Universitatea POLITEHNICA din București
Facultatea de Automatică și Calculatoare
Secția Ingineria Sistemelor
Anul 2021-2022
Semestrul II

Sistem interfon „smart-home”

Student: Postelnicu Andrei-Cosmin

Cuprins

1.Introducere

1.1 Obiectivele proiectului

Principalul obiectiv al proiectului este axat in jurul conceptului de securitate automatizata care are rolul de a proteja clientul non-stop. Acest sistem dispune de o interfață inteligibilă și care este ușor de folosit de către oricine. Acest concept prezintă ideea controlării sistemului de acces in incintă prin intermediul unor senzori capabili să diferențieze persoanele autorizate de persoanele neautorizate.

La un nivel foarte de bază, controlul accesului este un mijloc de a controla cine intră într-o locație și când. Persoana care intră poate fi un angajat, un antreprenor sau un vizitator și poate fi pe jos, conducând un vehicul sau folosind un alt mod de transport. Locația în care intră poate fi, de exemplu, un site, o clădire, o cameră sau un dulap.

Tindem să-l numim control fizic al accesului pentru a-l diferenția de controlul accesului care împiedică oamenii să intre în spații virtuale - de exemplu atunci când se conectează la o rețea de calculatoare. Și, deși una dintre utilizările sale principale este creșterea securității, un sistem de control al accesului fizic poate oferi și multe alte beneficii. Inclusiv eficiența îmbunătățită a proceselor dvs. de afaceri și a gestionării site-ului sau a clădirilor.

Referindu-ne la sistemul de control al accesului fizic, de obicei ne referim la un sistem electronic de securitate. De obicei, utilizează un identificator, cum ar fi un card de acces, pentru a autoriza oamenii să intre în anumite zone. Și, deoarece sunt capabili să înregistreze cine a accesat unde și când, pot furniza date valoroase pentru a vă ajuta să urmăriți modul în care sunt utilizate clădirile și site-urile dvs.

Acest tip de sistem vine in ajutorul utilizatorului cu următoarele avantaje (raportandu-ne la un sistem de securitate al cărui acces se face prin intermediul unei simple chei): cine are acces (de exemplu permiterea automata a accesului angajaților , întrucât dorim ca vizitatorii și contractanții să se prezinte in prealabil la un punct prestabilit, la recepție), așadar putem reduce din start costurile unui salariu in plus, accesul pe grade (o parte dintre persoane au accesul limitat in unele zone, de exemplu tehnicienii vor avea autorizație doar in camera de control), programarea intervalului de acces (de exemplu contractanților și personalului junior li se poate permite accesul numai în timpul programului de lucru, în timp ce personalul superior poate intra în clădire oricând).

Performanta sistemului este evidențiată prin controlul accesului care permite setarea parametrilor pentru fiecare persoană astfel putem actualiza rapid și ușor ori de câte ori este necesar. De asemenea, in cazul situațiilor neplăcute, identificarea cauzelor acestora poate fi realizata mai rapid prin verificarea istoricului accesărilor.

2.Descrierea domeniului ales & soluții similare

Domeniul ales este cel al securității inteligente („smart-home”) care este prezent la majoritatea clădirilor moderne din ziua de astăzi. După cum putem observa din titlu cuvântul „smart” se refera la capacitatea sistemului de a lua decizii singur, capacitate de baza in dezvoltarea proiectelor „de viitor”. Acest interfon presupune automatizarea unor procese prin intermediul plăcii de dezvoltare ARDUINO si a componentelor aferente.

Domeniul ales, „smart-home” nu implica neapărat termenul de securitate ci poate implica si tipul sistemului, acesta fiind automatizat, putând sa înregistreze cine intra, unde intra si la ce ora cat si capacitatea acestuia de a lua decizii singur in funcție de situație.

Ca soluție similara, am avut in vederea un produs deja existenta pe piață, si anume, produsul „**Post exterior Safer cu control acces, Negru, D23CCM04”** care oferă aproximativ aceleași facilitati pe care le oferă si sistemul propus de noi. Soluțiile similare nu diferă foarte mult de ceea ce am realizat noi, acestea având o opțiune sau doua in plus.

In continuare vom analiza succint caracteristicile sistemului nostru si caracteristicile sistemului similar, omologat.

Caracteristici	**Sistemul „smart-home”**	**Sistemul „D23CCM04”**
Avertizare sonora	Buzzer Activ de 5V	-
Led Confirmare/Infirmare	Existent	Existent
Camera video	Inexistent	Existent
Rezistent la apa	-	Rezistent la apa
Număr tag-uri suportate	200 tag-uri	150 tag-uri
Panoul de control	-	Comenzi pe tableta

3.Descrierea soluției

Pentru descrierea soluției prezentate vom descrie întâi lista componentelor utilizate si funcționalitatea acestora. După cum putem observa si in schema operațională componentele utilizate sunt:

- Arduino UNO R3 - placa pentru dezvoltarea circuitului, componenta prin intermediul căreia se conectează efectiv toate celelalte componente;
- Modul RFID RC522 - utilizat pentru citirea datelor de pe tag-uri cu ajutorul circuitului integrat RC522;
- Micro Servomotor SG90 90° - proiectat special pentru aplicații de mică putere, controlul servomotorului se realiză cu ajutorul unu semnal de tip PWM;
- LCD 2004 cu Backlight Albastru - componenta cu ajutorul căreia printam mesajul aferent răspunsului sistemului la citirea cartelei;
- Adaptor I2C pentru LCD 1602 - componenta care este conectata la LCD si care convertește semnalul acestuia in cod ASCII si poate regla contrastul si iluminarea de fundal prin intermediul celor doua fire;
- Buzzer Activ de 5V - conectat la pinii I / O digitali standard ai microcontrolerului, acesta produce un sunet puternic;
- 2 buc Rezistoare 220Ω - producerea căderii de tensiunii dorite între două puncte din circuit si implicit reglarea curentului printr-o alta componenta din circuit;
- LED Verde de 3 mm cu Lentile Difuze - componenta care indica validarea tag-ului;
- LED Roșu de 3 mm cu Lentile Difuze - componenta care indica infirmarea tag-ului;
- Breadboard HQ (400 Points) - placa de baza care asigura conexiunile componentelor;
- Mini Breadboard - componenta cu ajutorul căreia am multiplicat intrările plăcii arduino;
- Fire Tată-Tată – asigura funcționalitatea legăturilor intre componente;
- Fire Tată-Mamă - asigura funcționalitatea legăturilor intre componente;

4.Prezentarea funcționalităților

In cadrul proiectului ales sistemul nostru smart-home beneficiază de o securitate aparte, si anume, pentru testarea funcționalității acestuia am ales inițial doua access-key-uri, una pe care este stocat id-ul care v-a garanta accesul in incinta si cealaltă care nu va conține id-ul potrivit si care va fi respinsa in momentul scanării.

Sistemul inițial poate stocat in memoria lui unul sau mai multe id-uri „deja cunoscute" care exista si fizic stocat pe cartele. Deși sistemul permite mai multe id-uri stocate, pentru început am ales sa testam sistemul doar cu doua cartele „cea potrivita" si „cea greșită".

Suprafața destinată acestor cartele, este alimentată continuu si așteaptă sa recunoască cartelele pentru a garanta accesul. In consecință, vom avea doua cazuri de testat pentru sistemul nostru: primul caz – cazul cartelei potrivite, care deschide ușa si al doilea caz, cazul cartelei nepotrivite care nu permite accesul in incinta.

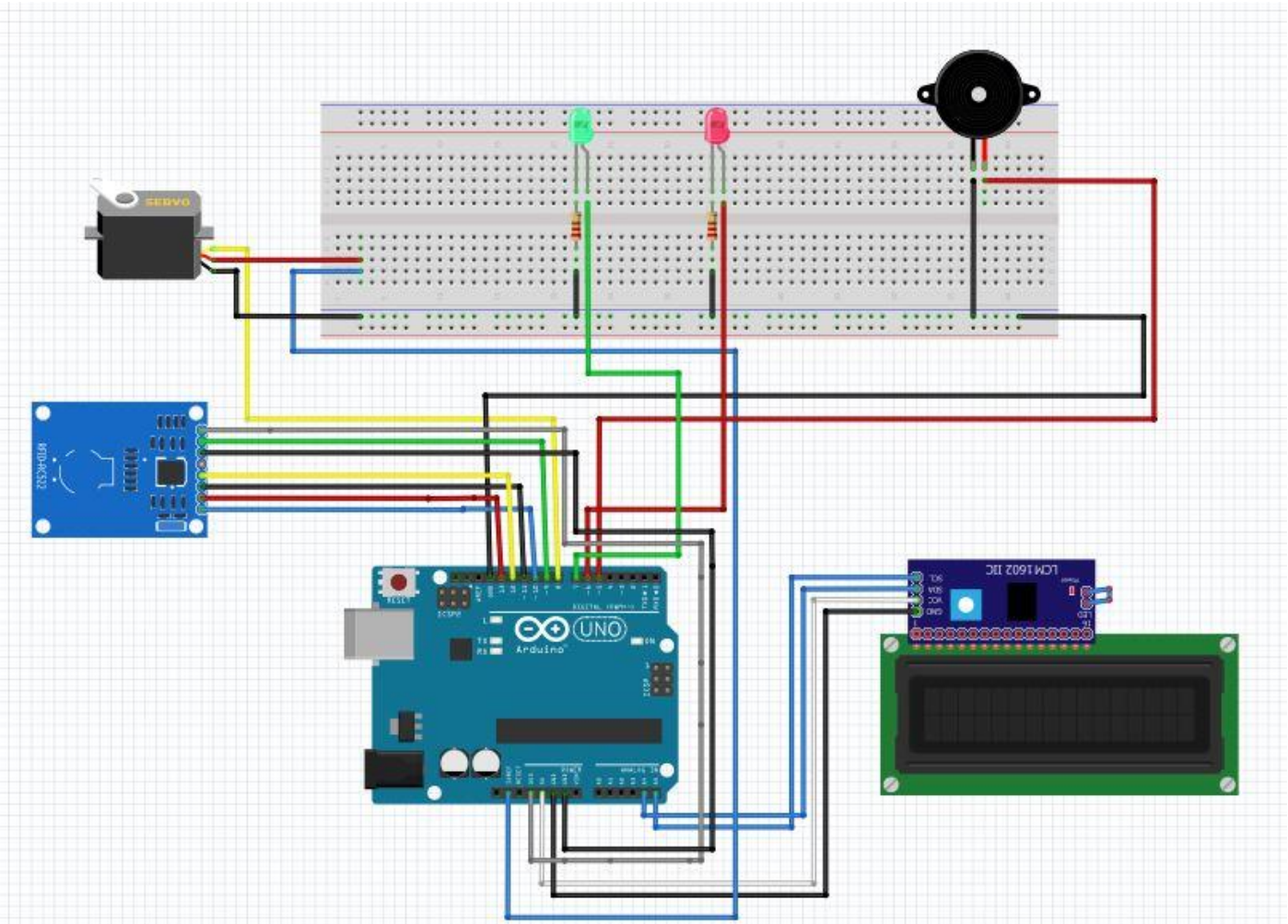
Pentru primul caz, cel al cartelei potrivite, in momentul aproprierii acesteia de suprafața destinata scanării, sistemul va recunoaște id-ul stocat pe aceasta si îl va găsii drept cel corect pe care îl are si el deja stocat in memoria lui, așadar sistemul va răspunde la acesta comanda prin: aprinderea led-ului verde, atenționarea sonora, ecranul va afișa „accesul permis" iar motorașul va deschide efectiv ușa.

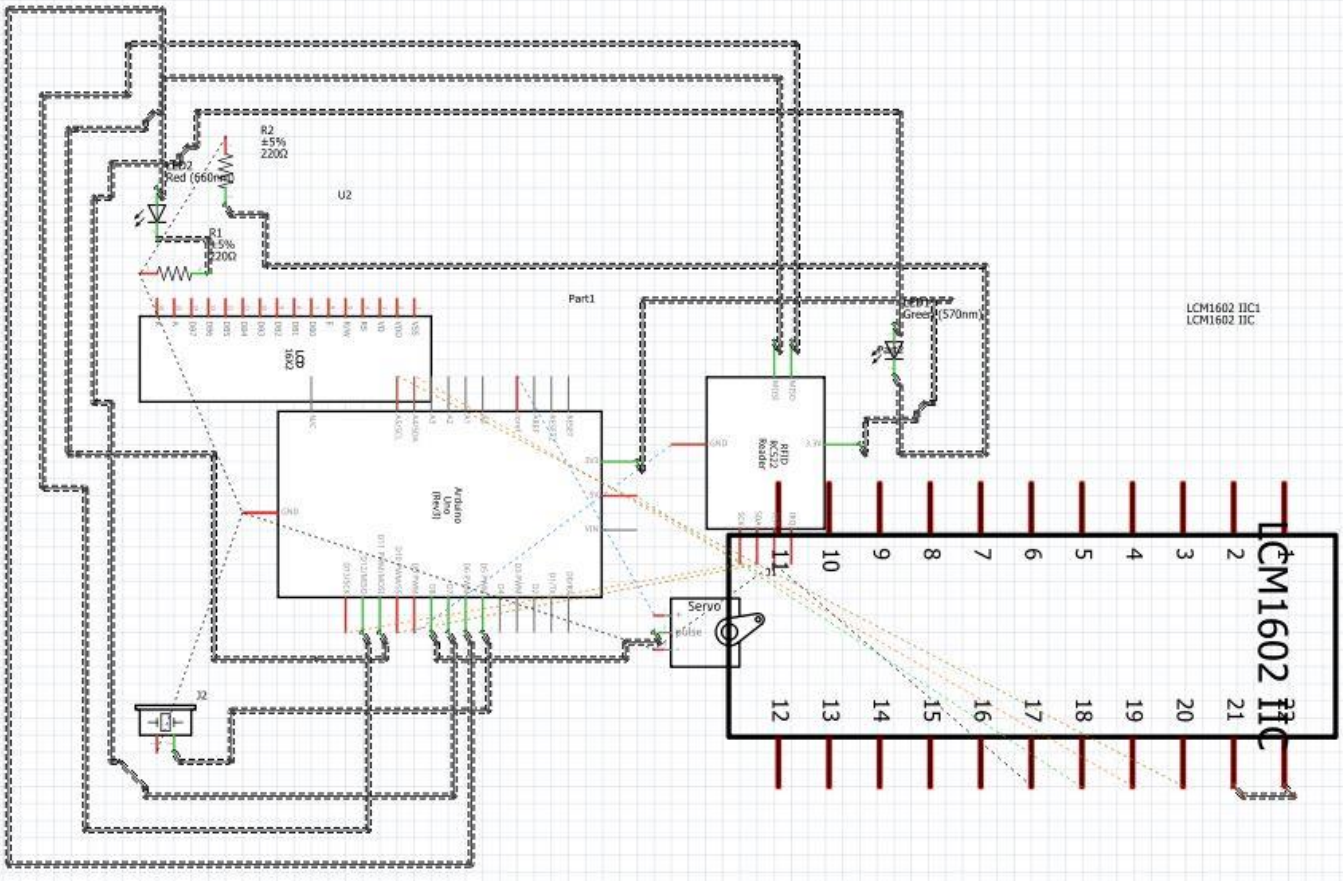
In cel de al doilea caz, in care id-ul stocat pe cartela nu va fi înregistrat si in memoria sistemului, acesta nu va răspunde întocmai comenzii si va reacționa astfel: se va aprinde led-ul roșu iar pe ecran va fi afișat „acces nepermis" iar componenta mecanica nu va reacționa in niciun mod, astfel persoana care nu este autorizata nu va putea intra in incinta.

Pentru recunoașterea mai multor cartele este necesar adăugării fiecărui id al acestora in codul aferent sistemului. De asemenea este de precizat faptul ca sistemul funcționează pe frecventa 13.56 Mhz. In consecință, cartele pe care stocam id-ul vor funcționa pe aceeași frecventa (de ex: cartela pe frecventa 125 khz nu poate fi folosita pe acest sistem). Tot un aspect important in cadrul prezentării funcționalităților este tensiunea de operare a sistemului care are valoarea de 5V.

Senzorul principal al sistemului, cel prin care reușim sa facem colectarea datelor este de tipul RFID (Radio-Frequency Identification) .Este o metodă de identificare automată care se bazează pe stocarea și regăsirea datelor fără atingere, la distanță, prin unde radio, folosind dispozitive numite etichete RFID (cartelele pe care stocam datele) și transpondere RFID.

5.Schemă operațională





6.Contribuție

Membru	Contribuție	Timp
Postelnicu Andrei-Cosmin	Hardware, Software, Documentatie	11h

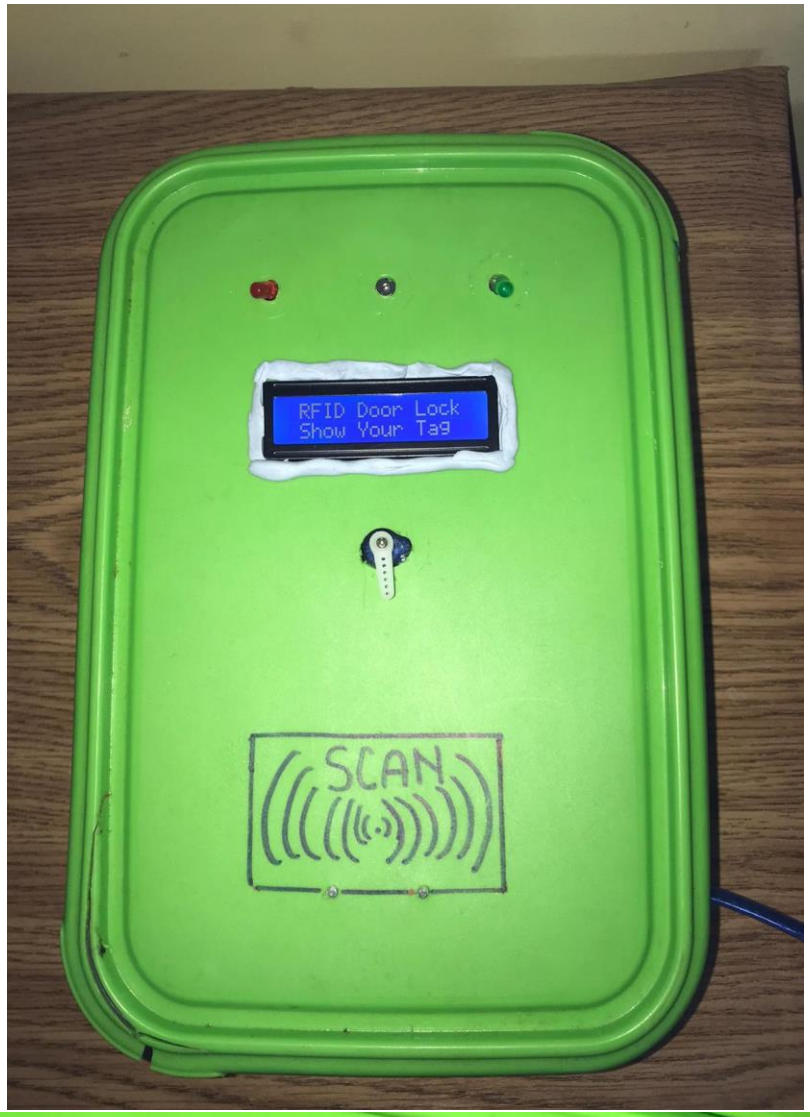
7.Circuit – partea hardware

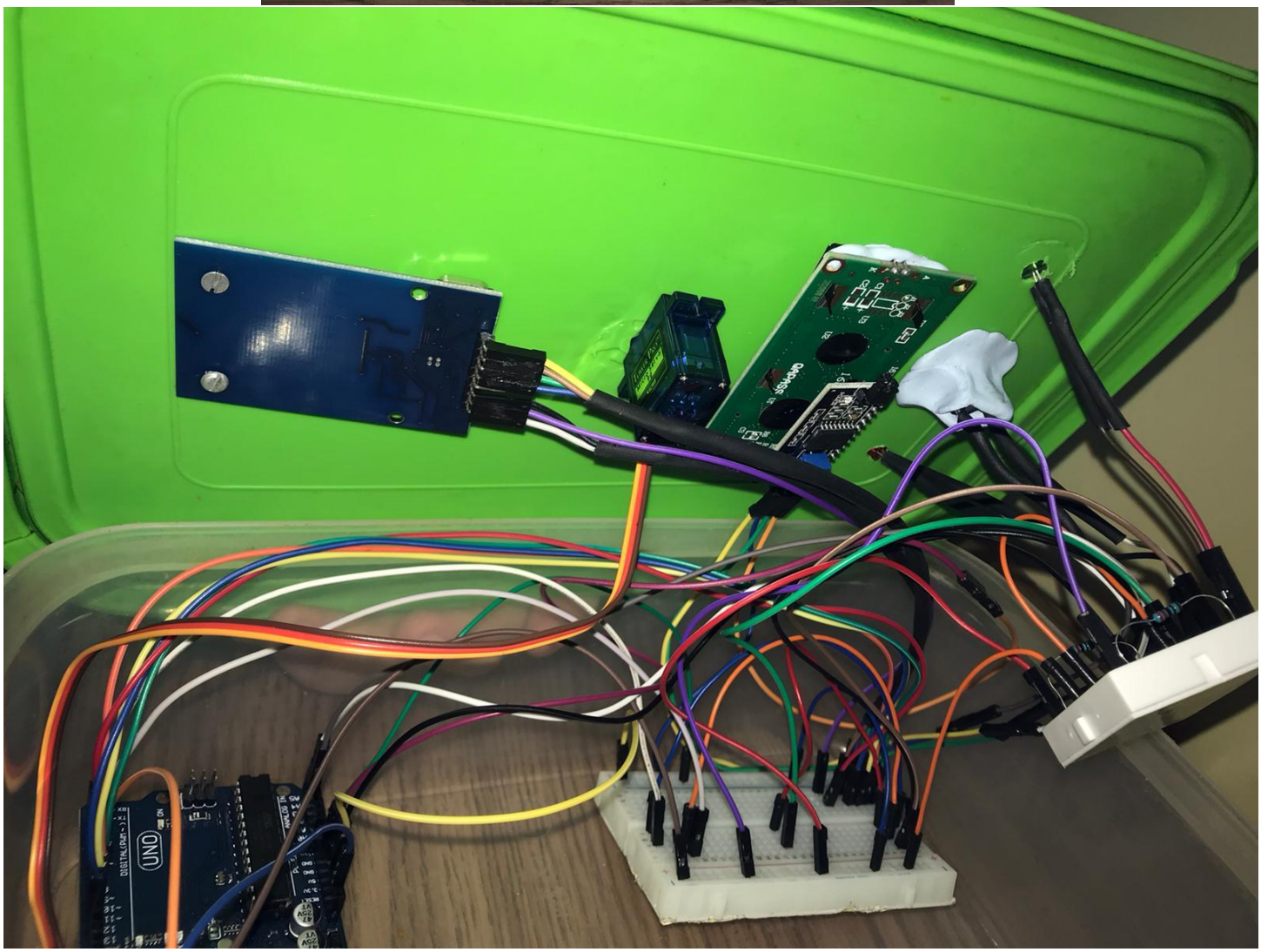
In următoarele poze este prezentata varianta finala a circuitului, produsul final, căruia ii mai trebuiesc câteva mici îmbunătățiri ale design-ului dar care, din punct de vedere mecanic este perfect funcțional.

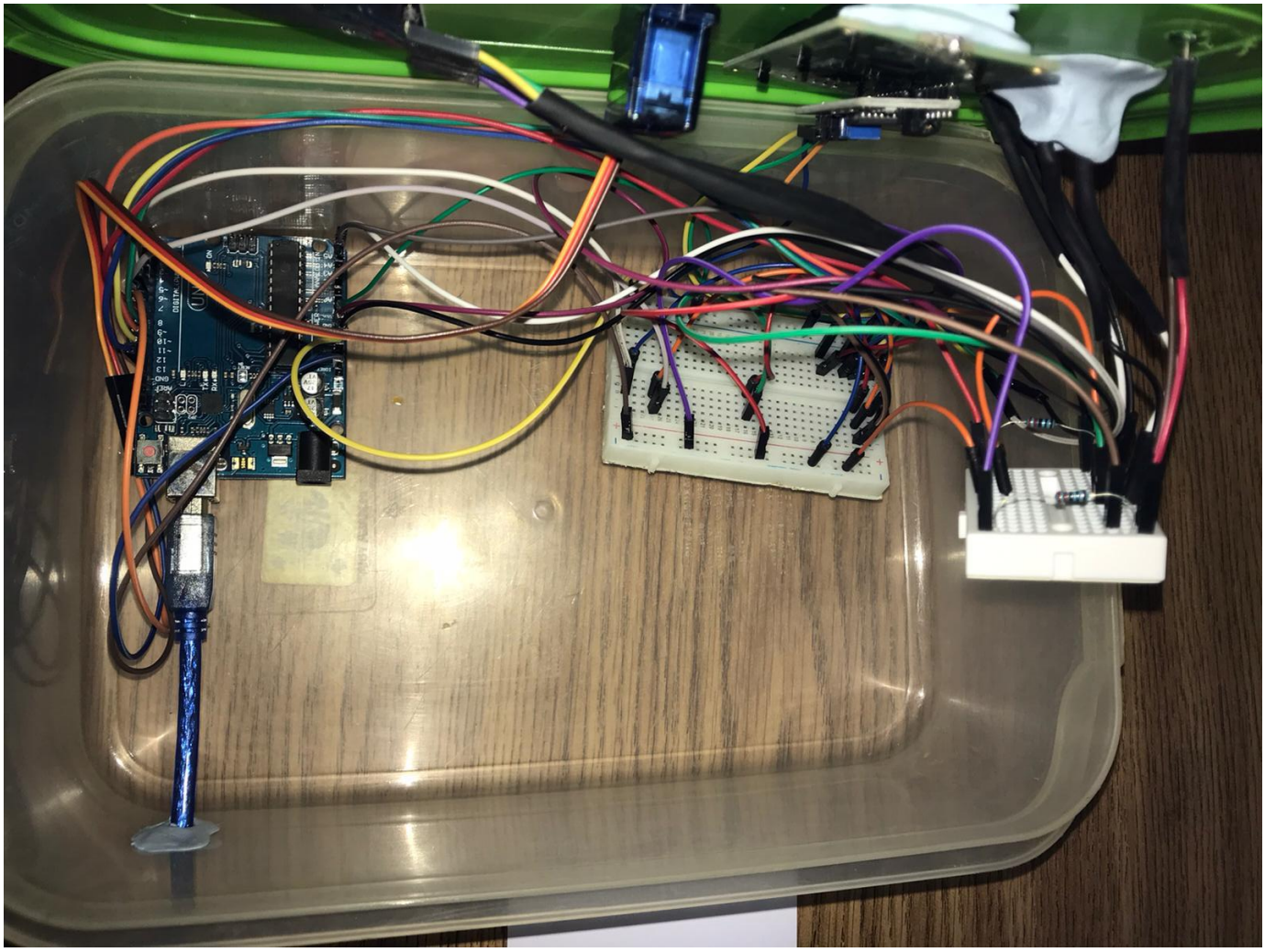
In prima poza este prezentata interfața, partea frontala a circuitului cu care utilizatorul interacționează cel mai mult. Aceasta are un design compact cu următoarele caracteristici:

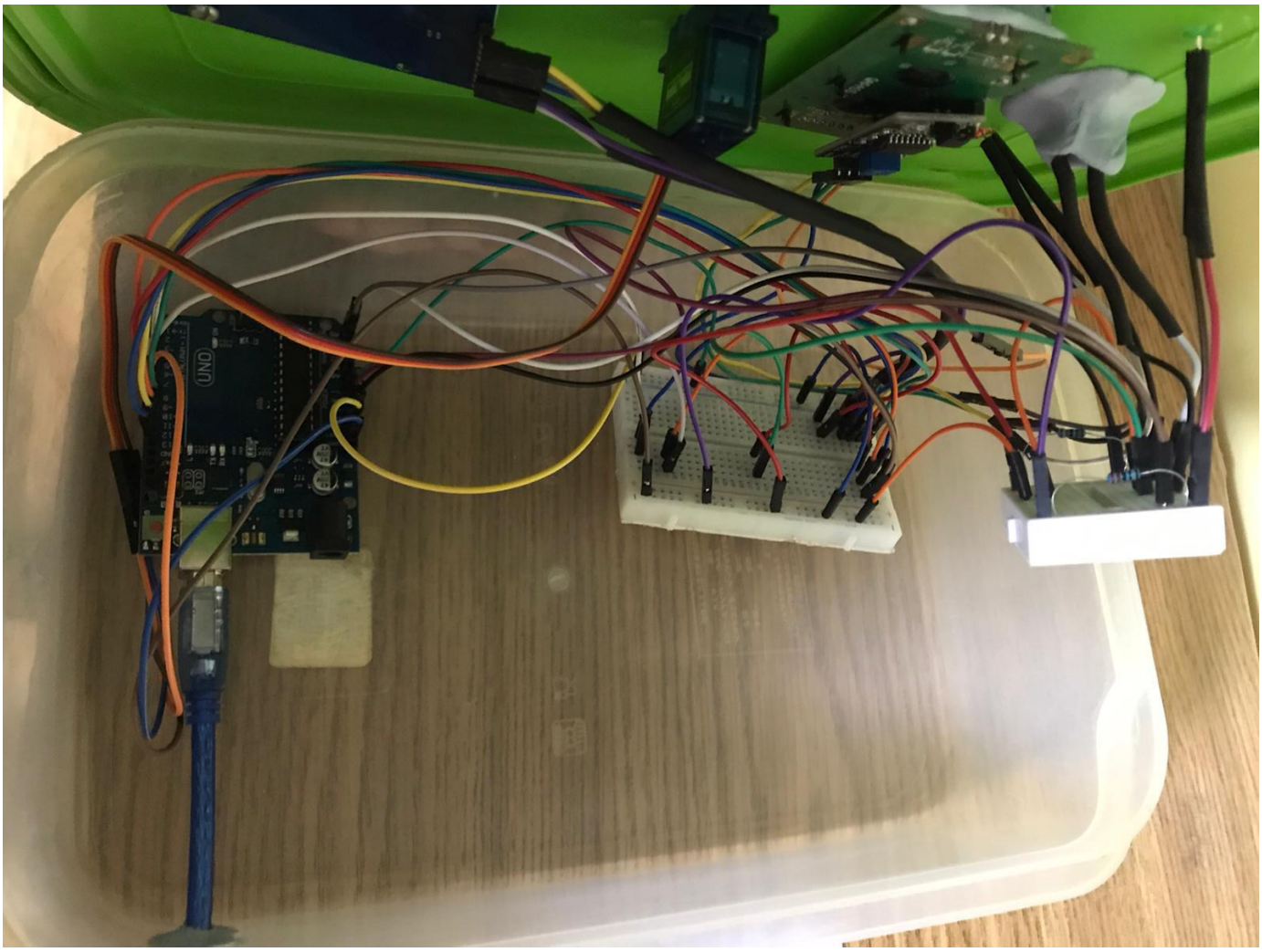
- Lungimea este de aproximativ 30cm.
- Lățimea are valoarea de 19cm.
- Înălțimea cu valoarea de 9cm.

In continuarea capitolului este prezentata legătura dintre componentele acestuia (firele care duc la breadboard,etc) si amplasarea modulelor.


RFID Door Lock
Show Your Tag
SCAN


UNO




UNO

8.Circuit – partea software

```
//Include required libraries
#include <LiquidCrystal_I2C.h>
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>

//Create instances
LiquidCrystal_I2C lcd(0x27, 16, 2);
MFRC522 mfrc522(10, 9); // MFRC522 mfrc522(SS_PIN, RST_PIN)
Servo sg90;

//Connected pins
unsigned long UID[3];
unsigned long UID1;
constexpr uint8_t greenLed = 7;
constexpr uint8_t redLed = 6;
constexpr uint8_t servoPin = 8;
constexpr uint8_t buzzerPin = 7;
String tagUID = "DB E2 B6 22";  // String to store UID of tag. Change it with your tag's UID

void setup() {
  //Arduino Pin configuration
  pinMode(buzzerPin, OUTPUT);
  pinMode(redLed, OUTPUT);
```

```
  pinMode(greenLed, OUTPUT);

  sg90.attach(servoPin);  //Declare pin 9 for servo
  sg90.write(0); // Set initial position at 90 degrees

  lcd.begin();// LCD screen
  lcd.backlight();

  Serial.begin(9600);
  SPI.begin();      // Init SPI bus
  mfrc522.PCD_Init();   // Init MFRC522

  lcd.clear();
}

void loop() {

    lcd.setCursor(0, 0);
    lcd.print(" RFID Door Lock");
    lcd.setCursor(0, 1);
    lcd.print(" Show Your Tag ");


  // Look for new cards
  if ( ! mfrc522.PICC_IsNewCardPresent()) {
    return;
  }
```

```
  // Select one of the cards
  if ( ! mfrc522.PICC_ReadCardSerial()) {
    return;
  }

  //Reading from the card
  String tag = "";
  for (byte i = 0; i < mfrc522.uid.size; i++)
  {
    tag.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
    tag.concat(String(mfrc522.uid.uidByte[i], HEX));
  }
  tag.toUpperCase();

  //Checking the card
  if (tag.substring(1) == tagUID) //change here the UID of the card/cards that
you want to give access
  {
    // If UID of tag is matched.
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Access Granted");
    lcd.setCursor(0, 1);
    lcd.print("Door Opened");
    sg90.write(90);
    digitalWrite(greenLed, HIGH);
    delay(1000);
```

```
    digitalWrite(greenLed, LOW);
    sg90.write(0);
    lcd.clear();
  }
  else
  {
    // If UID of tag is not matched.
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Wrong Tag Shown");
    lcd.setCursor(0, 1);
    lcd.print("Access Denied");
    digitalWrite(redLed, HIGH);
    delay(1000);
    digitalWrite(redLed, LOW);
    lcd.clear();
  }

  Serial.println("Your CardTagId is: ");
  for (int i = 0; i < 4; i++) {
    UID[i] = mfrc522.uid.uidByte[i];
    Serial.print(UID[i], HEX);
  }
  Serial.println("\n");
}
```

Partea software a fost realizata cu ajutorul programului Arduino cu care putem testa in funcție de placa de baza diferite funcționalități atat ale componentelor cat si a circuitului.

Mai exact, după terminarea partii hardware, a fost conectat arduino uno r3 (la care sunt conectate toate celelalte componente) la calculator iar prin intermediul programului am reușit sa „invatam” circuitul sa funcționeze dupa anumite instructiuni.

După selectarea in program a plăcii de baza aferente (Ard.Uno.R3), am verificat sintaxa codului si am testat bucăți mici de cod pentru fiecare componenta in parte (ex. am aprins led-ul verde, am pus in mișcare motorul cu servo) iar la final am adunat toate aceste mici bucatele (cu mici modificări) intr-un cod final.

Următorul pas pe care l-am urmat a fost sa compilam codul si sa verificam in integritate daca exista vreo eroare/warning sau orice altceva ce ar putea deturna funcționalitatea de baza a circuitului.

Ultimul pas este reprezentat de uploadarea codului in memoria circuitului, pentru ca acesta sa urmeze instrucțiunile date de fiecare data când acesta este conectat la o sursa de alimentare.

9.Testarea soluției

TESTARE - LIVE

TESTARE – LINK VIDEO