

UNIVERSITATEA TEHNICĂ „Gheorghe Asachi” din IAȘI
FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE
DOMENIUL: Calculatoare și Tehnologia Informației
SPECIALIZAREA: Calculatoare

LUCRARE DE DIPLOMĂ

Coordonator științific:
Ş. l. dr. Mihai Timiș

Absolvent:
Roberta-Georgiana Popa

Iași, 2023

UNIVERSITATEA TEHNICĂ „Gheorghe Asachi” din IASI
FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE
DOMENIUL: Calculatoare și Tehnologia Informației
SPECIALIZAREA: Calculatoare

Sistem de control al accesului securizat cu autentificare multiplă

LUCRARE DE DIPLOMĂ

Coordonator științific:
Ş. l. dr. Mihai Timiș

Absolvent:
Roberta-Georgiana Popa

Iași, 2023

DECLARAȚIE DE ASUMARE A AUTENTICITĂȚII PROIECTULUI DE DIPLOMĂ

Subsemnatul POPA ROBERTA-GEORGIANA,
legitimat cu CI seria MZ nr. 734502, CNP 6000923226761
autorul lucrării "SISTEM DE CONTROL AL ACCESULUI SECURIZAT CU AUTENTIFICARE
MULTIPLĂ"

elaborată în vederea susținerii examenului de finalizare a studiilor de licență, programul de studii CALCULATOARE ȘI TEHNOLOGIA INFORMATIEI organizat de către Facultatea de Automatică și Calculatoare din cadrul Universității Tehnice „Gheorghe Asachi” din Iași, sesiunea SEPTEMBRIE a anului universitar 2022-2023, luând în considerare conținutul Art. 34 din Codul de etică universitară al Universității Tehnice „Gheorghe Asachi” din Iași (Manualul Procedurilor, UTI.POM.02 - Funcționarea Comisiei de etică universitară), declar pe proprie răspundere, că această lucrare este rezultatul propriei activități intelectuale, nu conține porțiuni plagiate, iar sursele bibliografice au fost folosite cu respectarea legislației române (legea 8/1996) și a convențiilor internaționale privind drepturile de autor.

Data

06.09.2023

Semnătura



Cuprins

Introducere	1
1 Fundamentarea teoretică și documentarea bibliografică	3
1.1 Domeniul și contextul abordării temei alese	3
1.2 Analiza aplicațiilor similare	4
1.2.1 Fingerprint Door Lock	4
1.2.2 Home Security Motion Detector	5
1.3 Elaborarea specificațiilor privind caracteristicile aplicației	6
2 Proiectarea aplicației	7
2.1 Arhitectura aplicației	7
2.1.1 MicroPython	7
2.1.2 I2cLcd si MFRC522	7
2.2 Componente Hardware	8
2.2.1 Raspberry Pi Foundation	8
2.2.2 Raspberry Pi Pico W	8
2.2.3 Modul RFID RC522	11
2.2.4 Display LCD și adaptor I2C	13
2.2.5 Încuietoare electrică 12V	14
2.2.6 Modul Releu cu un singur canal	15
2.2.7 Tastatură keypad 3x4	17
2.2.8 Alte componente periferice	18
3 Implementarea aplicației	19
3.1 Configurarea microcontroller-ului	19
3.2 Conectarea componentelor	19
3.3 Implementarea componentelor	22
3.3.1 Modulul RFID RC522	22
3.3.2 Dispaly LCD și tastatura keypad 3x4	22
3.3.3 Incuietoare electrică	23
3.4 Proiectarea dispozitivului	24
3.5 Dificultăți întâmpinate și modalități de dezvoltare	25
4 Testarea aplicației și rezultate experimentale	27
4.1 Elemente de configurare ale aplicației	27
4.2 Rezultate obținute	27
4.3 Testarea generală a dispozitivului	36
Concluzii	37
Direcții viitoare de dezvoltare	38

Bibliografie	39
Anexe	41
1 Codul în MicroPython	41

Sistem de control al accesului securizat cu autentificare multiplă

Roberta-Georgiana Popa

Rezumat

În era digitală actuală, securitatea și controlul accesului reprezintă aspecte esențiale în diverse domenii, de la protejarea datelor personale până la gestionarea spațiilor restrânse. Această lucrare de licență propune dezvoltarea și implementarea unui sistem complex de control al accesului, cu accent pe securitatea sporită și autentificare multiplă. Acest sistem integrează o varietate de componente hardware și software pentru a oferi o soluție completă și eficientă. Scopul proiectului este de a controla încuietoarea electrică prin blocarea și deblocarea ei cu ajutorul a două metode de autentificare, respectiv modulul rfid și tastatura keypad. Pentru o simulare eficientă și controlată s-a folosit mediul de dezvoltare Thonny IDE împreună cu limbajul de programare MicroPython, alături de bibliotecile și librăriile necesare. La rularea programului, un ecran LCD va furniza informații utilizatorului pentru o comunicare mai interactivă. Modulul rfid folosește două etichete de tip rfid, una validă și cealaltă invalidă, pentru testare. În ceea ce privește autentificarea cu ajutorul keypad-ului, aceasta folosește un pin corect prestatibil, utilizatorul având posibilitatea a 3 încercări de deblocare a încuietorii. Prin urmare, sistemul oferă o soluție avansată pentru gestionarea și protecția accesului.

Introducere

În contextul zilelor noastre, odată cu evoluția tehnologiei, siguranța și securitatea sunt cele mai importante aspecte pe care ar trebui luate în considerare de toți utilizatorii. Există întotdeauna situații în viață în care siguranța este amenințată, iar cerințele privind sistemele de control al accesului securizat, fără erori și rentabile, sunt extrem de ridicate. Totodată, lipsa unui astfel de sistem înseamnă posibilitatea mai multor amenințări de securitate, cât și nesiguranța oamenilor și a anumitor informații. De aceea, multe industrii au apelat la sisteme monitorizate, unde doar anumite persoane pot fi autorizate pentru accesul securizat. Una dintre soluțiile pentru a asigura utilizatorului un mediu sigur de desfășurare îl reprezintă un sistem de monitorizare. Cu ajutorul său, utilizatorul poate controla accesul într-o instituție făcând-l mai sigur.

Titlul lucrării de licență se intitulează "Sistem de control al accesului securizat cu autentificare multiplă" și urmărește realizarea unui dispozitiv care să realizeze protejarea bunurilor și a informațiilor, oferind o soluție complexă și eficientă pentru gestionarea accesului în spații restrânse sau pentru protejarea datelor sensibile. În urma ideilor menționate anterior, lucrarea urmărește realizarea unui sistem cu ajutorul unui microcontroller și a unor componente hardware menite pentru un sistem de securitate, cum ar fi utilizarea unui RFID și unui KeyPad. Cu tehnologia RFID, utilizatorii pot fi identificați și verificați rapid și în siguranță, eliminând necesitatea cheilor tradiționale sau a codurilor PIN nesigure. Utilizatorilor autorizați li se oferă carduri RFID sau alte dispozitive compatibile pentru a face procesul de acces rapid și convenabil. Odată ce sistemul identifică și autentifică utilizatorul prin RFID, este permis accesul doar persoanelor autorizate. Această caracteristică oferă un nivel suplimentar de securitate și elimină riscul accesului neautorizat. Iar pentru a oferi sistemului un surplus de securitate lucrarea își propune și adăugarea unui Keypad, acest lucru permite utilizatorilor să introducă un cod PIN unic pentru a accesa zonele securizate. Această autentificare multiplă crește nivelul de securitate și reduce riscul accesului neautorizat.

Lucrarea este structurată în patru capitole, fiecare având un rol specific în prezentarea și evoluția proiectului dezvoltat. Aceste capitole oferă o privire de ansamblu asupra dezvoltării și implementării sistemului. În Capitolul 1 este expus scopul, contextul și domeniile în care se încadrează lucrarea, cât și o analiză a proiectelor similare. În Capitolul 2 sunt prezentate noțiunile teoretice esențiale prin descrierea resurselor hardware și software utilizate. În Capitolul 3 se descrie în detaliu procesul de implementare al sistemului de control. Aceasta include configurarea microcontroller-ului, conectarea componentelor, implementarea acestora, proiectarea dispozitivului, dar și dificultățile întâmpinate în procesul de dezvoltare a proiectului. În Capitolul 4 sunt descrise elementele ajutătoare de configurare ale aplicației, precum și rezultatele obținute în urma verificării sistemului.

Capitolul 1. Fundamentarea teoretică și documentarea bibliografică

1.1. Domeniul și contextul abordării temei alese

Tema aleasă pentru această lucrare se află în strânsă legătură cu domeniile securității și tehnologiei informației, deoarece se concentrează asupra controlului accesului în diferite medii. Această zonă se concentrează pe dezvoltarea și implementarea de soluții tehnice menite să asigure securitatea fizică a infrastructurii sau a datelor și să permită accesul doar utilizatorilor autorizați.

Totodată, lucrarea face posibilă încadrarea și în domeniul Embedded Systems, acesta fiind un sistem hardware bazat pe un microprocesor și software, conceput pentru a îndeplini o funcție specifică, fie ca sistem de sine stătător, fie ca parte a unui sistem mai mare. La baza sa este un circuit integrat conceput pentru a efectua calcule pentru operații în timp real. [1] Aceste sisteme sunt menite să funcționeze mult timp, procesând în mod repetat noi date de intrare și generând date de ieșire. Se amestecă în mediul înconjurător, pot afecta dinamica mediului, dar nu pot controla complet mediul. Fiecare sistem încorporat are capacitați de a percepere diferite aspecte ale stării mediului său. De asemenea, dispune de efectori care pot fi folosiți pentru a afecta starea mediului.[2]

În imaginea de mai jos (1.2) putem observa anumite sisteme incorporate pe care le găsim în viața de zi cu zi.

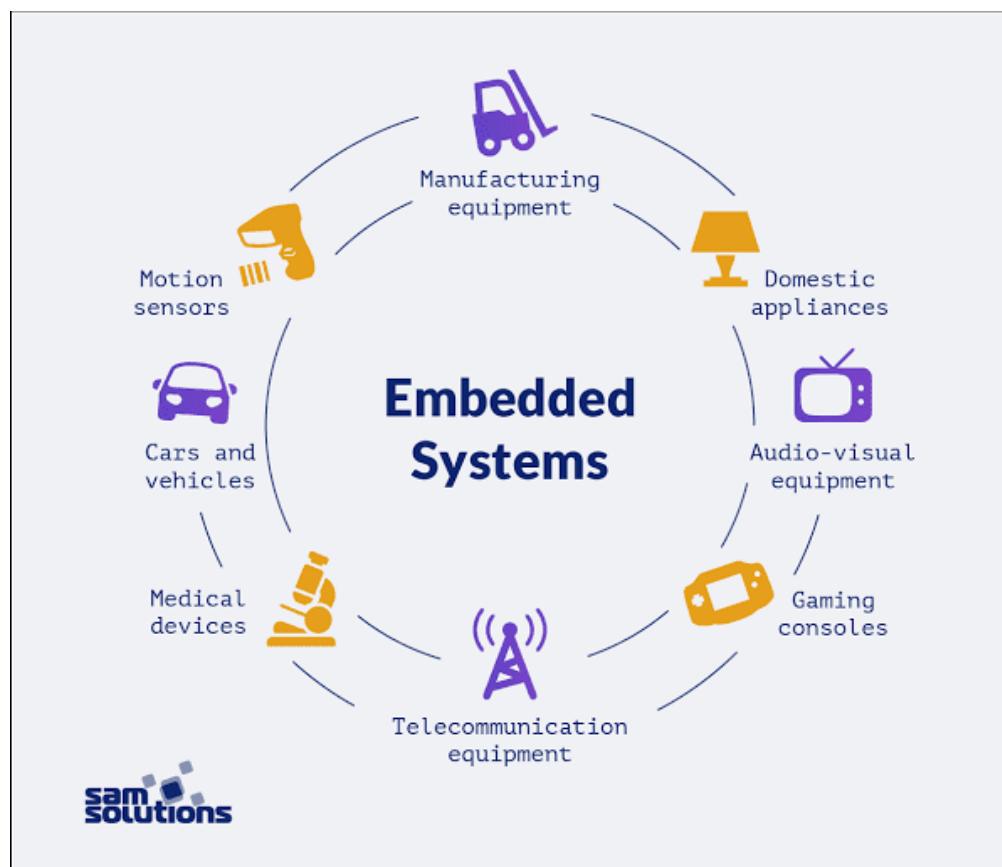


Figura 1.1. Diagrama Embedded Systems¹

Sistemele de control ale accesului au devenit o necesitate pentru a gestiona accesul la clădiri, sisteme IT și chiar case inteligente. Autentificarea multifactorială și utilizarea dispozitivelor

¹Figura a fost preluată de pe site-ul următor:<https://www.rs-online.com/designspark/what-is-an-embedded-system>

precum RFID, încuietori electrice, taste numerice și dispozitive Raspberry Pi au devenit standar-
dul pentru asigurarea unui mediu sigur și protejarea datelor. În acest context, proiectul nostru
urmărește să răspundă acestor nevoi de securitate în creștere și să ofere soluții inovatoare care pot
fi adaptate la diverse aplicații și medii.

În continuare, vom explora în detaliu aspectele tehnice, caracteristicile și beneficiile pe care
le oferă acest sistem sofisticat de control al accesului și modul în care răspunde nevoilor mediului
de securitate și tehnologie de astăzi.

1.2. Analiza aplicațiilor similare

Există o gamă variată de aplicații similare și proiecte care se axează pe dezvoltarea sis-
temelor de control al accesului. Aceste aplicații sunt concepute pentru a asigura securitatea și
autentificarea în diferite medii și contexte. Fie că este vorba despre protejarea unei încăperi, a unui
dispozitiv electronic sau a unor informații confidențiale, soluțiile de control al accesului au devenit
o parte esențială a vieții noastre moderne. Câteva dintre aceste aplicații și proiecte evidențiază
caracteristicile, tehnologiile și metodologiile utilizate pentru a oferi autentificare și securitate.

1.2.1. Fingerprint Door Lock

Unul dintre proiectele similare care implică securitatea și controlul accesului este un sistem
de închidere cu amprentă digitală realizat cu ajutorul Raspberry Pi Pico W. Acest proiect utilizează
tehnologia amprentelor digitale pentru a permite utilizatorilor să acceseze o încăpere sau un dis-
pozitiv electronic cu ușurință și securitate.

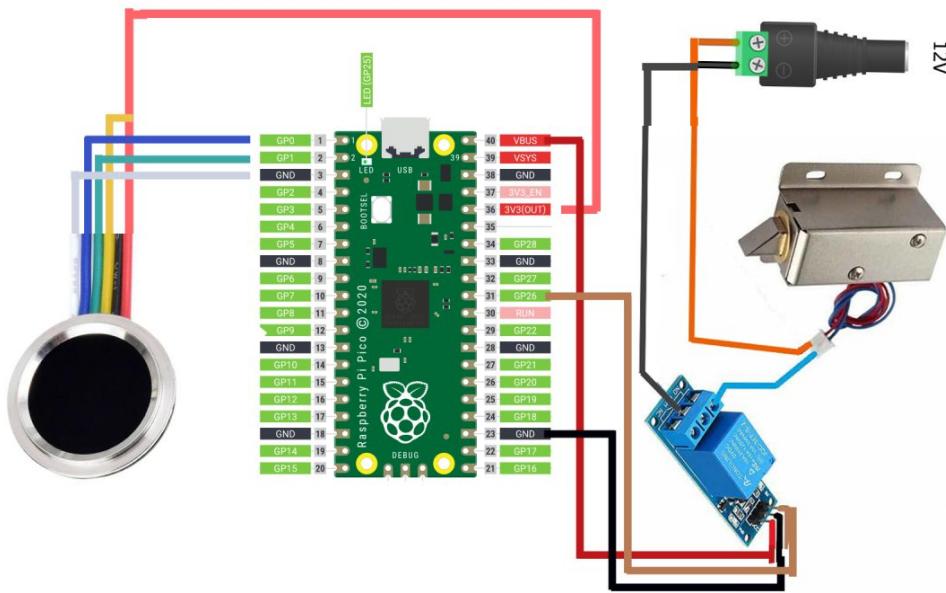


Figura 1.2. Sistem de închidere cu amprentă digitală²

Acest sistem utilizează senzori de amprentă digitală pentru a recunoaște și verifica iden-
titatea unui utilizator, aspect care oferă un nivel înalt de securitate, deoarece fiecare persoană are
amprente digitale unice. Își în cadrul acestui proiect, Raspberry Pi Pico servește drept bază a
sistemului. Aceasta gestionează citirea datelor de la senzorii de amprente și controlează încui-
toarea electrică. Tehnologia cu amprentă digitală identificată cu ajutorul unui modul biometric
de amprentă se bazează pe recunoașterea și înregistrarea caracteristicilor unice ale utilizatorului.

²Mai multe informații despre proiectul cu amprentă digitală pot fi găsite la:<https://www.electronicclinic.com/raspberry-pi-pico-fingerprint-door-lock-project/>

Procesul începe prin colectarea unei imagini a amprentei, apoi extrage caracteristicile distincte, precum crestele și intersecțiile acesteia. Aceste date sunt înregistrate sub formă de şablon și stocate într-o bază de date securizată. Atunci când o persoană încearcă să se autentifice, amprenta sa este comparată cu cele din baza de date, iar în funcție de rezultat, accesul este acordat sau refuzat. [3]



Figura 1.3. Modulul senzor de amprentă³

1.2.2. Home Security Motion Detector

O altă aplicație similară este un proiect care integrează Raspberry Pi și tehnologia IoT (Internet of Things) pentru a crea un sistem de securitate îmbunătățit, capabil să detecteze și să prevină potențiale riscuri, oferind în același timp utilizatorilor un control mai mare asupra securității lor. Sistemul propune o serie de caracteristici pentru monitorizarea și protecția locuinței, cum ar fi detectarea mișcării, controlul accesului și notificarea în timp real a evenimentelor de securitate. În principal, acesta utilizează senzori de mișcare și camere pentru a detecta și înregistra evenimente de securitate și poate fi controlat și monitorizat de la distanță prin intermediul unei aplicații mobile sau a unei interfețe web. [4]

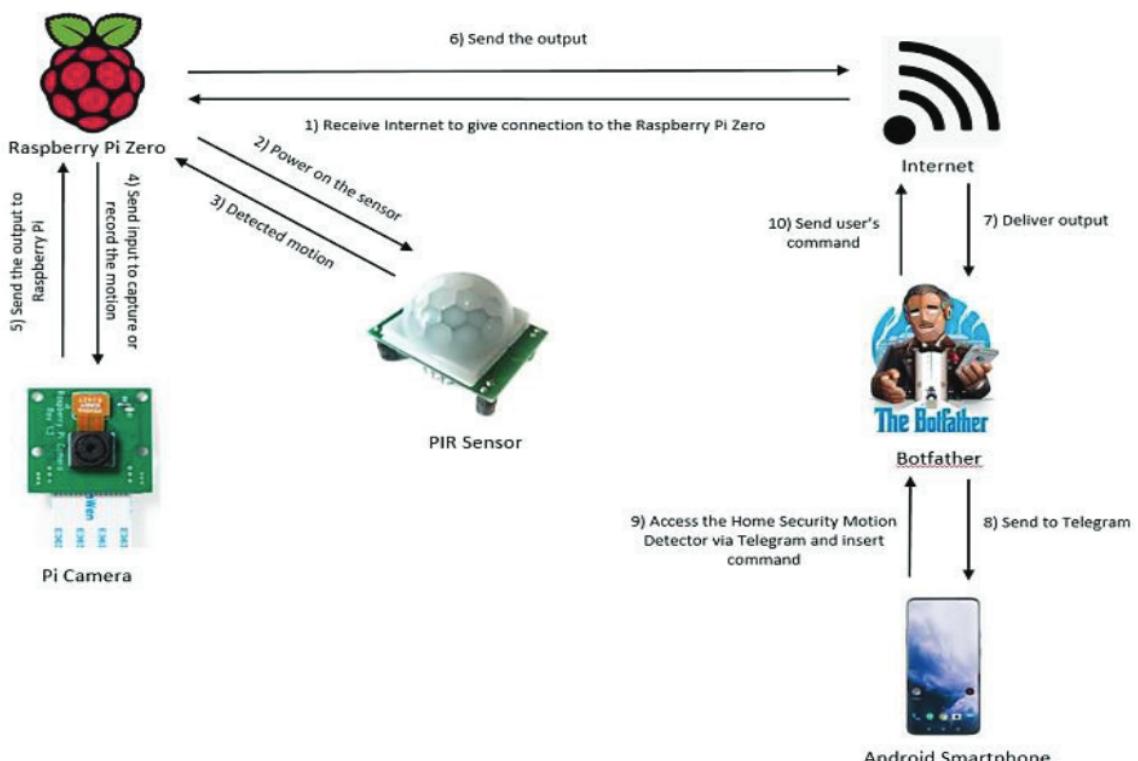


Figura 1.4. Arhitectură sistem securitate conform[4]

Comparând cele două aplicații, acestea se diferențiază prin metodologia de autentificare. În timp ce sistemul descris mai sus utilizează în principal camere și senzori pentru monitorizare și detectare, această lucrare se concentrează pe autentificarea utilizatorilor prin metode precum tastatura numerică și cardurile RFID. Aceasta oferă o alternativă robustă și flexibilă pentru gestionarea accesului în locuință, permitând utilizatorilor să aibă un control mai direct asupra securității și să personalizeze experiența lor.

1.3. Elaborarea specificațiilor privind caracteristicile aplicatiei

Scopul aplicatiei este crearea unei soluții eficiente pentru gestionarea accesului în zonele restrictionate și protejarea informațiilor sensibile cu ajutorul componentelor hardware și software utilizate. Astfel, sistemul își propune folosirea unor autentificări multiple care necesită implementarea unui mecanism de gestionare, inclusiv revocarea accesului pentru utilizatorii neautorizați.

De asemenea, lucrarea își propune și dezvoltarea unei interacțiuni ușor de înțeles și de accesat pentru utilizator, de aici și prezența unui display care va fi în strânsă legătură cu celelalte componente și-l va informa pe utilizator în funcție de gradul de autorizare pe care aceasta îl posedă. Prin urmare, aplicația are rolul de a facilita controlul prin mijloacele de securitate dispuse.

Capitolul 2. Proiectarea aplicației

2.1. Arhitectura aplicației

2.1.1. MicroPython

Pentru proiectul nostru, utilizăm MicroPython ca limbaj de programare compatibil. Acest limbaj este o versiune adaptată a Python 3 pentru microcontrolere și sisteme integrate. MicroPython oferă un mediu de dezvoltare rapid și ușor de utilizat pentru programarea dispozitivelor încorporate.

MicroPython se remarcă prin eficiența sa pentru sisteme încorporate și controlul direct asupra hardware-ului, în timp ce Python standard oferă o gamă mai largă de funcționalități și este potrivit pentru medii mai generoase în ceea ce privește resursele. Una dintre cele mai notabile diferențe este în ceea ce privește consumul de resurse. MicroPython este special optimizat pentru a funcționa în condiții cu resurse limitate, cum ar fi microcontrolerele, și ocupă mai puțin spațiu de memorie și necesită mai puțină memorie RAM decât Python standard. Pe de altă parte, Python este construit pentru a fi utilizat pe sisteme cu resurse mai bogate, precum computere și servere, și dispune de o bibliotecă standard mai completă și puternică. MicroPython gestionează direct operațiunile de bază ale unui sistem de operare, deoarece rulează direct pe hardware-ul dispozitivelor încorporate, oferind module pentru lucrul cu pini GPIO, periferice și alte componente specifice hardware-ului, în timp ce Python standard se bazează pe un sistem de operare complet. [5]

2.1.2. I2cLcd si MFRC522

În dezvoltarea proiectului este necesară utilizarea bibliotecilor care asigură funcționalitatea și eficiența sistemului. Aceste biblioteci reprezintă componente software esențiale care facilitează interacțiunea dintre microcontroller-ul Raspberry Pi Pico W și componente hardware, precum modulul de carduri RFID și ecranul LCD.

Biblioteca I2cLcd(Inter-Integrated Circuit Liquid Crystal) : această bibliotecă asigură funcționalitatea ecranului LCD conectat prin protocolul I2C și este responsabilă pentru afișarea mesajelor și a stării sistemului pe acesta. Protocolul I2C (Inter-Integrated Circuit) reprezintă o interfață de comunicare serială ce permite dispozitivelor electronice, precum Raspberry Pi Pico W și ecran LCD, să schimbe date și instrucțiuni între ele într-un mod eficient și fiabil.[6]

- Afișarea Textului: biblioteca permite afișarea mesajelor, stării sistemului și a informațiilor relevante pentru utilizator;
- Controlul Cursorului: aceasta este o funcționalitate importantă pentru a plasa textul în locațiile dorite de pe ecran;
- Modificarea Aspectului Textului: I2cLcd permite modificarea aspectului textului, inclusiv schimbarea culorii, dimensiunii și stilului acestuia, oferind flexibilitate în proiect pentru a crea o interfață cu aspect plăcut și informativă;
- Gestionarea Ecranului: I2cLcd facilitează gestionarea întregului ecran LCD, inclusiv activarea sau dezactivarea acestuia, ștergerea conținutului și resetarea afișajului;
- Interacțiune cu MicroPython: această bibliotecă a fost dezvoltată pentru a fi compatibilă și ușor de utilizat în cadrul mediului de dezvoltare MicroPython, astfel încât să poți programa interacțiunea cu ecranul LCD cu ușurință.

Biblioteca MFRC522 : această bibliotecă este dedicată modului RFID și permite comunicarea cu cardurile RFID, extragerea datelor și verificarea accesului în funcție de cardul citit.[7]

- Citirea Datelor de pe Carduri: biblioteca MFRC522 a fost creată pentru a face citirea datelor de pe cardurile RFID o sarcină simplă și eficientă. Oferă funcționalități și metode specializate pentru extragerea datelor stocate pe aceste carduri, inclusiv informații precum identificatori unici;
- Detectarea Cardurilor RFID: una dintre funcțiile-cheie ale acestei biblioteci este capacitatea să de a detecta prezența cardurilor RFID în zona de citire a cititorului MFRC522. Acest aspect este esențial pentru inițierea procesului de autentificare sau pentru acordarea accesului utilizatorilor;
- Inițializarea Cititorului: biblioteca MFRC522 oferă funcții dedicate pentru inițializarea și configurarea modulului RFID;
- Verificarea Cardurilor: cu datele citite de la cartelele RFID, biblioteca furnizează instrumente pentru a verifica dacă un card citit corespunde unei înregistrări din baza de date. Aceasta este o parte importantă a procesului de control al accesului sau autentificare a utilizatorilor;
- Integrare cu MicroPython: precum biblioteca I2cLcd, și MFRC522 este dezvoltată pentru a se potrivi perfect cu mediul MicroPython.

2.2. Componente Hardware

În cadrul proiectului, am utilizat o serie de componente hardware pentru a implementa un sistem de control al accesului avansat și sigur. Aceste componente au roluri esențiale în asigurarea funcționării corecte a sistemului și în furnizarea unei experiențe de utilizare fluide și securizate.

2.2.1. Raspberry Pi Foundation

Raspberry Pi Foundation este o organizație care își propune să promoveze și să revoluționeze domeniul tehnologiilor digitale prin furnizarea unor plăci de calcul puternice la un cost redus. Raspberry Pi a fost creat cu o orientare către educație, utilizatorii având posibilitatea să dezvolte proiecte în domeniul informaticii, electronicii, automatizării hardware și proiecte Internet of Things (IoT), folosind limbajele de programare precum Python, Java sau C++.

2.2.2. Raspberry Pi Pico W

Placa de dezvoltare Raspberry Pi Pico W este o versiune Wireless a modelului său anterior Raspberry Pi Pico. Varianta îmbunătățită se bazează pe același microcontroler RP2040, dar se remarcă prin conectivitatea Wireless (încorporând un chip wireless Infineon CYW43439), permitând o integrare mai bună în aplicațiile Internet of Things (IoT). [8]

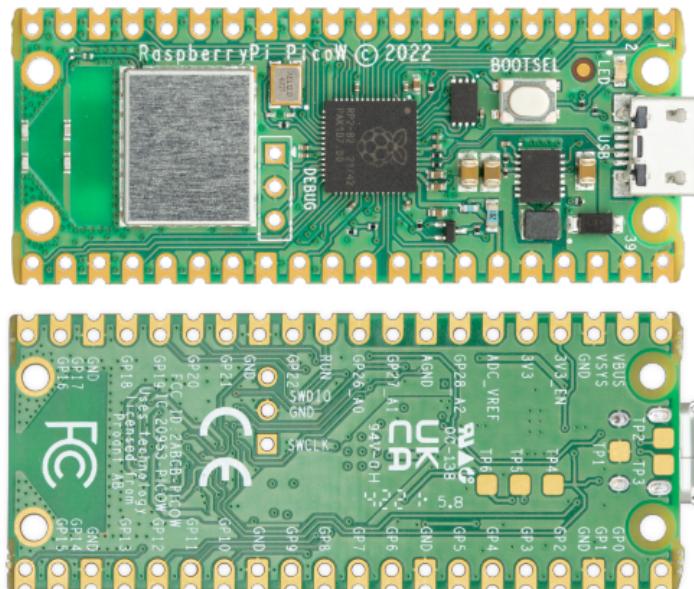


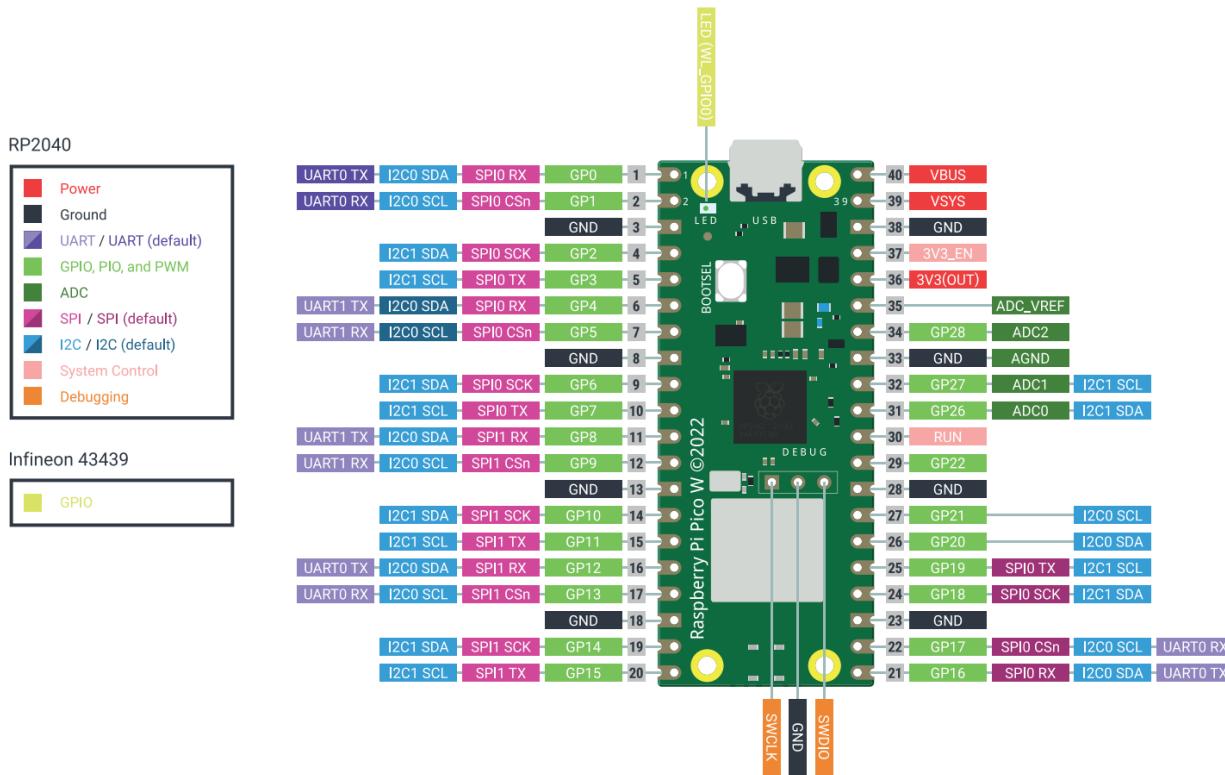
Figura 2.1. Raspberry Pi Pico W⁴

- **Performanță:**

- **Procesor:** Raspberry Pi Pico W cu microcontroler dual-core ARM Cortex M0+, frecvență flexibilă de până la 133 MHz;
 - **Memorie:** Dispune de o memorie SRAM de înaltă performanță de 264 kB și 2 MB memorie Flash extern Quad-SPIF pentru stocarea programelor și a datelor;
 - **Conecțitate:** Conectare wi-fi prin interfețe wireless 2.4GHz 802.11b/g/n și Bluetooth Low Energy (BLE) 5.2, oferind comunicarea cu alte dispozitive și retele;
 - **Alimentare:** Pentru alimentare și transmiterea datelor, aceasta dispune de un port micro USB B;

⁴Figura preluată din urmatorul pdf : <https://datasheets.raspberrypi.com/picow/pico-w-datasheet.pdf>

- Periferice:

Figura 2.2. Schema de conectare Pico W Rev3 conform⁵

Microcontroler-ul *Raspberry Pi Pico W* dispune de o serie de 40 de pini, dintre care 26 sunt de tipul GPIO (General-Purpose Input/Output) care pot fi utilizati pentru a conecta periferice precum LED-uri, motoare si senzori sau chiar pentru a stabili o comunicare cu alte plăci de microcontroler. Vom realiza o descriere a principalilor pini de pe Raspberry Pi Pico W, după cum reiese și din figura 2.2:

- Pinii de alimentare evidențiați prin culoarea roșie în schema de conectare sunt: pinul **VCC 3V3(OUT)** care furnizează o ieșire de 3,3V, permitând alimentarea cu succes a dispozitivelor externe; pinul **VBUS(USB Power Input)** care este tensiunea de intrare micro-USB; pinul **VSYS(External Power Input)** care permite conectarea unei surse de alimentare externe pentru a furniza energie placii dacă nu utilizați intrarea micro-USB;
- **GND(Ground)**: acești pini sunt conectați la masă (GND) și sunt folosiți pentru a asigura o referință comună pentru toate semnalele;
- **GPIO** : dispune de 26 de pini GPIO care pot fi configurați să funcționeze pentru intrări sau ieșiri digitale, comunicare serială, PWM etc;
- **UART** : placă dispune de pini UART (Universal Asynchronous Receiver-Transmitter) pentru comunicare serială;
- **SPI** : Interfața Serial Peripheral Interface (SPI) permite comunicarea rapidă între microcontroler și alte dispozitive(transferul de date sincron);
- **I2C** : acceptă interfața de comunicație I2C (Inter-Integrated Circuit), utilizată pentru conectarea mai multor dispozitive la un singur set de pini;

⁵Schema de conectare preluată din următorul site: <https://www.raspberrypi-spy.co.uk/2022/11/pi-pico-w-pinout-and-power-pins/>

- **ADC(Converter analog-digital)** : acești pini pot fi utilizați pentru a măsura semnale analogice, cum ar fi senzori sau alte componente care furnizează semnale variabile;
- **PWM (Pulse Width Modulation)** : raspberry pi pico w oferă pini care pot genera semnale PWM, utile pentru controlul motoarelor sau ajustarea luminozității LED-urilor;
- **LED-uri integrate** : placa include LED-uri integrate care pot fi controlate din software pentru a indica diverse stări sau activități;
- **Boot Mode** : pini speciali pentru setarea modului de boot al plăcii (mod normal, modul de programare etc.).

2.2.3. Modul RFID RC522

Modulul RFID RC522 este un dispozitiv electronic utilizat pentru a citi și a interacționa cu etichetele și cardurile RFID (Radio-Frequency Identification). Acesta este adesea folosit în proiecte de securitate, control de acces, automatizare și alte aplicații în care este necesară identificarea fără contact a obiectelor sau persoanelor.



Figura 2.3. Modulul RFID-RC522

Câteva caracteristici și specificații despre acest modul:

- Tensiune de funcționare: 2,5 V până la 3,3 V;
- Frecvența de operare: 13,56 MHz;
- Comunicare(9 pini): SPI, protocol I2C, UART;
- Consum de curent: 13-26mA;
- Viteza maximă de transfer de date: 10 Mbit/s pentru SPI;
- Curent maxim: 30mA

Modulul RFID RC522 generează un câmp electromagnetic la frecvență de 13,56 MHz pentru a stabili o legătură de comunicare cu etichetele RFID pasive din apropiere. Acesta dispune de un conector SPI cu 4 pini, permitând comunicarea cu o gamă variată de microcontrolere. Capacitatea sa de comunicare prin interfața SPI atinge o rată maximă de transfer de date de 10 Mbps. În plus, modulul suportă protocoalele I2C și UART pentru a asigura opțiuni flexibile de comunicare.[9]

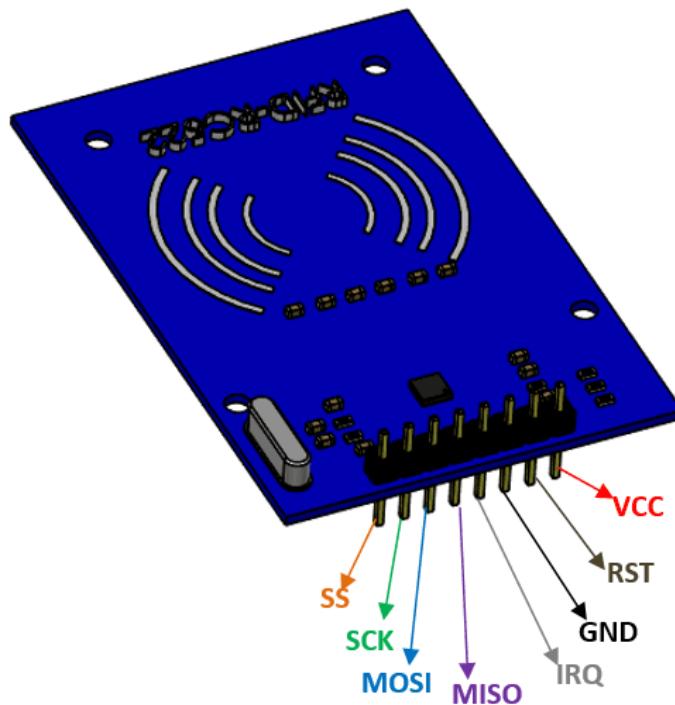


Figura 2.4. Configurație pini RFID-RC522⁶

În figura 2.4 putem observa schema de configurație a pinilor de pe RC522:

- **VCC** : furnizează tensiunea de alimentare de 3.3V;
- **RST** : pin de resetare folosit pentru a reseta sau a opri modulul;
- **GND** : pin sunt conectat la masă(GND), folosit pentru a asigura o referință comună pentru toate semnalele;
- **IRQ** : este utilizat pentru a semnaliza microcontroller-ului că modulul RC522 a înregistrat o situație specială, cum ar fi detectarea unei etichete;
- **MISO** : acest pin este folosit pentru a transmite datele de la modulul RC522 la microcontroler în interfața SPI;
- **MOSI** : este pinul prin care datele sunt transmise de la microcontroller către modulul RC522 în cadrul interfeței SPI;
- **SCK** : pinul SCK este semnalul de ceas pentru interfața SPI, sincronizând transferul datelor între modulul RC522 și microcontroler;
- **SS/SDA/Rx** : acest pin este folosit pentru a transmite date seriale între modulul RC522 și microcontroler prin interfața SPI;

⁶Mai multe informații despre modulul RFID-RC522 pot fi găsite la: <https://components101.com/wireless/rc522-rfid-module>

2.2.4. Display LCD și adaptor I2C

Ecranul LCD împreună cu modulul I2C reprezintă un dispozitiv de afișare care utilizează protocolul I2C (Inter-Integrated Circuit) pentru a transmite informații de la microcontroler la display.



Figura 2.5. Display LCD cu I2C⁷

Modulul LCD(16x2) este utilizat pentru a afișa informații vizuale, cum ar fi caractere și simboluri specifice prin cele două linii cu 16 caractere fiecare. Acest tip de afișaj funcționează pe baza cristalelor lichide care reacționează la electricitate pentru a modifica lumina care trece prin ele, creând astfel imaginea pe ecran.[10]

Alte specificații pentru display-ul LCD:

- Tensiune de alimentare: 5V;
- Tensiune alimentare backlight: 4.2V;
- Curent de lucru: 3mA;
- Nr. total de 16 pini utilizați pentru conectarea și controlul afisajului;

Adaptorul I2C este un modul adițional utilizat pentru comunicarea dintre display-ul LCD și microcontroller folosind interfața I2C (Inter-Integrated Circuit). Aceasta convertește datele primite în semnale seriale I2C, reducând numărul de pini necesari pentru conectivitate și control și simplificând astfel conexiunea între cele 2 dispozitive.

⁷Mai multe informații despre display-ul 16x2 și adaptorul I2C pot fi găsite la:http://handsontec.com/datasheets/module/I2C_1602_LCD.pdf

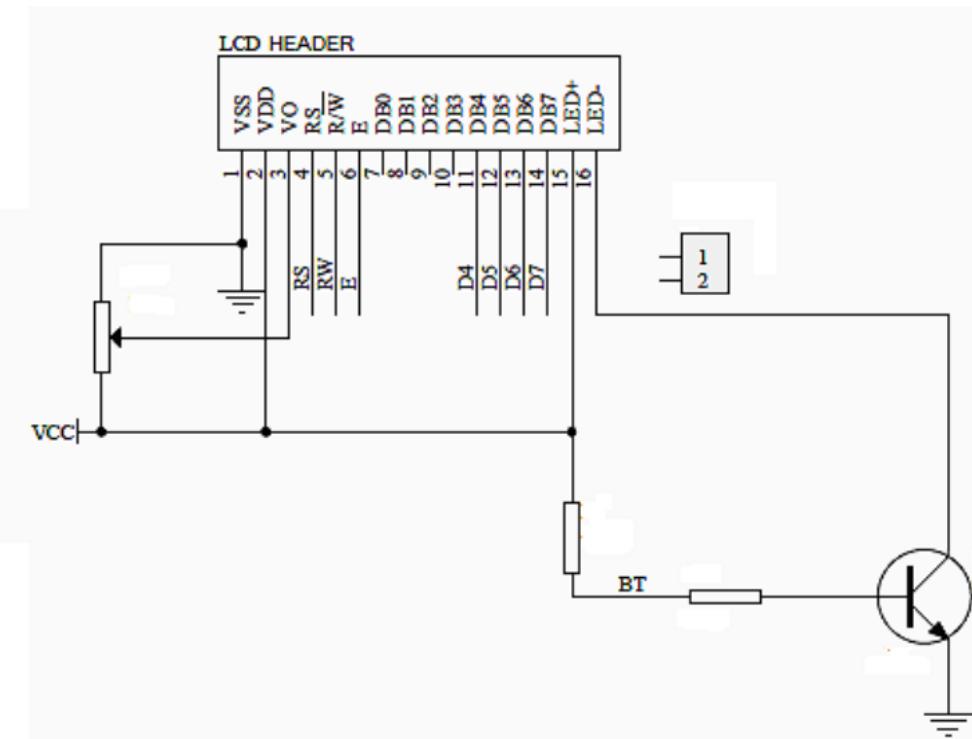


Figura 2.6. Diagrama circuitului de referință pentru LCD 16x2 I2C

2.2.5. Încuietoare electrică 12V

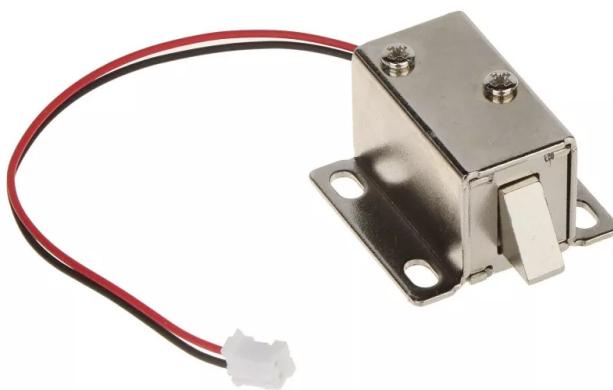


Figura 2.7. Încuietoare electrică 12V

Încuietoarea prezentată în figura 2.7 este dispozitivul pe care îl vom utiliza pentru a controla accesul securizat, prin intermediul unui semnal controlat de un releu și alimentat de la o sursă de energie(12V).

Câteva caracteristici și informații despre încuietoarea electrică:

- Tensiune : 12V DC
- Timp de deblocare : 1 secunda

- Consum: 650 mA;
- Putere : 9.6W
- Curent: 0.6 A, maxim :0.9 A

2.2.6. Modul Releu cu un singur canal

Modulul de releu cu un singur canal este un dispozitiv electronic utilizat pentru a controla comutarea circuitelor mai mari, cum ar fi alimentarea sau oprirea unor dispozitive sau aparate electrice, prin intermediul unui semnal de control mai mic.



Figura 2.8. Modul Releu cu un singur canal⁸

Un modul releu funcționează ca un întrerupător care poate fi acționat de la distanță, permitând controlul unui dispozitiv de mare putere cu un semnal electric de intensitate mică. Prin bobina de sârmă înfășurată în jurul electromagnetului releului, curentul electric circulă, generând un câmp magnetic. Acest câmp magnetic atrage armătura metalică din interiorul releului, declanșându-i mișcarea pentru a face contact cu un comutator. Acest comutator are capacitatea de a controla fluxul electric către un dispozitiv de finală putere, precum o lumină, un motor sau un element de încălzire. Când alimentarea electrică către bobină este întreruptă, câmpul magnetic se disipează, iar armătura revine în poziția inițială, întrerupând astfel conexiunea cu comutatorul.[11]

⁸Mai multe informații despre modulul releu cu un singur canal pot fi găsite la:<https://circuitdigest.com/microcontroller-projects/interface-single-channel-relay-module-with-arduino>



Figura 2.9. Configurație pini Modul Releu

În figura de mai sus 2.9, este prezentată configurația pinilor și schema de conectare pentru modulul releu cu un singur canal:

- **VCC** : pin folosit pentru a furniza alimentare de 5V la bobina releului;
- **GND** : acest pin este conectat la masă (tensiunea de referință a circuitului);
- **IN** : acest pin este numit și pin de control deoarece este utilizat pentru a furniza semnalul de control sau de activare pentru a actiona releul. Când semnalul de control este activat (HIGH), releul comută contactele sale. Semnalul de control poate fi furnizat de la un microcontroler, un senzor sau un alt dispozitiv de control;
- **COM** : acest pin este contactul comun al releului, care este conectat la circuitul controlat;
- **NO** : reprezintă contactul normal deschis al releului, când releul este în starea inactivă (necomutat), acest contact este deschis, întrerupând circuitul controlat. Când releul este activat, acest contact se închide;
- **NC** : reprezintă contactul normal închis al releului, când releul este în starea inactivă, acest contact este închis, permitând trecerea curentului prin circuitul controlat. Când releul este activat, acest contact se deschide;

2.2.7. Tastatură keypad 3x4



Figura 2.10. Tastatura membrană 3x4 keypad

Un keypad 3x4 este un dispozitiv de intrare utilizat pentru introducerea rapidă a cifrelor și a unor funcții de bază. Este compus dintr-o matrice de 12 butoane, organizate în 3 rânduri și 4 coloane. Butoanelor le sunt atribuite cifre de la 1 la 9, împreună cu 0 și câteva caractere speciale sau funcționale, fiecare buton fiind poziționat la intersecția dintre un rând și o coloană.

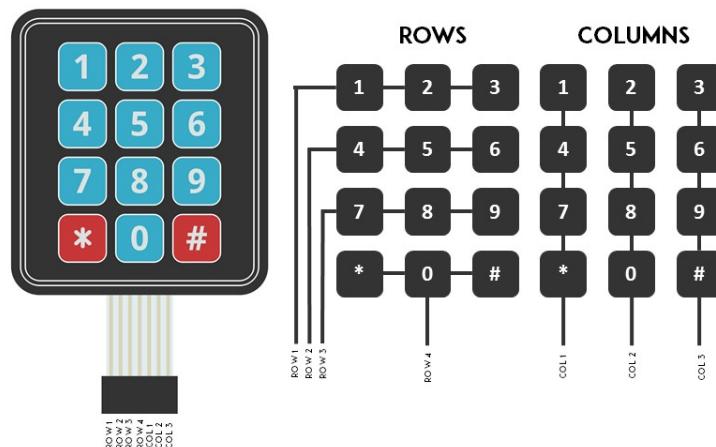


Figura 2.11. Schema de funcționare keypad⁹

Câteva caracteristici și funcționalități despre keypad 3x4:

- Tensiune de operare : max. 34V DC;
- Consum curent : 100mA;
- Pini: keypad-ul dispunde de 7 pini conectati la microcontroller, 3 pini(ROW) pentru identificarea fiecarei linii si 4 pini(COL) pentru indentificarea coloanelor;

Microcontroler-ul scanează în mod repetat matricea butoanelor. Pentru a identifica butonul apăsat, microcontroller-ul activează un rând și verifică starea fiecărei coloane pentru a detecta închiderea circuitului (apăsarea butonului). Aceasta permite determinarea poziției butonului în funcție de rând și coloană.[12]

2.2.8. Alte componente periferice

Modulul Buzzer este un dispozitiv de ieșire audio care generează sunete sau semnale sonore atunci când este activat. Acesta constă într-un element piezoelectric sau electro-mecanic care, atunci când este alimentat cu un semnal electric, generează o vibrație în frecvență specificată, rezultând un sunet.



Figura 2.12. Modul Buzzer

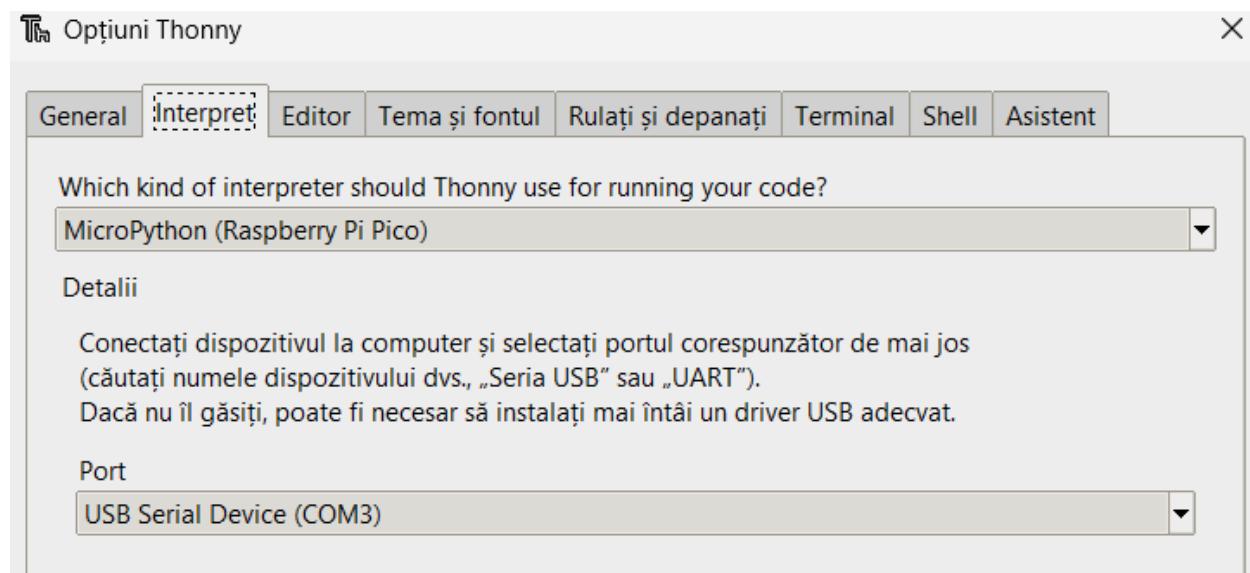
⁹Figura preluată de pe următorul site:<https://www.sigmanortec.ro/Tastatura-membrana-Keypad-3x4-p125941834>

Capitolul 3. Implementarea aplicației

Implementarea aplicației s-a realizat pe placa Raspberry Pi Pico W, utilizând limbajul MicroPython și bibliotecile corespunzătoare pentru interacțiunea cu modulele hardware. Dezvoltarea s-a bazat pe un proces etapizat, care a inclus configurarea modulelor hardware și dezvoltarea logicii de control.

3.1. Configurarea microcontroller-ului

Un prim pas în realizarea practică a proiectului după partea hardware și asamblarea componentelor, a fost configurarea microcontroller-ului Raspberry Pi Pico W. Am vizitat platforma Raspberry Pi și am descărcat o versiune a firmware-ului din secțiunea Datasheets. Apoi, am conectat microcontrollerul la calculator și am transferat fișierul descărcat în directorul corespunzător al microcontrollerului. În continuare, am deschis editorul Thonny IDE, am ales portul pe care era conectat RP2040 și am început să scriu cod într-un fișier nou.



```
MicroPython v1.19.1-88-g74e33e714 on 2022-06-30; Raspberry Pi Pico W with RP2040
Type "help()" for more information.
MicroPython v1.19.1-88-g74e33e714 on 2022-06-30; Raspberry Pi Pico W with RP2040
Type "help()" for more information.
>>>
```

3.2. Conectarea componentelor

Pentru funcționalitatea proiectului, am conectat toate componentele prezentate mai sus [2.2], plecând de la documentația microcontroler-ului.[8]

În primul rând am început prin conectarea modulului RFID prezentat în subcapitolul 2.2.3 la pinii corespunzători Raspberry Pi Pico W și mai apoi cu cele 2 led-uri (rosu pentru o posibilă conectare incorectă și verde pentru un card corect), respectiv modulul buzzer. Acest prim pas m-a ajutat să pot afla dacă cele 2 etichete rfid funcționează în mod corespunzător odată cu apropierea lor de modul.

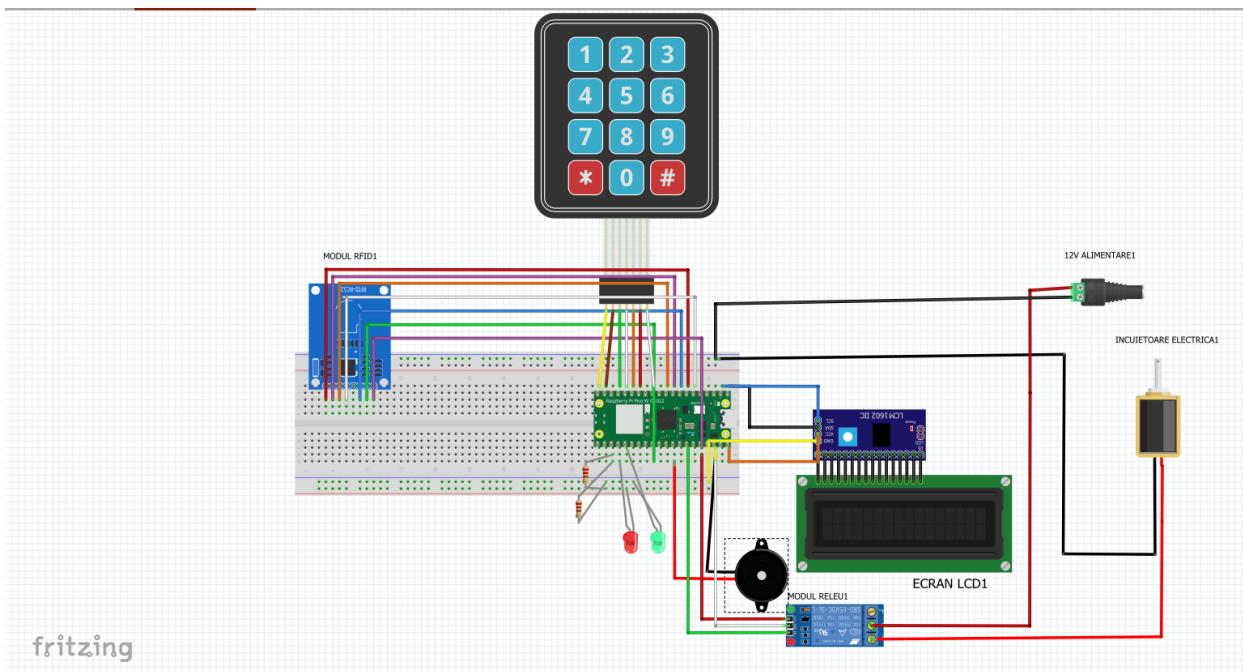


Figura 3.1. Diagrama grafică a circuitului¹⁰

Am continuat cu asamblarea încuietorii electrice alimentată la o baterie de 12V și modul releu pentru a verifica dacă aceasta funcționează la declanșarea semnalului primit de la modulul RFID. Așa cum am menționat în subcapitolele 2.2.5, 2.2.6 modulul releu este un dispozitiv ce funcționează ca un întrerupător controlat electronic, fiind astfel folosit pentru a controla încuietarea electrică, care are nevoie de o tensiune de 12V pentru a se debloca. Când releul este închis, permite curentului electric să circule, iar când este deschis, înlătruje fluxul de curent.

Firele corespunzătoare pentru GND ale încuietorii și sursei de alimentare de 12V au fost conectate împreună la borna negativă a breadboard-ului și astfel, firele de alimentare (VCC) au fost legate la porturile releului (NO și COM). Pinii VCC, GND și IN ai modulului releu au fost conectați la pinii 3V3(OUT), GND și GP28 ai microcontroler-ului.

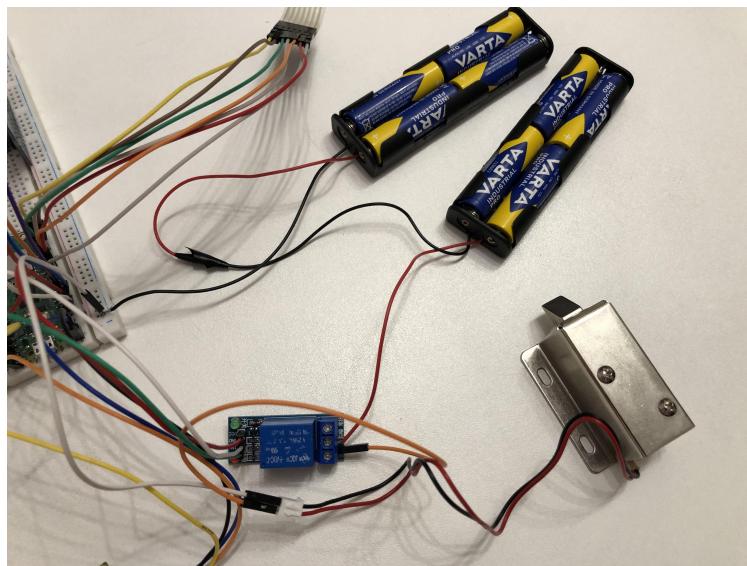


Figura 3.2. Conectarea încuietorii electrice la sursa de alimentare și modulul releu

În final, am completat schema de componente cu adăugarea display-ului LCD și tastatura

¹⁰Figura realizată cu ajutorul pragrului :<https://fritzing.org/>

membrană 3x4 keypad.

Am conectat display-ul LCD [2.2.4] la adaptorul I2C, acesta fiind pus în legătură prin intermediul pinilor GP0,GP1 și de asemenea conectat la VBUS și GND. Keypad-ul 3x4 [2.2.7] dispune de 7 pini de conectare: 4 pentru rândurile tastaturii(GP15,GP14,GP13,GP12) și 3 pentru coloane (GP11,GP10,GP9).

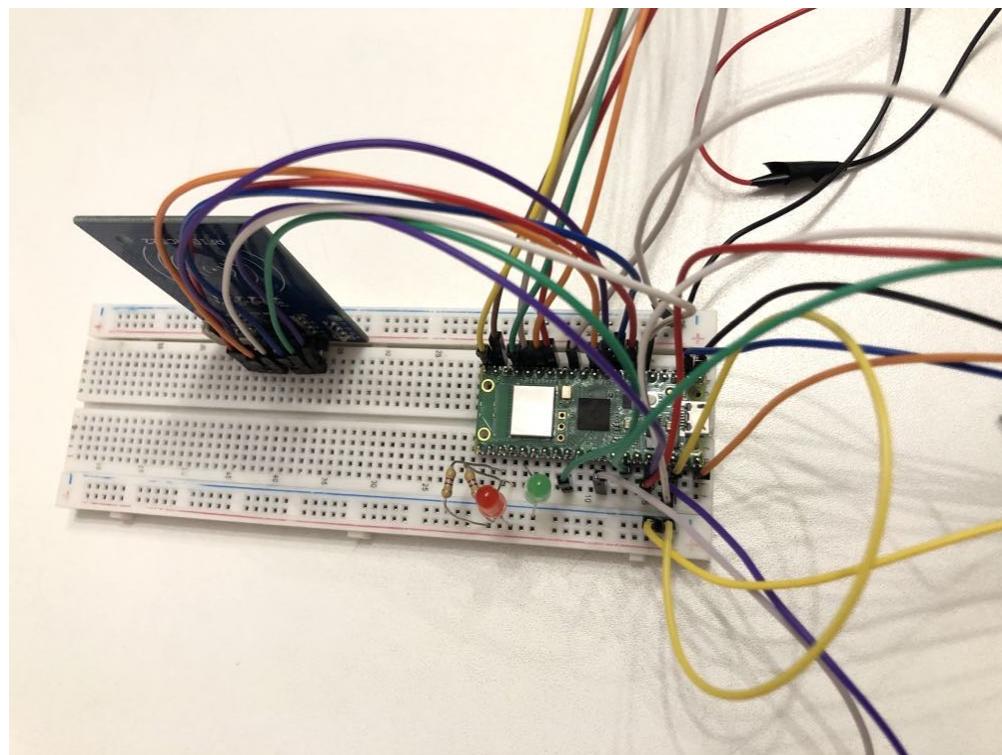
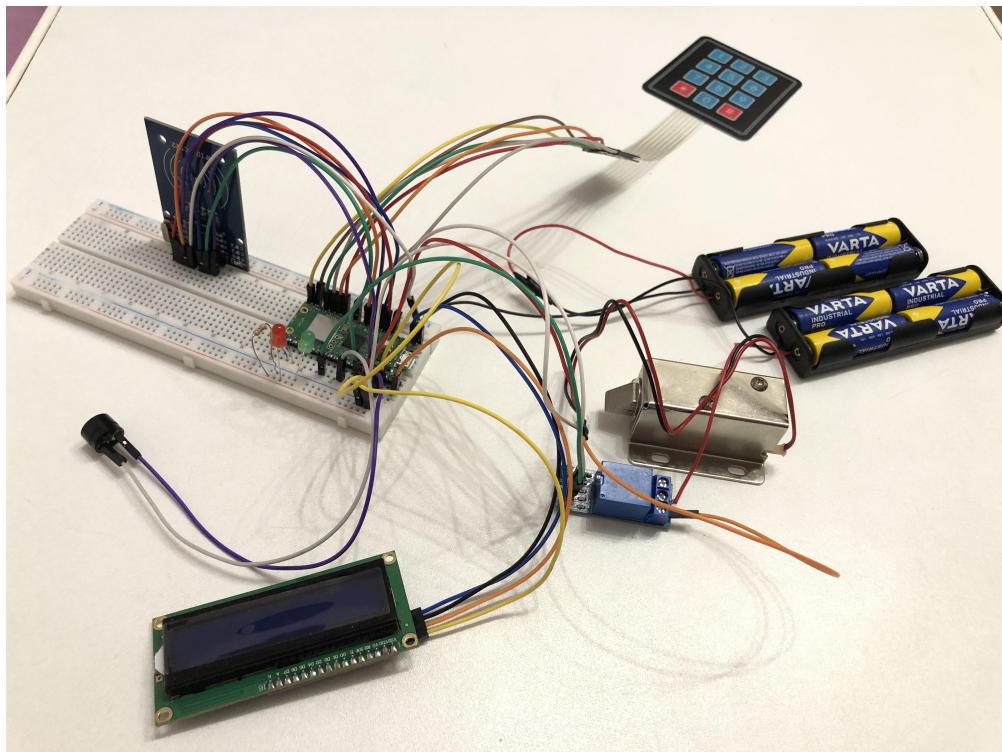


Figura 3.3. Conecțarea componentelor la Pico W

3.3. Implementarea componentelor

După ce am realizat conectarea componentelor, am deschis o filă nouă în editorul Thonny IDE și am început să verificăm dacă componentele sunt funcționale.

3.3.1. Modulul RFID RC522

Am început prin verificarea modului RFID pentru a putea obține cele 2 adrese UID (Unique Identifier Address) pentru etichetele RFID.

```

25 print("")
26 print("Apropiati cardul RFID")
27 print("")
28
29 while True:
30
31     (stat, tag_type) = rc522.request(rc522.REQALL)
32
33     if stat == rc522.OK:
34         (status, raw_uid) = rc522.SelectTagSN()
35         if stat == rc522.OK:
36             rfid_data = "{:02x}{:02x}{:02x}{:02x}".format(raw_uid[0], raw_uid[1], raw_uid[2], raw_uid[3])
37             print("Card detectat! Adresa: {}".format(rfid_data))

```

Shell >>> %Run -c \$EDITOR_CONTENT

Apropiati cardul RFID

Card detectat! Adresa: 739cd1aa
Card detectat! Adresa: c30fa91b

Figura 3.4. Adresele UID de conectare pentru etichetele rfid

La detectarea cu succes a cititorului RFID, informația extrasă, respectiv adresa UID va fi sub forma unei liste de octeți. Funcția 'uidToString(uid)' va converti lista de octeți într-un sir de caractere hexazecimale mai ușor de citit și de comparat. Acest sir poate fi folosit pentru a efectua verificări sau pentru a identifica cartela. După ce am găsit adresele specifice modului RFID am creat o instanță a obiectului MFRC522, care este folosit pentru a controla cititorul de tip MFRC522 conectat la Pico W. Această instanță este inițializată cu pinii de conectare pentru comunicația SPI (Serial Peripheral Interface).

```

def uidToString(uid):
    mystring = ""
    for i in uid:
        mystring = "%02X" % i + mystring
    return mystring

rc522 = MFRC522(spi_id=0,sck=6,miso=4,mosi=7,cs=5,rst=22)

```

3.3.2. Dispaly LCD și tastatura keypad 3x4

Ecranul LCD și tastatura keypad sunt componente interconectate care lucrează împreună pentru a permite utilizatorului să controleze și să interacționeze cu sistemul. Ecranul este utilizat pentru a afișa informații către utilizator și pentru a furniza feedback vizual cu privire la starea sistemului, cum ar fi confirmarea sau respingerea unui cod PIN introdus, sau validarea uneia dintre cartelele RFID. Tastatura keypad este o interfață de introducere de date, care permite utilizatorului să introducă un cod PIN pentru a accesa încuietoarea.

Pentru a implementa funcționalitatea tastaturii keypad, am construit o matrice de butoane cu 12 taste, aranjate în patru rânduri și trei coloane. Am utilizat un set de pini pentru a controla rândurile și coloanele tastelor. Atunci când utilizatorul apasă o tastă, programul detectează tasta apăsată și adaugă caracterul corespunzător într-o listă. Legătura dintre listele rowValue și colValue este esențială pentru funcționarea corectă a unui keypad matrice. Ele trebuie să fie setate în moduri diferite (unul ca ieșire și celălalt ca intrare) pentru a efectua scanarea și identificarea butoanelor apăsate.

Liniile de ieșire (rowPins) sunt activate secvențial pentru a verifica care tastă este apăsată într-o anumită coloană, în timp ce coloanele (colPins) sunt monitorizate pentru a detecta schimbările de stare atunci când o tastă este apăsată sau eliberată. În timpul scanării, fiecare linie (rând) este setată pe valoarea 1, ceea ce face ca acea linie să fie activă și să furnizeze curent printr-un rând specific de butoane. Apoi, se setează starea inițială a coloanelor pe valoare logică 0. Când un buton este apăsat într-o anumită coloană, nivelul pinului va deveni 1. Acest lucru se repetă pentru fiecare rând și coloană, astfel încât toate butoanele să fie scanate.

```
def checkKeyPress():
    for row in range(4):
        for col in range(3):
            rowValue[row].high()
            if colValue[col].value() == 1:
                print("Tastă apasată:", keyPad[row][col])
                key_press = keyPad[row][col]
                utime.sleep(0.3)
                password.append(key_press)
            if len(password) == 4:
                checkPassword(password)
                for x in range(0, 4):
                    password.pop()
            rowValue[row].low()
```

Figura 3.5. Funcție verificare keypad

Funcția checkKeyPress() [3.5] este responsabilă pentru detectarea și gestionarea apăsărilor de taste. Aceasta utilizează buclele for pentru a parcurge toate liniile și coloanele tastaturii. Atunci când găsește o tastă apăsată (când valoarea coloanei este 1), afișează caracterele corespunzătoare în consolă (print("Tastă apasată:", keyPad[row][col])) și le adaugă în lista password. Dacă parola are 4 caractere, apelăm funcția checkPassword(password) pentru a verifica dacă parola introdusă este corectă. După ce parola este verificată, se golește lista password pentru a pregăti introducerea unei noi parole. În final, după ce s-au scanat toate butoanele dintr-un rând, pinurile corespunzătoare rândului sunt setate pe nivelul LOW (0) pentru a dezactiva acel rând și a permite trecerea la scanarea următorului rând.

3.3.3. Încuietoare electrică

Încuietoarea electrică servește ca mecanism de securitate central, fiind în strânsă legătură cu toate celelalte componente. Blocarea sau deblocarea acestora depinde doar de semnalele primite de la modulul RFID și tastatura keypad.

Cardul RFID autorizat poate declansa deblocarea încuietoarei electrice. Acest lucru se realizează prin intermediul unui semnal electric sau al unui protocol de comunicație între cititorul RFID și sistemul de control al accesului. Atunci când un card este detectat, sistemul va comanda încuietoarea să se deschidă pentru a permite accesul.

3.4. Proiectarea dispozitivului

Pentru a reprezenta cât mai sugestiv ideea lucrării și a înțelege mai ușor cum funcționează întregul sistem, a fost realizată o machetă care înfățișează imaginea unui spațiu care poate fi deblocat.

Prima etapă a dispozitivului a implicat confectionarea unei cutii din materialul Komatex. Acest material a fost ales pentru durabilitatea și ușurința sa de prelucrare. Am început prin efectuarea unor măsurători precise pentru a adapta ulterior componentele dispozitivului. S-a realizat și o mini ușă cu mâner cu ajutorul a 2 balamale, fiecare de câte 3 cm, asigurând o fixare solidă și garantând astfel accesul ușor la interior și legătura cu încuietoarea electrică.

A doua etapă a constat în efectuarea unor decupaje în partea de sus a dispozitivului pentru a integra ușor ecranul LCD, tastatura keypad, modulul RFID și implicit led-urile pentru a vizualiza starea încuietorii.

Etapa finală a constat în testarea dispozitivului, verificarea funcționalității corespunzătoare a componentelor și a mecanismului de blocare/deblocare.





Figura 3.6. Proiectarea dispozitivului

3.5. Dificultăți întâmpinate și modalități de dezvoltare

Dificultățile întâmpinate pe parcursul dezvoltării proiectului au fost legate de conectarea componentelor hardware implicate. Fiind un dispozitiv care funcționează cu ajutorul unei surse de alimentare pentru blocarea sau deblocarea încuietorii electrice, documentația detaliată despre configurarea pinilor de pe microcontroller a fost necesară pentru potențialul risc al apariției unui fenomen de supratensiune, întrucât niciunul dintre pinii de alimentare ai Pico W nu trebuie expus la tensiune peste 5.5V. Alimentarea pentru încuietoarea electrică trebuie să fie complet separată de cea pentru Raspberry Pi Pico W, orice legătură între acestea fiind susținută de modulul releu cu un singur canal. Pentru partea de software, dificultățile întâmpinate au apărut la implementarea funcționalității keypad-ului, întrucât acesta folosește o matrice de îmbinare a liniilor cu coloane, dar logica din spatele acestuia se bazează doar pe stările butoanelor (active sau inactive).

Capitolul 4. Testarea aplicației și rezultate experimentale

4.1. Elemente de configurare ale aplicației

Pentru a valida, evalua și asigura o bună funcționare a sistemului dezvoltat, este necesară o etapă de testare. Toate componentele hardware utilizate, precum microcontroller-ul Pico W, modulul RFID, tastatura keypad 3x4, led-urile, dar și ecranul LCD, trebuie să fie alimentate corespunzător și să beneficieze de o sursă de alimentare electrică stabilă (8 baterii a câte 1.5V fiecare). De asemenea, toate componentele trebuie să fie conectate corect la microcontroller și să comunice eficient între ele pentru funcționarea corespunzătoare. În figura 4.1 este explicată logica de conectare a dispozitivului.

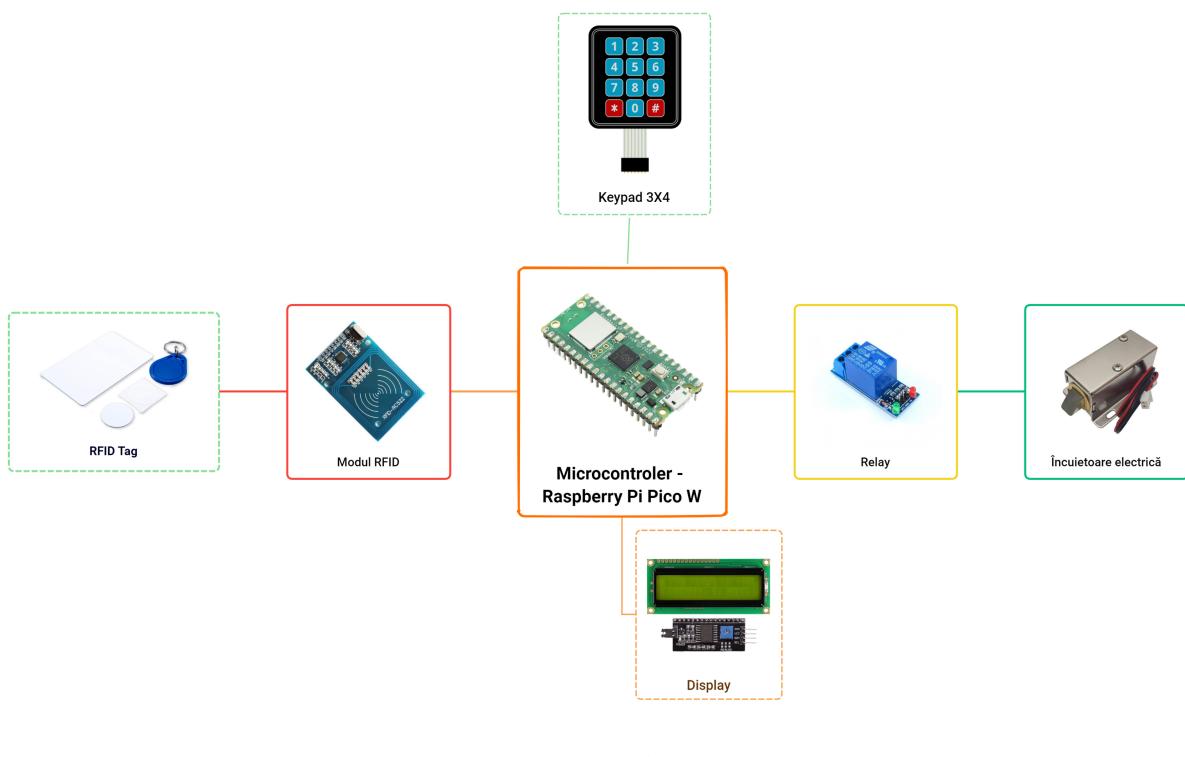


Figura 4.1. Logica de conectare a componentelor

Cu ajutorul programului Thonny IDE, limbajului de programare MicroPython și bibliotecile necesare folosite, a fost configurat microcontroller-ul Pico W pentru a interpreta și gestiona interacțiunile cu toate componentele hardware.

4.2. Rezultate obținute

Așa cum reiese și din titlul lucrării, sistemul se bazează pe o autentificare multiplă, aceasta însemnând apropierea etichetelor RFID sau introducerea unui cod PIN pe keypad-ul 3x4, ambele metode comunicând direct cu ecranul LCD și încuietoarea electrică. Pentru o comunicare mai bună cu utilizatorul, înainte de verificarea accesului, ecranul LCD va afișa un mesaj de început prin care se specifică care poate fi metoda de control al accesului [4.2].

```
lcd.clear()
lcd.move_to(0,0)
lcd.putstr("Proiect") # mesajul de inceput
utime.sleep(3)
lcd.clear()
lcd.putstr("Card sau pin:")
```

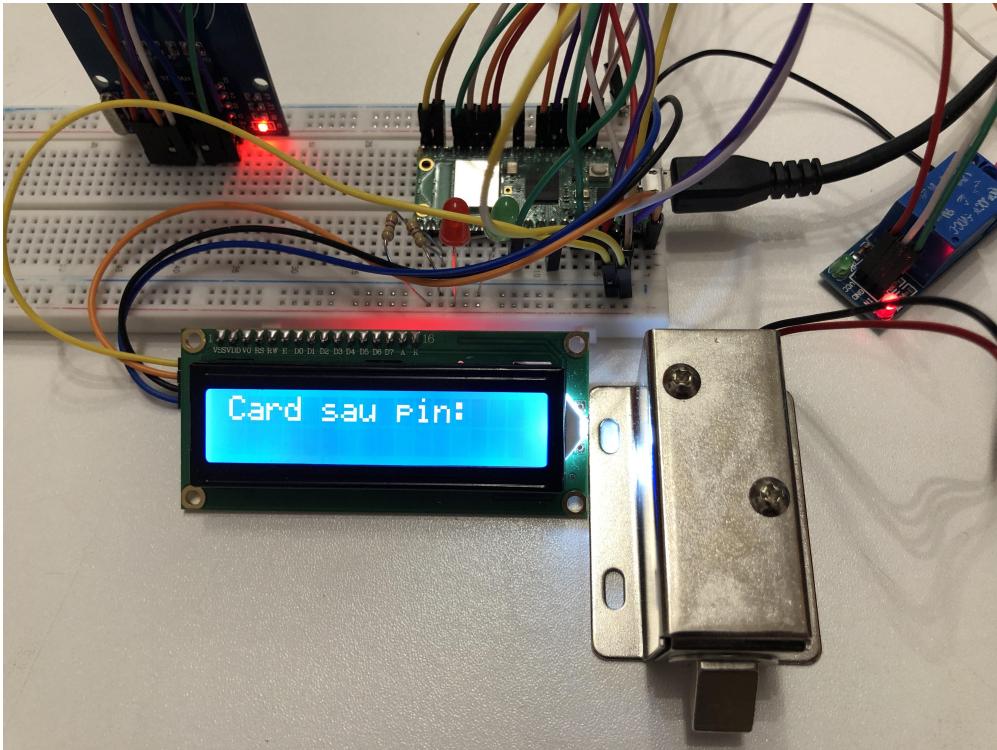
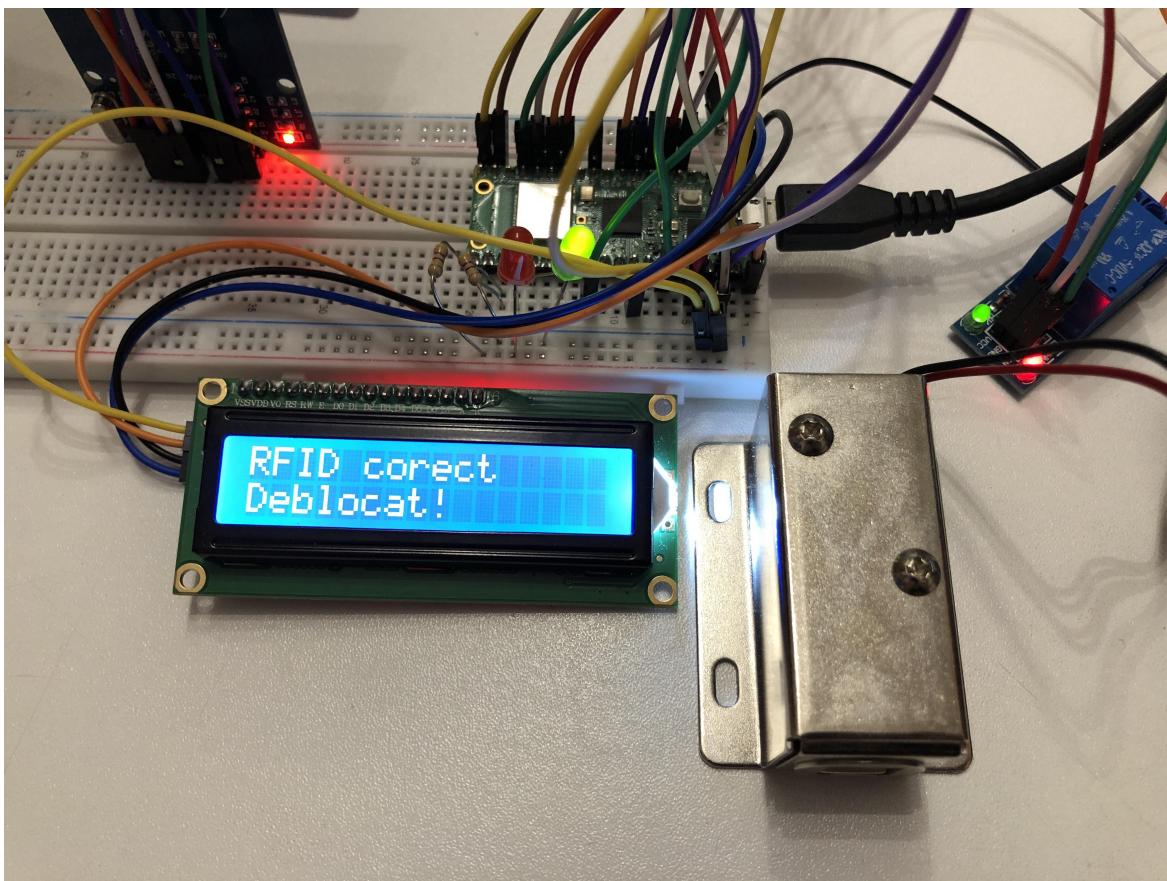


Figura 4.2. Mesaj de început

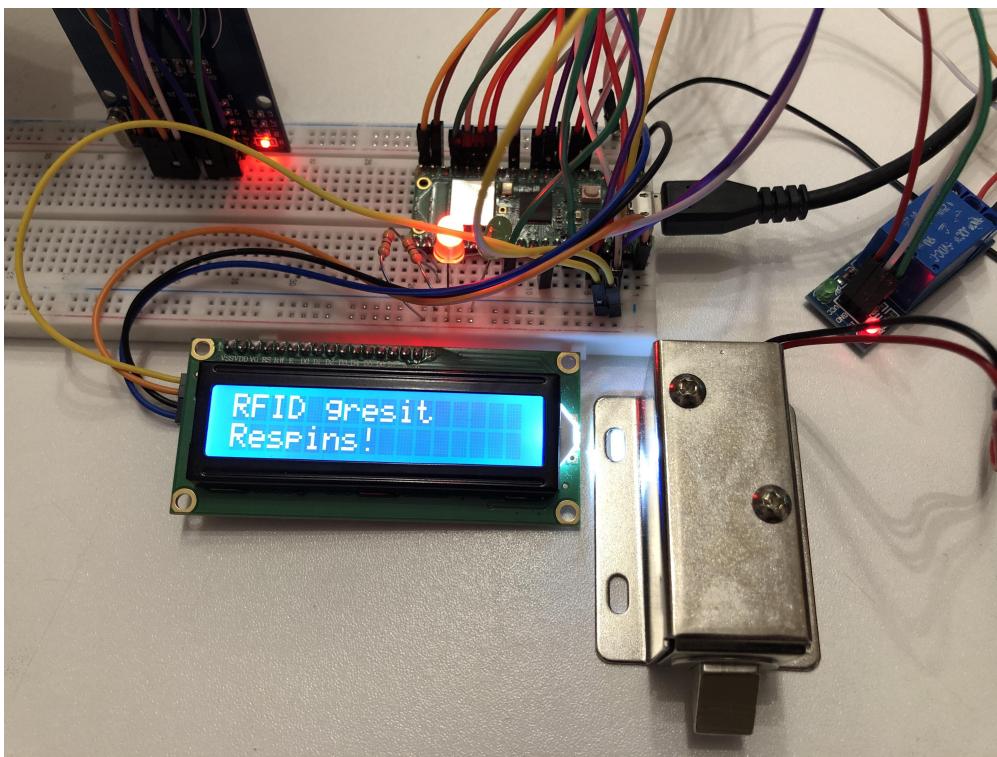
Cele 2 metode de autentificare pot lucra în concomitent, deci nu contează ordinea în care sunt folosite. Când un card RFID este detectat, datele cardului sunt comparate cu o valoare specifică ("739cd1aa"). Dacă cardul este recunoscut, încuietoarea se deblochează, afișându-se mesajul corespunzător, și se declanșează led-ul de culoare verde.

```
if rfid_data == "739cd1aa":

    lcd.clear()
    lcd.move_to(0,0)
    lcd.putstr("RFID corect")
    lcd.move_to(0, 1)
    lcd.putstr("Deblocat!")
    lock.value(0)
    GLed.value(1)
    utime.sleep(5)
    lcd.clear()
    lcd.putstr("Card sau pin:")
    lock.value(1)
    GLed.value(0)
```



Dacă cardul RFID este cel incorect, pe ecran se va afișa un mesaj de tipul 'RFID greșit', se va declanșa led-ul de culoare roșie și buzzer-ul se va activa.



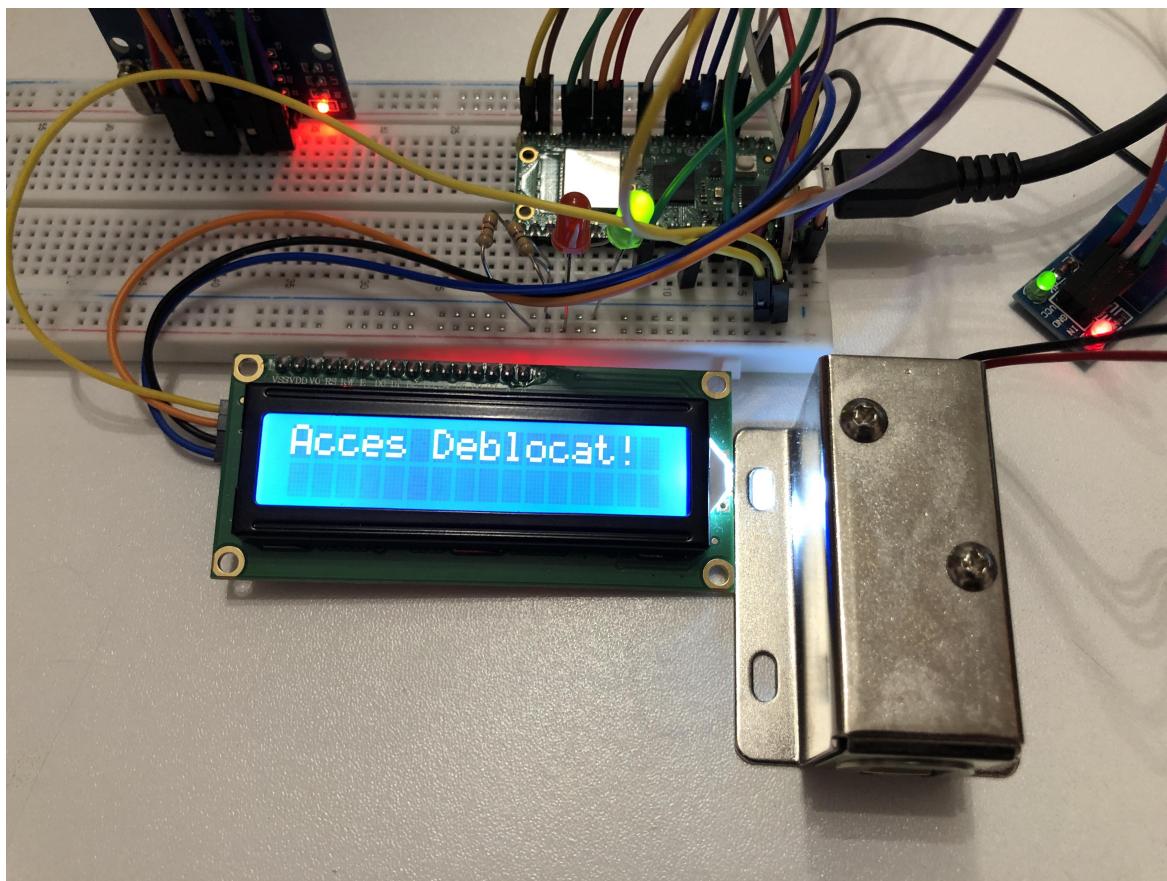
```
else:  
  
    lcd.move_to(0,0)  
    lcd.clear()  
    lcd.putstr("RFID gresit")  
    lcd.move_to(0, 1)  
    lcd.putstr("Respins!")  
    buzzer.value(1)  
    RLed.value(1)  
    utime.sleep(2)  
    lcd.clear()  
    lcd.putstr("Card sau pin:")  
    buzzer.value(0)  
    RLed.value(0)
```

Comenziile lcd.clear() și utime.sleep() sunt utilizate în contextul afișării și pentru gestionarea timpului: lcd.clear() șterge orice mesaj precedent sau orice informație anterioară de pe ecran pentru a face loc afișării unui mesaj sau a unei informații noi; utime.sleep() introduce o întârziere, o pauză pentru o perioadă specificată în milisecunde, pentru a menține un mesaj pe display.



Pentru a efectua testarea autentificării cu ajutorul tastaturii, folosim funcția `checkPassword()`. Această funcție preia parola introdusă de utilizator și o compară cu parola predefinită (`setPassword`). Dacă parola introdusă este corectă, funcția afișează pe ecranul LCD mesajul "Acces Deblocat!", deblochează încuietoarea și activează LED-ul verde pentru a indica că accesul este permis.

```
def checkPassword(password):
    global failed_attempts
    RLed.value(0)
    if password == setPassword:
        lcd.clear()
        lcd.move_to(0, 0)
        lcd.putstr("Acces Deblocat!")
        lock.value(0)
        GLed.value(1)
        utime.sleep(2)
        lock.value(1)
        lcd.clear()
        lcd.putstr("Card sau pin:")
        GLed.value(0)
        failed_attempts = 0
```



În caz contrar, dacă parola este incorectă, funcția afișează "Acces Respins!", activează LED-ul roșu, buzzer-ul și așteaptă 2 secunde după care acestea sunt dezactivate.



```
else:  
    lcd.clear()  
    lcd.move_to(0, 0)  
    lcd.putstr("Acces Respins!")  
    buzzer.value(1)  
    RLed.value(1)  
    utime.sleep(2)  
    buzzer.value(0)  
    RLed.value(0)
```

După dezactivarea lor, pe ecran se afișează mesaje pentru a indica că PIN-ul introdus este incorrect și că utilizatorul trebuie să încerce din nou, astfel numărul încercărilor rămase crescând cu 1.



```
lcd.putstr("PIN Incorrect")
lcd.move_to(0, 1)
lcd.putstr("Incearca din nou")
utime.sleep(2)
lcd.clear()
lcd.putstr("Introduceti")
lcd.move_to(0, 1)
lcd.putstr("parola:")
failed_attempts += 1
```



Dacă numărul de încercări gresite depășește limita de 3, microcontroler-ul se va reseta și programul se va închide.



```

if failed_attempts >= max_attempts:
    lcd.clear()
    lcd.move_to(0, 0)
    lcd.putstr("Prea multe")
    lcd.move_to(0, 1)
    lcd.putstr("pin-uri gresite!")
    utime.sleep(2)
    machine.reset()

```

În terminalul editorului, la fiecare rulare a codului se va afișa un mesaj pentru introducerea parolei, precum și valoarea variabilei pentru tasta apăsată de utilizator. Acesta este un mod util de a monitoriza și de a verifica ce taste au fost apăsate pentru a efectua ulterior verificări sau acțiuni în funcție de aceste apăsări.

```

Shell ✘
>>> %Run -c $EDITOR_CONTENT
Introduceți parola:
Tastă apasată: 1
Tastă apasată: 2
Tastă apasată: 3
Tastă apasată: 4

```

4.3. Testarea generală a dispozitivului

Autentificarea cu carduri rfid a demonstrat o detectare rapidă și precisă, iar procesul de autentificare prin tastarea codurilor pin s-a dovedit la fel de eficient și securizat. Ecranul LCD a furnizat în mod clar și prompt mesajele utilizatorului, în timp ce led-urile și dispozitivul sonor(buzzer) au oferit indicii vizuale și auditive privind statutul accesului. De asemenea, controlul accesului asupra încuietorii a funcționat conform implementării, asigurându-se că doar utilizatorii autorizați au avut acces la spațiul securizat.

Concluzii

În cadrul acestui proiect, s-a urmărit dezvoltarea și implementarea unui sistem de verificare și control cu ajutorul unei autentificări multiple, care să ofere o soluție complexă și eficientă pentru gestionarea accesului în spații securizate. Scopul acestei lucrări a fost și dezvoltarea unor comenzi analizate și a unor interacțiuni între microcontroller-ul Raspberry Pi Pico W și componente interconectate cu acesta. Proiectul utilizează o încuietoare electrică pentru a controla accesul în zonele restricționate, astfel doar persoanele autorizate având acces. Sistemul de blocare/deblocare este controlat cu ajutorul microcontroller-ului care comunică cu modulul RFID, tastatura keypad 3x4, modulul releu cu un singur canal, ecranul LCD, buzzer-ul și LED-urile. Modulul RFID a oferit o metodă rapidă și sigură de autentificare a utilizatorilor, eliminând necesitatea metodelor tradiționale sau a codurilor PIN nesigure. Pentru autentificare multiplă s-a folosit o tastatură membrană keypad 3x4, permitând astfel utilizatorilor să introducă un cod PIN unic pentru a accesa zona securizată. Această autentificare multiplă a crescut nivelul de securitate și a redus riscul accesului neautorizat. Comunicarea cu utilizatorul a fost realizată prin intermediul ecranului LCD, acesta afișând mesaje și informații cu privire la starea sistemului. Un buzzer a fost integrat pentru a oferi feedback auditiv în momentul în care un acces a fost permis sau respins, iar led-urile au fost utilizate pentru a furniza informații suplimentare despre starea verificării accesului. Pentru testarea sistemului, a fost utilizat mediul de dezvoltare Thonny împreună cu limbajul de programare MicroPython, permitând simularea și monitorizarea comportamentului sistemului într-un mediu controlat. Acest lucru a permis depistarea și remedierea oricărei erori sau probleme înainte de a implementa sistemul într-un mediu real.

În ceea ce privește motivul alegerii acestei teme, acesta a fost relevanța tehnologică privind securitatea și controlul accesului, dar și aprofundarea cunoștințelor tehnice și dezvoltarea abilităților practice.

Direcții viitoare de dezvoltare

Din punct de vedere al actualizării și dezvoltării sistemului, acesta poate fi îmbunătățit atât pe partea resurselor hardware, cât și din perspectiva software. Proiectul poate fi dezvoltat prin extinderea funcționalităților și integrarea unor noi componente cum ar fi camere video pentru accesul prin înregistrare vizuală, senzori pentru amprente digitale sau recunoaștere facială pentru o autentificare biometrică. Din perspectiva resurselor software, lucrarea poate fi extinsă prin adăugarea unui server web pentru gestionarea utilizatorilor, cardurilor RFID și a codurilor PIN. Acestea ar permite administratorilor să adauge sau să eliminate utilizatori, să actualizeze parole și să monitorizeze activitatea de acces.

Bibliografie

- [1] “Embedded systems,” <https://www.heavy.ai/technical-glossary/embedded-systems>, 2022, Ultima accesare: 30.08.2023.
- [2] L. P. Kaelbling, *Learning in Embedded Systems*, 1993.
- [3] E. Fahad, “Biometric door lock project using raspberry pi pico,” <https://www.electronicclinic.com/raspberry-pi-pico-fingerprint-door-lock-project/>, 2023.
- [4] N. B. M. Z. M. Z. S. Amir Hifzan Azhar, Mohd Fairuz Iskandar Othman, “Implementation of home security motion detector using raspberry pi and pir sensor,” *ournal of Advanced Computing Technology and Application (JACTA)*, vol. 3, no. 2, 2021.
- [5] N. H. Tollervey, *Programming with MicroPython*, 2017.
- [6] “Rpi-pico-i2c-lcd,” <https://github.com/T-622/RPI-PICO-I2C-LCD>, 2021, Ultima accesare: 25.08.2023.
- [7] “Micropython:mfrc522 rfid module,” <https://techtotinker.com/2021/09/026-esp32-micropython-mfrc522-rfid-module/>, 2021, Ultima accesare: 27.08.2023.
- [8] “Raspberry pi pico w,” <https://datasheets.raspberrypi.com/picow/pico-w-datasheet.pdf>, 2023, Ultima accesare: 20.08.2023.
- [9] “Rfid based door lock control system using raspberry pi pico,” <https://iotprojectsideas.com/rfid-based-door-lock-control-system-using-raspberry-pi-pico/>, 2023, Ultima accesare: 02.09.2023.
- [10] “How to interface i2c lcd using raspberry pi pico,” <https://myengineeringstuffs.com/2023/02/how-to-interface-i2c-lcd-using-raspberry-pi-pico/>, 2023, Ultima accesare: 27.08.2023.
- [11] “Understanding how a single channel relay module works and how to use it with arduino to control ac loads,” <https://circuitdigest.com/microcontroller-projects/interface-single-channel-relay-module-with-arduino>, 2023.
- [12] “keypad-interfacing-and-authentication-using-raspberry-pi-pico,” <https://myengineeringstuffs.com/2023/02/keypad-interfacing-and-authentication-using-raspberry-pi-pico/>, 2023, Ultima accesare: 25.08.2023.

Anexe

Anexa 1. Codul în MicroPython

```

1  from mfrc522 import MFRC522
2  import utime
3  from machine import Pin
4  import machine
5  from machine import I2C
6  from lcd_api import LcdApi
7  from pico_i2c_lcd import I2cLcd
8
9  lock =Pin(28,Pin.OUT)
10 GLed =Pin(19,Pin.OUT)
11 buzzer = Pin(27, Pin.OUT)
12 RLed =Pin(18,Pin.OUT)
13
14 lock.value(1)
15 buzzer.value(0)
16 RLed.value(0)
17 GLed.value(0)
18
19 I2C_ADDR      = 0x27
20 I2C_NUM_ROWS  = 2
21 I2C_NUM_COLS = 16
22
23 i2c = I2C(0, sda=machine.Pin(0), scl=machine.Pin(1), freq=400000)
24 lcd = I2cLcd(i2c, I2C_ADDR, I2C_NUM_ROWS, I2C_NUM_COLS)
25
26 keyPad =[['1', '2', '3'],
27           ['4', '5', '6'],
28           ['7', '8', '9'],
29           ['*', '0', '#']]
30
31 rowPins = [15,14,13,12]
32 colPins = [11,10,9]
33
34 colValue = []
35 rowValue = []
36
37 password = []
38 setPassword = ['1','2','3','4']
39
40 for i in range(0, 4):
41     rowValue.append(Pin(rowPins[i], Pin.OUT))
42     rowValue[i].value(1)
43 for i in range(0, 3):
44     colValue.append(Pin(colPins[i], Pin.IN, Pin.PULL_DOWN))
45     colValue[i].value(0)
46
47
48 def checkKeyPress():

```

```
49     for row in range(4):
50         for col in range(3):
51             rowValue[row].high()
52             if colValue[col].value() == 1:
53                 print("Tastă apasată:", keyPad[row][col])
54                 key_press = keyPad[row][col]
55                 utime.sleep(0.3)
56                 password.append(key_press)
57             if len(password) == 4:
58                 checkPassword(password)
59                 for x in range(0, 4):
60                     password.pop()
61             rowValue[row].low()
62
63
64 failed_attempts = 0
65 max_attempts = 3
66
67 def checkPassword(password):
68     global failed_attempts
69     RLed.value(0)
70     if password == setPassword:
71         lcd.clear()
72         lcd.move_to(0, 0)
73         lcd.putstr("Acces Deblocat!")
74         lock.value(0)
75         GLed.value(1)
76         utime.sleep(2)
77         lock.value(1)
78         lcd.clear()
79         lcd.putstr("Card sau pin:")
80         GLed.value(0)
81         failed_attempts = 0
82     else:
83         lcd.clear()
84         lcd.move_to(0, 0)
85         lcd.putstr("Acces Respins!")
86         buzzer.value(1)
87         RLed.value(1)
88         utime.sleep(2)
89         buzzer.value(0)
90         RLed.value(0)
91         lcd.clear()
92         lcd.putstr("PIN Incorrect")
93         lcd.move_to(0, 1)
94         lcd.putstr("Incearca din nou")
95         utime.sleep(2)
96         lcd.clear()
97         lcd.putstr("Introduceti")
98         lcd.move_to(0, 1)
99         lcd.putstr("parola:")
100        failed_attempts += 1
101        if failed_attempts >= max_attempts:
```

```

102         lcd.clear()
103         lcd.move_to(0, 0)
104         lcd.putstr("Prea multe")
105         lcd.move_to(0, 1)
106         lcd.putstr("pin-uri gresite!")
107         utime.sleep(2)
108         machine.reset()
109
110
111     print("Introduceti parola:")
112
113     def uidToString(uid):
114         mystring = ""
115         for i in uid:
116             mystring = "%02X" % i + mystring
117         return mystring
118
119     rc522 = MFRC522(spi_id=0, sck=6, miso=4, mosi=7, cs=5, rst=22)
120
121     lcd.clear()
122     lcd.move_to(0, 0)
123     lcd.putstr("Proiect")
124     utime.sleep(3)
125     lcd.clear()
126     lcd.putstr("Card sau pin:")
127
128     while True:
129         checkKeyPress()
130         (stat, tag_type) = rc522.request(rc522.REQALL)
131
132         if stat == rc522.OK:
133             (status, raw_uid) = rc522.SelectTagSN()
134             if stat == rc522.OK:
135                 rfid_data = "{:02x}{:02x}{:02x}{:02x}".format(raw_uid[0], raw_uid[1],
136 # print("Card detectat! Adresa: {}".format(rfid_data))
137
138             if rfid_data == "739cd1aa":
139
140                 lcd.clear()
141                 lcd.move_to(0, 0)
142                 lcd.putstr("RFID corect")
143                 lcd.move_to(0, 1)
144                 lcd.putstr("Deblocat!")
145                 lock.value(0)
146                 GLed.value(1)
147                 utime.sleep(5)
148                 lcd.clear()
149                 lcd.putstr("Card sau pin:")
150                 lock.value(1)
151                 GLed.value(0)
152
153
154     else:

```

```
155
156         lcd.move_to(0, 0)
157         lcd.clear()
158         lcd.putstr("RFID gresit")
159         lcd.move_to(0, 1)
160         lcd.putstr("Respins!")
161         buzzer.value(1)
162         RLed.value(1)
163         utime.sleep(3)
164         lcd.clear()
165         lcd.putstr("Card sau pin:")
166         buzzer.value(0)
167         RLed.value(0)
```