IV. Construction V. unit of seeUsee VI. Conclusion

II. IDEA

A. Concept –

The main device will be in Proprietor hands always , and each secondary device consists of two small components only with the help of main device one can establish or create a contact between the two secondary peripherals with the help of a patch chord, once the contact has been made the sensor i.e. LM 35[2] will produces a sensor surrounding the object , The Proprietor can remove the patch chord and take along with him where ever he go , The main point is that , the main device and the secondary peripherals which he have activated will always remain synchronized and once the contact has been broken between or in and around the peripherals , He get an alert in the main device and with the help of GPS , He come to know where the object has been stolen or where it is hijacked . And he can turn off that Secondary peripheral Synchronization only if he has that main device in his hands, and none can cross the secondary peripherals without crossing the activated sensors, hence primary device remains with you and secondary peripherals remains fixed to the material you wanted to be secure

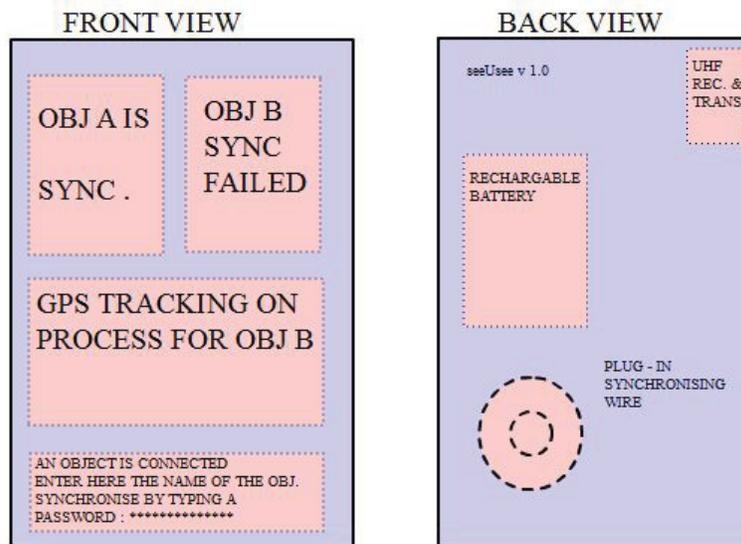


Figure 1. Main Device

Imaginary view of the main device (Front & Back View)

B. Applications –

- 1) Highly expandable and up gradation to any extent is possible
- 2) Easily portable and reliable
- 3) One single device for everything , can be synchronized with any Kind of Automobile , locker , Debit Card lock , Door safety , Computer Safety etc. with the advancement anything can be achieved these are just the start for the next generation ,

Take seeUsee device throw your keys off , switch off your cameras , just synchronize your peripherals and be secure with everything .

C. Technical Feasibility –

It is possible with the special kind of software's designed specifically for this device and some alterations , according to the necessity .

- 1) Main device consists of specially designed , with UHF receiver (For this being a basic model and first of its kind We prefer Ultra High Frequency[1] signal because it has wide range of frequencies and also high secure, so signal can be received easily) , GPS , ports to make synchronization possible in the secondary peripherals
- 2) Secondary Peripherals can be made according to the area we prefer , It can be a beam of light in the case of doors , and sensors in the case of Automobiles etc.

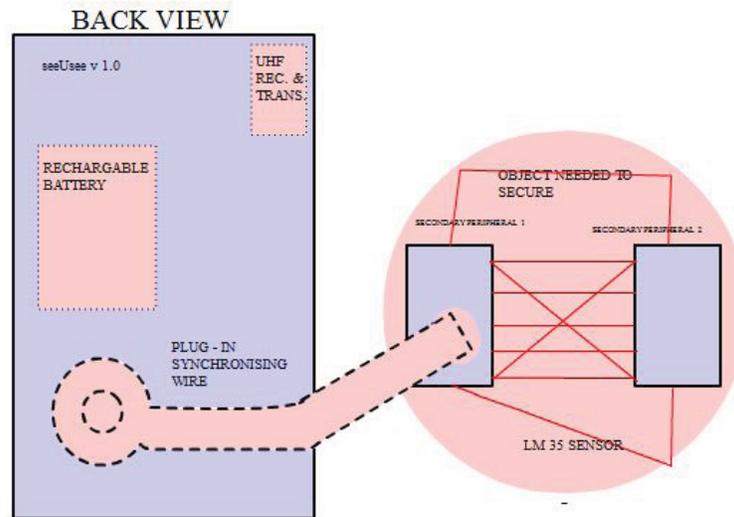


Figure 2. Synchronization Process

Imaginary view of the main device synchronizing with the Secondary peripherals with the patch chord (Back View)

III. BASIC OPERATION

A. Working –

If the security has to be given to two or more objects, According to the object the designed secondary peripherals are fixed in the object A, then with the main device and the patch chord the synchronization is made between the object A and the main device by typing a password by doing this the synchronization is made between them, In the main device screen you can see that object A is synchronized, and in the same way you can synchronize for object B also, If suppose the synchronization fails in the object B, then GPS tracking process starts for the object B refer Figure. 1, The entered password will be stored in the EEPROM[3] and the controller used in this basic design is ATMEGA 16 AVR[4].

B. Case Study –

For Example, As Shown in the Figure. 2 I have made Synchronization with my cupboard and I need my cupboard not to be open other than my mother and I need my bike not to be moved other than my father, Assume it, So I have a main device, I have a secondary peripheral attached to my cup board and another secondary peripheral in my bike, so I have attached these both permanently in my cup board and in my bike, with the help of my main device I have connected in the secondary peripherals of the cupboard and established an synchronization and similarly I did the same with my bike (note: the secondary peripherals can be of any model according to the necessity refer Figure. 3 but the main device is of same type) So I have an synchronization with my cup board and my bike in my main device and I have gone out of station with my main device, If the synchronization in the cupboard somehow got disturbed, I will get the notification immediately and surrounding my cupboard the reliable person i.e. my mother, so I'll immediately inform her to have a look what's going on by this way I can secure my cup board to some extent, If suppose I get a notification that my bike has been hijacked I'll immediately call my reliable person that is my father to have a look at it, if at all the situation is out of hand, the GPS in the main device tells us exactly where is our bike located and thereby I can take some action to safeguard it, So by this device I'm totally taking care of whole of my property even when I'm not near.

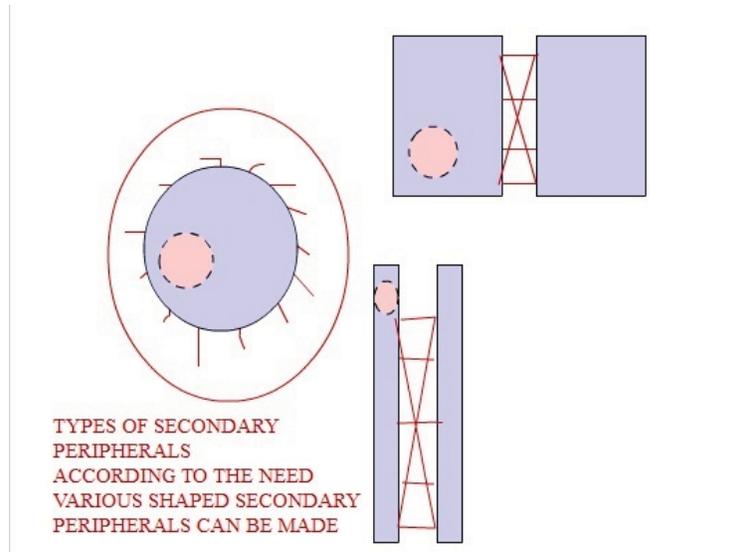


Figure 3. Secondary Peripherals

Imaginary view of different types of Secondary peripherals with the activated sensors surrounding it

IV. CONSTRUCTION

The Secondary peripherals consists of the following components embedded in it they are

- [1] ATMEGA 16 AVR[4]
- [2] EEPROM[3]
- [3] LM 35[2]
- [4] GPS TRANSMITTER
- [5] PATCH CHORD OPENING
- [6] UHF TRANSMITTING RANGE
- [7] BATTERY

The Microcontroller used , has the program embedded in it , and the Patch chord port is used to connect with the main device and the LM 35 produces a sensor , It will get activated only by the instruction send by the microprocessor and this in turn activates the GPS transmitter which remain contact with the main device , the signal is transmitted via the Ultra high frequency range , The whole process is supported by the Battery attached to it refer Figure. 4 . By looking at the specified area the Battery can be varied or it can be connected to the power supply when the object is always in a permanent place , This can be set up like , when the power supply goes off , Intimation is provided in the main device as such .

The Main device consists of the following component embedded in it

- [1] The Same Microcontroller
- [2] Memory Space
- [3] Battery
- [4] UHF receiving signal
- [5] Display space
- [6] GPS Receiver
- [7] Patch chord opening

The Main device consists of the components which the size is all controlled to that of a smart phone so that it can be easily portable and handled easily , After synchronization the signal is received by the UHF range to the main device , here the signals are processed and the microcontroller process the signal which displays the data in the display so that it can be viewed by the user . For synchronization the password is typed by the user in the display of the main device .

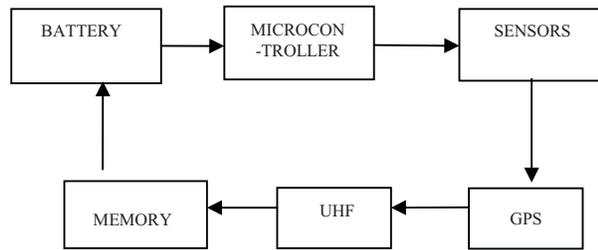


Figure 4. Secondary Peripheral Block Diagram

View of the components attached in the Secondary peripherals

V. UNIT OF SEEUSEE

If suppose the user misses his main device , He can approach the unit of seeUsee to have a change or have a similar duplication of the device with proper submission of proof , If at all he loses his main device we suggest to immediately look after the object he has put in a security . Any type of hacking in the secondary peripherals or any kind of removal desynchronizes the main devices which will show the intimation in the display unit , By this any kind of interrupts can be easily noted and intimated . So the ultimate aim of the project satisfied by this process .

VI. CONCLUSION

seeUsee device is in the initial stage of development , The ultimate aim is to reach the end user the common people , No one should hesitate to buy this device , Since most of the Security devices cost is too high and only few come forward to buy them that too the security device they buy is specified to only one purpose , But this seeUsee is being built in the idea of multipurpose use , with high security and also at a nominal cost .

REFERENCES

- [1] http://www.myerseng.com/uhf_transmitter2.
- [2] <http://www.ti.com/lit/ds/symlink/lm35.pdf>
- [3] <http://www.atmel.in/products/memories/default.aspx>
- [4] http://www.atmel.com/images/atmel-2486-8-bit-avr-microcontroller-atmega8_1_datasheet.pdf.