Genti PROGRI, Julian PRISKA, Entela PROGRI

THE DEVELOPMENT OF A SECURITY SYSTEM FOR AN AUTHORIZED ENTRANCE

Abstract

The development of a security system for an authorized entrance.

The purpose of this work is to study and to create a new way of controlling the passage in secured buildings and objects that require a specific degree of security. The creation of a certain system would improve the activities of many companies, malls, shopping centers, parking lots, airports, banks etc. The security system that will be presented in this work is based on the activation of magnetic keys through a microcontroller that is dictated by a computer or an infrared remote control system. The passage of the magnetic key from '1' or '0', when the command comes from the computer, a scan of the fingerprint of the
person passing through the door is carried out, but also when the personnel is intervening in cases such as:

- The presence of VIP.
- The lack of the ability to read fingerprints.

The system automatically provides visuals of the people appearing at the point of passage. Built-in applications provide the ability to file data as well as provide up-to-date reports and information.

Key Words: *Arduino Uno, DC 5V Stepper Motor 28BYJ-48, ULN2003 Driver, Wireless Camera, Magnetic Door Locks 12V, YL-99 Collision Switch Module, 5V Relay Module for Arduino, PIR Motion Sensor*

1. INTRODUCTION

The security system being presented in this article is part of the group known as Access Control & Security Systems Integration. The purpose of these systems is the surveillance and control of the building at every moment. Nowadays these systems are widely used not only by companies but also individuals who want to secure their property. Each system has three steps which are:

- Gathering of the data from electronis devices such as sensors, which are of different physical properties.
- Analysis of this data, as well as getting results.
- Activation of parts of the system according to the results gathered from the second part, which help in the completion of the predetermined steps.

The three previous steps can be expressed as components such as:

- Identification/Gathering of information *Identification*
- Authentication of the gathered information *Authentication*
- Authorization of the subject to have access *Authorization*

Identification/Gatheing of the information is a process which can be realised through electronic devices (sensors, magnetic readers, optical readers, RFID, etc) or through registartion from the service staff. The technology used for gathering the information is really important as the mistakes that are formed during the process of identification can result in the failure of the system. So:

1. The biometric verification through the fingerprint can sometimes cause problems that are related to the physical changes that happen to the fingerprint of an individual. The system would not be able to identify the person.
2. The RFID verification, known as Radio Frequency Identification, is a technology that has a wide use in some fields such as the one of

the doors. However, these sistems are not insensitive when it comes to electromagnetic noises[1].

There are two methods that use the eye characteristics for the identification.

- The first method is based on reading the eye retina. The user should look straight at a device that scans the retina using a laser. The device then analyzes the configuration of the blood vessels of the picture obtained from the scan. This way, the device can identify the user. The configuration of the blood vessels is unique for each eye. However,being that we are using a laser, it is not fully safe for the user. It is not easy to manipulate the system when using such a technology. The main issues related to this technology are the damage of the eye as well as the high cost of the system[2][3].
- The second method is based on the identification of the iris of the eye. A photographic device takes a picture of the eye. Different from the first method, you do not need to be close to the device that will take a picture of the eye. The picture is then analyzed by another device and it has 266 different identifying dots. It is said that this is the most reliable method. Furthermore, the irisis stable thourghout our whole life. All 266 dots are based upon characteristics of the iris for each person. Just like in the first method, it is not easy to manipulate a system using this technology. Both methods are currently applied in some developed countries[2][3].

Authentication of the gathered information is done using computer programs or microcontrollers that analyze this information using algorithms and specific mathematical logics bringing as a result the simplest values as an aswer, ‘True’ or ‘False’. The authorization of the subject to have access is based upon a couple of criteria. Access is given through authorized lists or the users profile.

In order for all of the three components to work, they need an environment made of applications,

operating systems, database, ruters, firewalls etc [4].

The security system that is being presented in this article is based upon the activization of the magnetic key, which allows the door of the room to open or not, using an Arduino Uno microcontroller which can be directed from:

- The computer which communicates with the Arduino Uno through a serial port.
- A system using infrared distance, which are known in literaturea as Remote Control Infrared.

The autorized individuals are identified by the system through the use of their credentials. These credentials can be the magnetic key, fingerprints, retina of the eye or a personal identification number (for example a passport) for this individual. Each credential is unique for each person. The switch of the magnetic key from '1' (open- the door is free or open) to '0' (closed- the door is blocked and can not be opened) is done after the scan of the fingerprint of the person that needs to pass. Staff can interfere in these two cases when:

- There are VIP-s present.
- Inability to have an identification through the fingerprint.

The system automatically collects visuals of the people that are present at the passing point as well as manually obtaining visuals of the person from the staff. The aplications provide the possibility of hourly reports that include all this data.

2. THE MODEL OF THE SYSTEM FOR THE DOOR SECURITY

The elements that are part of this system are being introduced as below, separated in two different groups, devices and applications.

Devices:

- Computer

- Arduino Uno microcontroller [8]

- DC 5V Stepper Motor 28BYJ-48 + ULN2003 Driver + Wireless Camera

- Power Supply 12V, 25A
- Magnetic Door Locks 12V
- 5V Relay Module for Arduino

- YL-99 Collision Switch Module
- LED

- PIR Motion Sensor (movement sensor for arduino)
- LED

- HX1838 VS1838 NEC Infrared IR Wireless Remote Control Sensor Module For arduino

Applications:

- The computer application that sends commands and information to arduino, while directing the movement of the camera mounted on the axis of the stepper-motor connected to the microcontroller, and takes the images and videos which are being transimtted through waves to the computer. This application can manage all the information taken from the system data+image.

- The application inside the microcontroller analyzes the information gathered from the sensors, it activates the magnetic key through rele as well as LED lights that show the state of the door, and the identification of any object in front of the door.

- The front-office application that manages personal data of the staff, information regarding the time each individual of the staff spends at work, their history as well as a library including images obtained from the security system. This application will be part of another article.

In Figure 1, we have showed the schematics of the security system for the door.

.

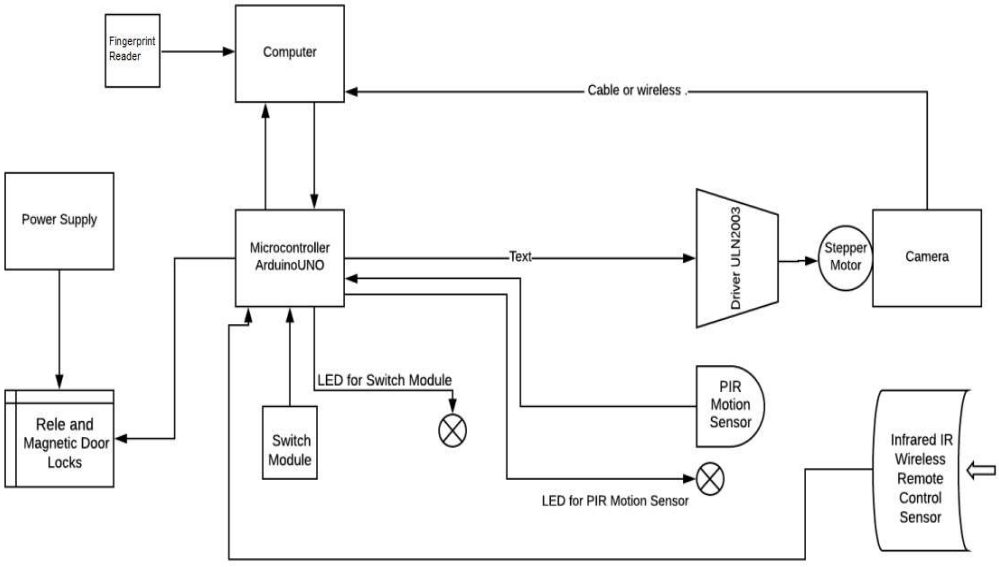

Fig 1. Schematics of the security system for the door

In Figure 2 we have shown in detail the main schematics for the security system that we are presenting, where we have not included the computer and its communication with the microcontroller and camera.

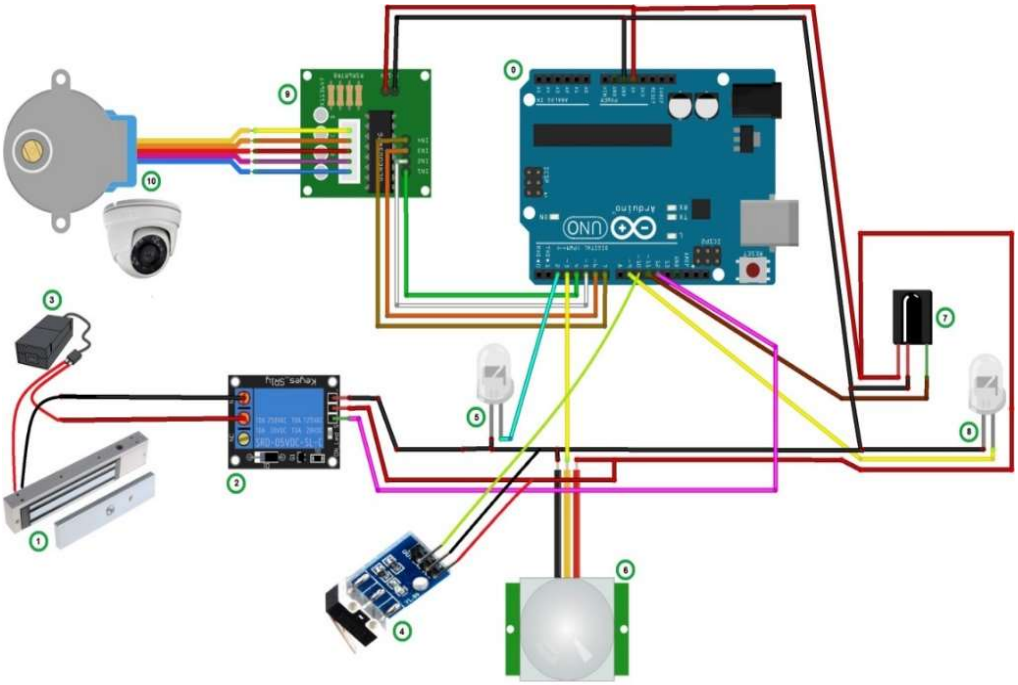

Fig 2. Detailed schematics of the security system for the door

2. ELEMENTS OF THE SECURITY SYSTEM FOR THE DOOR

The elements mentioned above are presented in detail below. In Figure 3, we have shown the DC 5V Stepper Motor 28BYJ-48 + ULN2003 Driver. Some of the parameters of the Stepper Motor 28BYJ-48 are as follows:

- Rated voltage : 5VDC
- Number of Phase 4
- Speed Variation Ratio 1/64
- Stride Angle 5.625° /64
- Frequency 100Hz
- DC resistance 50Ω±7%(25℃)
- Idle In-traction Frequency > 600Hz

- Idle Out-traction Frequency > 1000Hz
- In-traction Torque >34.3mN.m(120Hz)
- Self-positioning Torque >34.3mN.m
- Friction torque 600-1200 gf.cm
- Pull in torque 300 gf.cm
- Insulation grade A

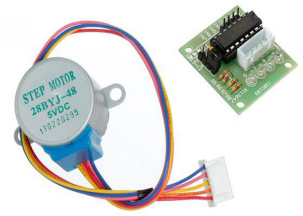

Fig 3. The stepper motor and its module

The stepper motor has a camera mounted on its axis, which is connected through a cable or through wireless with the computer. The motor is used to move the camera 360^0, from which we gather information in forms of video and audio. The control of the motor is done manually from the service staff.
In Figure 4 we have the magnetic key used to block the door. The key blocks the door when there is voltage from the power supply, a process that happens after the rele, given in Figure 5, takes the signal for the blocking of the door from the Arduino Uno microcontroller [8].

The parameters for 280KG Electro Magnetic Door Lock- Holding Force NC for Access Control are:

- 280KG/600lbs magnetic lock for door access control system
- Secure NC mode: unlocked when power off, locked when power on
- Power supply: DC12V holding force: 280KG/600lbs

- High quality and durable in performance
- Suitable for: wooden door, glass door, metal door, fire-proof door

Fig 4. Magnetic key to block the door

Fig 5.Rele used to command the magnetic key

In Figure 6 we have shown the package of the key known as YL-99 Collision Switch Module. It has three pins *Vcc*, *Gnd* and *Out.* The *Vcc* pin is connected to +5V, *Gnd* is conected to the ground of the system and *Out* is connected to a port in the microcontroller. When the switch is open (the door is open) in the *Out* pin we have voltage of 0V and when the switch is closed (the door is closed), we have a voltage of +5V. These values are given to the input port in the microcontroller and doing so it helps us to know the state of the door, open or closed.

Fig 6. The key module with the 'Output' state

In Figure 7, is given the power supply which is used in order to supply with current the magnetic key which normally needs high currents. The powerful magnetic field which is created around the magnetic field can be obtained from high currents. In order to test this system in a laboratory, I have used a power supply from a computer.

Fig 7. Power supply of a DC voltage 12V, 25A

In Figure 8 it is shown a motion sensor with infrared. This sensor is known as PIR Motion Sensor ("Passive Infrared", "Pyroelectric", or "IR motion" sensor). Any body that has a temperature above 0, emits infrared electromagnetic waves. The PIR Motion Sensor detects movements as a result of a process which is connected to the level change of the infrared electromagnetic waves that hit the pyroelectric crystals inside the sensor. The sensor is divided in two parts in order to detect the difference of the infrared waves level and not the flux.

Fig 8. PIR Motion Sensor

In Figure 9 it is shown an Infrared IR Wireless Remote Control Sensor Module, made of two parts:

- Infrared sender
- Infrared receiver

The infrared sender looks like a standard LED, with the difference that it emits electromagnetic waves in the IR spectrum instead of the visible spectrum. The infrared sender generates a modulated IR signal with a frequency of 38 kHz. A device inside the sender called Encoder generates, based on a binary code, a modulated voltage given to the LED diode.
The infrared receiver is a module with photodiodes which identifies the IR emission in the 38 kHz frequency, helped by a system of electrical filters, and converts the voltage.

Fig 9. HX1838 VS1838 NEC Infrared IR Wireless Remote Control Sensor Module

In Figure 10, we have shown the fingerprint reader which can be used after it is connected to the computer. After the device is connected physically with the computer through the USB port and after the installing of the drivers, using the U.are.U SDK DigitalPersona [6] library in the Microsoft Visual Basic 6 [7] programming language, we were able to realize the gathering of the data for the fingerprints.

Fig 10. U.are.U 4500 USB Fingerprint Reader

TESTING OF SECURITY SYSTEM FOR THE DOORS.

The application built in the microcontroller is almost independet, meaning that it can work without the computer once that the system has been initialized. The initialization of the system is connected to the work of:

- Power supply for the magnetic key
- microcontroller
- computer
- the start of the computer program

After the initialization the computer program, Figure 11, the command 'Connect' is given, which is executed after the button with the same name is clicked (the communication can be stopped using the same button which now is called 'Disconnect').After the connection between the two devices, the computer and the microcntroller, has ben confirmed, we go on to the next step of the final initialization of the work. This step requires a starting code which is different for each individual of the staff. The input of this code can be done in two different ways:

a) through the computer
b) through the modules' keyboard of the *Infrared IR Wireless Remote Control Sensor*

Later, after the code has been verified, the microcontroller activates the magnetic key to close the door: at this moment the door should be closed or should close if it was open.The application in the mirocontroller notifies the computer application showing the state of work. The computer application initializes the camera and starts it.

When a person is approaching the secured door, the module *PIR sensor* detects the movement, and the microcontroller that gathers this information sends it to the computer application. This one activates the camera placed at the top of the door, and takes a number of pictures that is set before. The person sets their finger on the fingerprint reader module, which in our case is the *U.are.U 4500 USB Fingerprint Reader*.

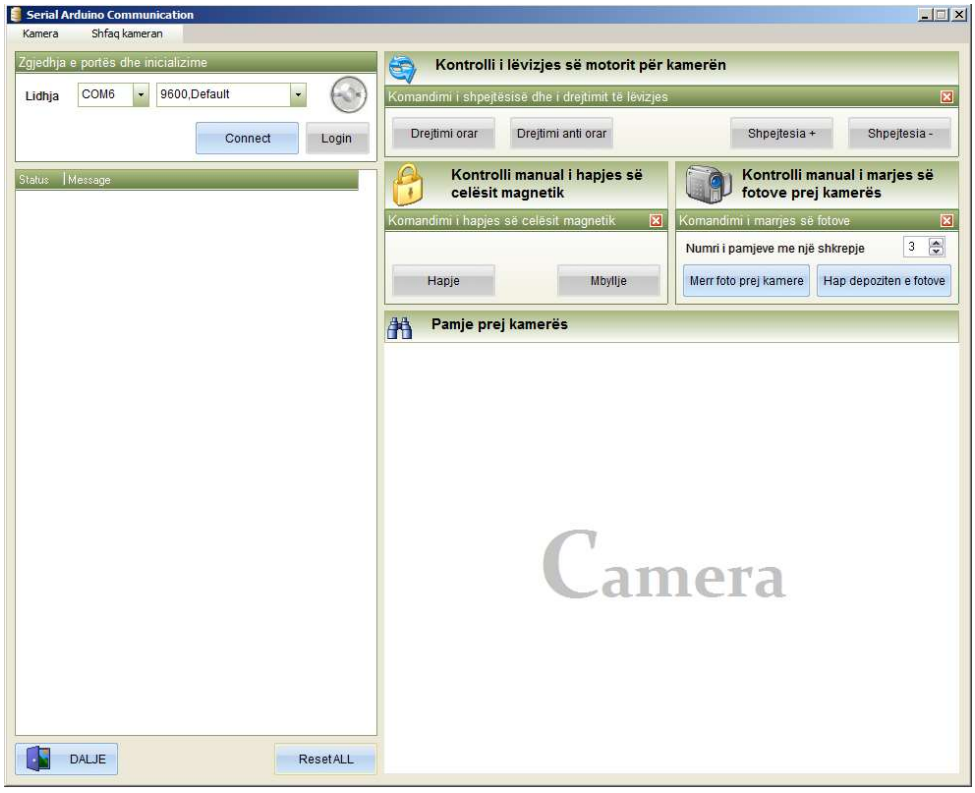

Fig 11. *Picture: The robot in pursuit of the moving object*

The gathered information goes to the computer application where the existence of the fingerprint is verified, with respect to the list of the data from the people authorized to pass (this list of data is updated with information from the office of registration of the staff), Figure 12. The fingerprint reader can alsobe connected to the Arduino Uno microcontroller [8];in this case the information goes to the microcontroller and then towards the computer where the existence of the fingerprint is verified. After the verification with the list of the authorized people, the computer application gives directions for the deactivization of the magnetic key (this command is taken by the microcontroller which unlocks the electrical rele which holds the electrical circuit of the magnetic key closed). After the magnetic key is deactivated, the person can go through. The YL-99 key, that is connected on the door, as shown in Figure 6, notifies the microcontroller about the state of the door (in this case it is open as the switch is open) as well as a LEDlight which signals for the same reason (when the door is open, the LED will light up). As long as the door will be open, the system will be on stand-by. Once the door is closed, the YL-99 key notifies the microcontroller that the door is now closed (the switch is closed) as well as the turned off LED. After this moment the system switches from stand by, and it is now ready to work and waiting for another person to pass by.

Fig 12. *Testing of the security system of the door*

In the computer application it can be made possible the orientation of the camera manually through the command of the stepper motor which are transmitted using the microcontroller. The buttons are shown in Figure 13.

Fig 13. *Manual control of the position of the camera*

In the computer application it is made possible the manual command of themagnetic key for the opening of the door for VIP-sor in any cases of malfunction, commands that are passed through the help of the microcontroller. The buttons are shown in figure 14.

Fig 14.*Manual command of the magnetic key from the computer*

In Figure15 it is shown how the images are obtained manually and how to open the folder where the previous images are stored.

Fig 15.*Manually obtaining pictures*

In Figure 16 it is presented an image of the security system for the door, without the computer.

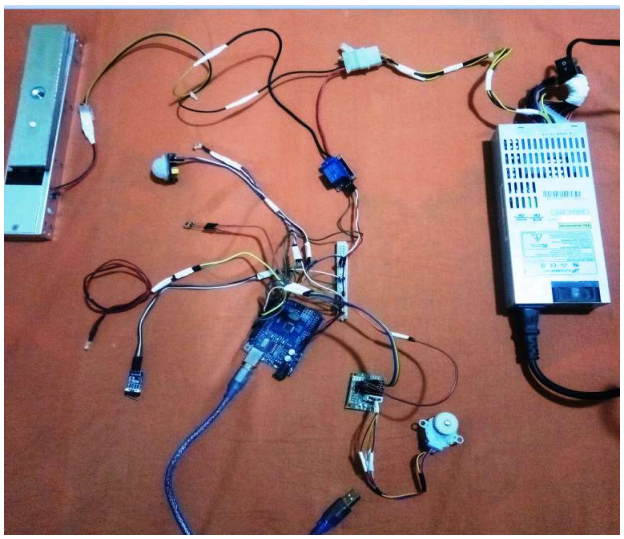

Fig 16. *The security system*

Conclusions

- Through this article it is shown how we can practically build a security system on a door.
- The schematics show how different modules are connected in one and the way that this one system can function without any problems gives us further reassurance that we can implement such a system widely.
- The results that we obtained from this experiment are fundamental in building a more advanced system.

Literatura

[1] Samuel, D. (2008). RFID security in door locks. Master thesis performed in information coding at Linköping Institute of Technology.
[2] Introduction to Computer Security (Matt Bishop)
[3] Network Security- Private Communication in a public world (Charlie Kaufman, Radia Perlman, Mike Spenicer)
[4] Hawrra, H.A. & Al-Rubiae (2007). Design and Implementation of Computerized Control Room. Journal of Karbala University, 5(2).
[5] Axelson, J. (2000). Parallel Port Complete.Programming, Interfacing, & Using the PC's Parallel Printer Port. Published by Lakeview Research
[6] https://www.crossmatch.com/wp-content/uploads/2017/03/UareU-SDK-2-2DeveloperGuide20121128.pdf - 14.10.2018
[7] Microsoft Visual Basic 6
[8] https://www.arduino.cc/en/Main/Tutorials - 14.10.2018