Sistem de acces cu RFID

Claudiu Acosti
Facultatea de Sisteme Informatice şi Securitate Cibernetică
Academia Tehnică Militară „Ferdinand I”
Bucureşti, România
claudiu.acosti@mta.ro

Cristina Lupescu
Facultatea de Sisteme Informatice şi Securitate Cibernetică
Academia Tehnică Militară „Ferdinand I”
Bucureşti, România
cristina.lupescu@mta.ro

Mircea Ivescu
Facultatea de Sisteme Informatice şi Securitate Cibernetică
Academia Tehnică Militară „Ferdinand I”
Bucureşti, România
mircea.ivescu@mta.ro

Bianca Ciobanu
Facultatea de Sisteme Informatice şi Securitate Cibernetică
Academia Tehnică Militară „Ferdinand I”
Bucureşti, România
bianca.ciobanu@mta.ro

***Rezumat*—Acest proiect prezintă dezvoltarea unui sistem electronic inteligent de control al accesului, realizat pe platforma FRDM-KL25Z și bazat pe identificare prin radiofrecvență (RFID). Sistemul utilizează un modul RFID pentru citirea și autentificarea cardurilor, completat de o tastatură 4×4 pentru introducerea unui cod PIN secundar, crescând astfel nivelul de securitate printr-o verificare în doi pași. Cifrele introduse de utilizator prin tastatură sunt afișate în timp real pe un ecran OLED, care este folosit și pentru prezentarea mesajelor de stare și a interfeței cu utilizatorul, facilitând operarea și diagnosticarea sistemului. Două LED-uri asigură semnalizarea vizuală rapidă asupra validității autentificării (acces permis / acces refuzat). Mecanismul fizic de blocare este implementat cu ajutorul unui electromagnet, activat numai după validarea cu succes a cardului RFID și a codului PIN.**

Pentru extinderea funcționalităților, proiectul include un modul Wi-Fi, ce permite transmiterea datelor către o rețea locală sau infrastructură cloud pentru monitorizarea accesului în timp real, precum și un modul microSD pentru stocarea locală a logurilor de evenimente. Integrarea acestor componente conduce la un sistem modular, scalabil și eficient energetic, reprezentând o soluție modernă și sigură de control al accesului pentru aplicații rezidențiale și industriale. Pentru vizualizarea proiectului prezentat se poate accesa https://github.com/Claudiu203/Sistem-access-RFID.

***Index Terms*—RFID, controlul accesului, sisteme embedded, FRDM-KL25Z, securitate.**

Acronim	Denumire
RFID	Radio Frequency Identification
PIN	Personal Identification Number
OLED	Organic Light Emitting Diode
LED	Light Emitting Diode
MCU	Microcontroller Unit
SPI	Serial Peripheral Interface
I2C	Inter-Integrated Circuit
UART	Universal Asynchronous Receiver-Transmitter
GPIO	General Purpose Input/Output
UID	Unique Identifier
SD	Secure Digital
Wi-Fi	Wireless Fidelity
FRDM	Freedom Development Platform
MOSFET	Metal-Oxide-Semiconductor Field-Effect Transistor
SysTick	System Timer Tick

Tabela I
LISTA ACRONIMELOR UTILIZATE

I. Introducere

Sistemele moderne de control al accesului reprezintă o componentă esențială în creșterea nivelului de securitate pentru clădiri, laboratoare, zone industriale sau spații rezidențiale. În contextul dezvoltării accelerate a tehnologiilor embedded și IoT, soluțiile de identificare inteligentă devin tot mai accesibile, mai flexibile și mai sigure. Una dintre tehnologiile utilizate pe scară largă este identificarea prin radiofrecvență (RFID), care permite autentificarea rapidă și fără contact a utilizatorilor, asigurând un nivel ridicat de confort și fiabilitate.

Proiectul de față propune realizarea unui sistem electronic integrat de control al accesului utilizând platforma FRDM-KL25Z, un microcontroler performant și versatil, potrivit aplicațiilor embedded de nivel mediu-complex. Sistemul combină autentificarea pe bază de card RFID cu introducerea unui cod PIN prin intermediul unei tastaturi 4×4, asigurând un mecanism de securitate în doi pași. Pentru interacțiunea cu utilizatorul, un afișaj OLED este utilizat atât pentru vizualizarea în timp real a cifrelor introduse, cât și pentru afișarea mesajelor și stărilor sistemului.

Elementele hardware auxiliare, precum LED-urile de semnalizare și electromagnetul utilizat pentru mecanismul de blocare, completează partea funcțională a sistemului, oferind feedback vizual și acționare fizică a ușii. În plus, integrarea unui modul Wi-Fi permite transmiterea datelor de acces către o rețea sau un server extern, facilitând monitorizarea de la distanță, iar modulul microSD oferă posibilitatea stocării locale a logurilor și a evenimentelor de securitate.

Prin combinația acestor componente, proiectul demonstrează modul în care un sistem embedded poate implementa o soluție modernă, sigură și extensibilă de control al accesului, adaptabilă unei game largi de aplicații practice.

A. Contextul general al temei

Controlul accesului în spații securizate reprezintă o necesitate tot mai importantă în contextul creșterii cerințelor de securitate fizică. Metodele tradiționale bazate pe chei mecanice sau cartele simple prezintă limitări semnificative, precum riscul de pierdere, copiere sau utilizare neautorizată. În plus, aceste soluții nu oferă un mecanism eficient de monitorizare și nici un feedback clar către utilizator.

În acest context, sistemele embedded de control al accesului, bazate pe tehnologii fără contact precum RFID și autentificare suplimentară prin cod PIN, devin soluții moderne, flexibile și scalabile. Proiectul de față se încadrează în această categorie, propunând o implementare practică a unui sistem de acces inteligent, realizat pe platforma FRDM-KL25Z.

B. Motivația alegerii proiectului

Alegerea acestui proiect a fost determinată de dorința de a realiza un sistem embedded complet, care să integreze mai multe tipuri de interfețe hardware și protocoale de comunicație. Sistemul combină comunicații SPI (pentru RFID), I2C (pentru OLED), GPIO (pentru tastatură, LED-uri, buton și electromagnet) și mecanisme de temporizare prin SysTick.

Proiectul oferă o imagine de ansamblu asupra modului în care un microcontroler poate coordona simultan mai multe periferice și poate implementa o logică de securitate reală, utilizată în aplicații de control al accesului folosind exclusiv placuta frdm-kl25z.

C. Utilitatea soluției propuse

Soluția propusă automatizează procesul de autentificare și acces, reducând intervenția umană directă și crescând nivelul de securitate. Sistemul permite accesul doar în urma validării a doi factori: cardul RFID și codul PIN introdus de utilizator. Feedback-ul este oferit prin LED-uri și mesaje afișate pe ecranul OLED, ceea ce îmbunătățește experiența de utilizare și claritatea interacțiunii.

Prin integrarea modulelor Wi-Fi și microSD, sistemul poate fi extins pentru monitorizarea accesului de la distanță și stocarea locală a evenimentelor, ceea ce îl face potrivit pentru aplicații reale.

D. Domenii de aplicare

Sistemul dezvoltat poate fi adaptat pentru multiple scenarii practice, precum:

- controlul accesului în clădiri de birouri sau instituții publice;
- acces securizat în laboratoare universitare sau industriale;
- sisteme de acces pentru campusuri, cămine sau zone rezidențiale;
- integrarea în soluții de tip smart home sau smart building.

E. Exemple de dispozitive similare

Sistemele comerciale moderne de control al accesului utilizează frecvent autentificarea prin card RFID sau tag NFC, combinată cu introducerea unui cod PIN pentru un nivel suplimentar de securitate. În mediul educațional și de prototipare, platforme precum Arduino, ESP32 sau plăci din seria NXP FRDM sunt utilizate pentru dezvoltarea de sisteme similare, care includ cititoare RFID, tastaturi matriceale, afișaje și mecanisme electromecanice de blocare.

F. Obiectivele proiectului

Principalele obiective ale proiectului sunt:

- proiectarea și realizarea unui sistem embedded de control al accesului bazat pe RFID și cod PIN;
- integrarea mai multor interfețe hardware (SPI, I2C, GPIO) într-o aplicație unitară;
- implementarea unui mecanism de autentificare în doi pași (card + PIN);
- afișarea în timp real a informațiilor relevante pe un ecran OLED;
- realizarea unui sistem de semnalizare vizuală cu LED-uri pentru starea accesului;
- controlul unui electromagnet pentru blocarea/deblocarea mecanismului de acces;
- utilizarea temporizărilor neblocante prin intermediul timerului SysTick;
- posibilitatea extinderii sistemului prin conectivitate Wi-Fi și stocare pe microSD.

II. Arhitectura și designul sistemului

Arhitectura sistemului de control al accesului este concepută într-o manieră modulară, pentru a facilita integrarea mai multor componente hardware distincte și gestionarea lor printr-un flux logic bine definit. Sistemul este construit în jurul microcontrolerului FRDM-KL25Z, care acționează ca unitate centrală de control și coordonează comunicația dintre modulele periferice prin interfețe precum SPI, I2C, UART și GPIO.

Structura aplicației este organizată pe straturi logice, incluzând: *nivelul hardware*, *nivelul de abstractizare a driverelor*, *modulul de logică aplicativă* și *interfața cu utilizatorul*. Această abordare permite scalabilitate crescută, mentenanță ușoară și posibilitatea extinderii ulterioare cu funcționalități suplimentare.

A. Componentele majore ale sistemului

Sistemul este alcătuit din următoarele componente principale:

- **Placa de dezvoltare FRDM-KL25Z** – unitatea centrală de control (MCU) care coordonează toate modulele hardware și execută logica sistemului de acces;
- **Modulul RFID MFRC522** – utilizat pentru citirea cardurilor RFID și obținerea identificatorului unic (UID) al utilizatorului;
- **Tastatura matricială 4×4** – permite introducerea codului PIN, reprezentând al doilea factor de autentificare;
- **Afișaj OLED SSD1306** – interfață vizuală pentru afișarea mesajelor de stare, a instrucțiunilor și a PIN-ului introdus;

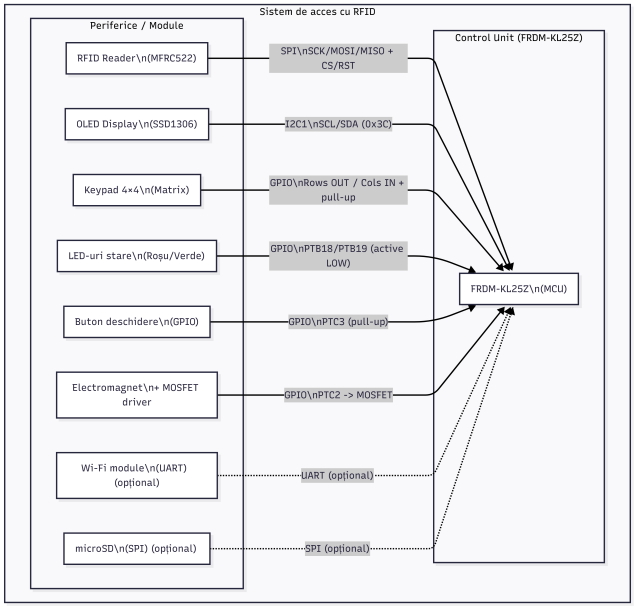

Figura 1. Diagramă de componente a arhitecturii hardware a sistemului de control al accesului bazat pe RFID

- **Electromagnet de blocare** – elementul de acționare mecanică ce permite blocarea și deblocarea ușii;
- **Driver cu MOSFET pentru electromagnet** – circuit de comandă care permite controlul unei sarcini inductive de putere prin intermediul unui pin GPIO al microcontrolerului;
- **LED-uri de stare (roșu și verde)** – oferă feedback vizual rapid privind starea sistemului (acces permis / acces refuzat);
- **Buton fizic de deschidere** – permite acționarea manuală a mecanismului de acces în anumite scenarii;
- **Modul Wi-Fi** – asigură posibilitatea transmiterii datelor de acces către o rețea sau un server extern pentru monitorizare;
- **Modul microSD** – utilizat pentru stocarea locală a logurilor de acces și a evenimentelor generate de sistem.

B. Interacțiunea dintre module

Fiecare componentă hardware comunică cu microcontrolerul printr-o interfață dedicată:

- RFID MFRC522 – interfață **SPI**;
- microSD – interfață **SPI**;
- OLED – interfață **I2C** (sau SPI, în funcție de versiune);
- Tastatură 4×4 – **GPIO** configurat în mod scan matrix;
- Electromagnet – **GPIO + driver MOSFET**;
- Wi-Fi – interfață **UART**.

Fluxul general al sistemului urmează o mașină de stări ce gestionează citirea cardului, introducerea PIN-ului, validarea și acționarea electromagnetului.

C. Diagramă bloc a arhitecturii sistemului

În Figura 1 este prezentată o schemă bloc ce ilustrează conexiunile dintre module.

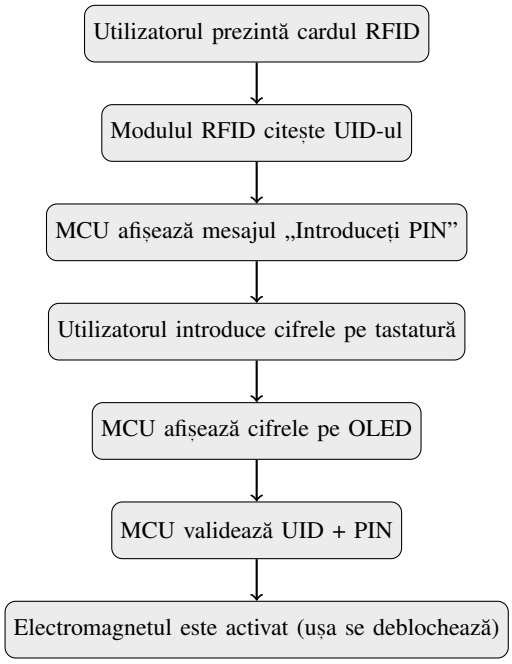

Figura 2. Flux compact al procesului de autentificare RFID + PIN

D. Diagramă de secvență a procesului de autentificare

Pentru a ilustra interacțiunea dintre module în timpul autentificării, este prezentată următoarea diagramă de secvență simplificată:

III. Integrarea modulului RFID MFRC522 cu platforma FRDM-KL25Z

Identificarea utilizatorilor în cadrul sistemului de control al accesului este realizată cu ajutorul modulului RFID MFRC522, un cititor RFID de joasă frecvență, compatibil cu carduri pasive, utilizat pe scară largă în aplicații embedded. Modulul permite autentificarea rapidă și fără contact, fiind potrivit pentru sisteme de acces datorită costului redus, consumului scăzut de energie și ușurinței în integrare.

A. Interfața de comunicație și conexiunile hardware

Comunicarea dintre microcontrolerul FRDM-KL25Z și modulul MFRC522 se realizează prin interfața **SPI (Serial Peripheral Interface)**, aleasă pentru fiabilitatea și viteza sa. Conexiunile hardware implementate în cadrul proiectului sunt prezentate mai jos:

- **SCK** (Serial Clock) – conectat la pinul **PTC5**, configurat ca SPI clock;
- **MOSI** (Master Out Slave In) – conectat la pinul **PTC6**, utilizat pentru transmiterea datelor către modulul RFID;
- **MISO** (Master In Slave Out) – conectat la pinul **PTC7**, utilizat pentru recepția datelor de la modulul RFID;
- **CS (Chip Select / SDA)** – conectat la pinul **PTC4**, configurat ca GPIO și controlat manual;
- **RST** (Reset) – conectat la pinul **PTA1**, utilizat pentru resetarea modulului MFRC522;
- **VCC** – alimentare la **3.3V**, conform cerințelor modulului;

- **GND** – masă comună cu microcontrolerul.

Linia CS nu este gestionată automat de perifericul SPI al microcontrolerului, ci este controlată manual din software, fiind activată (nivel logic LOW) strict pe durata transferurilor SPI. Această abordare oferă un control precis asupra comunicației și elimină erorile cauzate de sincronizarea incorectă a semnalului de selecție.

B. Configurarea modulului RFID

După realizarea conexiunilor hardware, modulul MFRC522 este inițializat software printr-o secvență de configurări recomandate în datasheet. Acestea includ setarea timerelor interne, a modului de transmisie și activarea antenei RF. Comunicația SPI este configurată în **Mode 0** (CPOL = 0, CPHA = 0), iar frecvența este menținută sub 1 MHz pentru a asigura stabilitatea comunicației, în special în cazul utilizării firelor de tip jumper.

Resetarea modulului se realizează printr-un pin GPIO dedicat, asigurând inițializarea corectă la pornirea sistemului.

C. Probleme întâmpinate în implementare

În procesul de dezvoltare au fost identificate mai multe dificultăți practice. Una dintre principalele probleme a fost legată de gestionarea semnalului Chip Select. Utilizarea inițială a controlului automat al CS de către perifericul SPI a condus la lipsa răspunsurilor valide din partea modulului RFID. Această problemă a fost rezolvată prin controlul manual al CS ca pin GPIO.

O altă problemă a fost reprezentată de detecțiile false ale cardurilor RFID. Inițial, sistemul interpreta greșit anumite flaguri de întrerupere, ceea ce ducea la semnalarea prezenței unui card chiar și în absența acestuia. Soluția adoptată a constat în verificarea explicită a existenței unui răspuns valid în FIFO-ul modulului MFRC522, conform protocolului REQA.

D. Detecția cardului și semnalizarea accesului

Detecția unui card RFID se realizează prin trimiterea comenzii **REQA**, utilizată pentru identificarea cardurilor aflate în apropierea antenei. În momentul în care modulul RFID primește un răspuns valid, microcontrolerul interpretează acest eveniment ca o autentificare inițială reușită.

Ca feedback vizual pentru utilizator, LED-ul verde integrat pe placa FRDM-KL25Z este aprins, indicând detectarea cardului. Simultan, electromagnetul care controlează mecanismul fizic de acces este activat. Atât LED-ul verde, cât și electromagnetul rămân active pentru o durată de **5 secunde**, după care sistemul revine automat în starea de repaus, cu accesul blocat.

Această temporizare contribuie la creșterea siguranței sistemului și previne menținerea accesului deschis pentru o perioadă nedeterminată.

IV. Integrarea tastaturii 4×4 pentru introducerea codului PIN

Pentru creșterea nivelului de securitate, sistemul implementează un al doilea factor de autentificare prin intermediul unei tastaturi matriceale 4×4, utilizată pentru introducerea unui cod PIN numeric. Această metodă adaugă un nivel suplimentar de protecție față de autentificarea exclusivă prin card RFID.

A. Conectarea hardware

Tastatura este organizată sub forma unei matrice de 4 rânduri și 4 coloane, fiecare linie fiind conectată la pini GPIO ai microcontrolerului FRDM-KL25Z:

- **Rânduri (outputs):** PTD5, PTD0, PTD2, PTD3
- **Coloane (inputs cu pull-up):** PTD7, PTA13, PTE0, PTE1

Rândurile sunt configurate ca ieșiri digitale, iar coloanele ca intrări cu rezistențe interne de pull-up activate. Astfel, în starea de repaus, toate coloanele se află în nivel logic HIGH.

B. Principiul de funcționare

Citirea tastaturii se face prin tehnica *row scanning*. Pe rând, fiecare linie este adusă la nivel logic LOW, iar coloanele sunt citite pentru a detecta dacă una dintre ele devine LOW, semn că tasta corespunzătoare intersecției rând–coloană este apăsată.

Pentru eliminarea efectului de *debounce*, este introdus un mic timp de întârziere software după detectarea unei apăsări, urmat de așteptarea eliberării tastei înainte de a continua scanarea.

C. Maparea tastelor și logica PIN

Fiecărei combinații rând–coloană îi corespunde un caracter (0–9, A–F). În cadrul aplicației:

- Tastele numerice sunt folosite pentru introducerea PIN-ului
- Tasta **A** are rol de **RESET** (șterge PIN-ul introdus)
- Tasta **C** are rol de **ENTER** (confirmă PIN-ul)

PIN-ul este stocat într-un buffer de 4 caractere și comparat cu un cod prestabilit în firmware. În funcție de rezultat, sistemul afișează un mesaj corespunzător pe OLED și comandă LED-urile și electromagnetul.

V. Interfața de afișare OLED (SSD1306)

Pentru interacțiunea vizuală cu utilizatorul, sistemul utilizează un afișaj OLED monocrom controlat de driverul SSD1306. Acesta este folosit pentru afișarea codului PIN introdus, a mesajelor de stare și a feedback-ului sistemului.

A. Conectarea hardware și interfața de comunicație

Afișajul OLED comunică cu microcontrolerul prin magistrala **I2C1**, utilizând următorii pini:

- **SCL** – PTC10
- **SDA** – PTC11

Adresa I2C utilizată este **0x3C**. Liniile sunt configurate în mod *open-drain*, conform cerințelor protocolului I2C.

B. Inițializarea afișajului

La pornirea sistemului, afișajul este inițializat printr-o secvență de comenzi care configurează:

- modul de adresare a memoriei grafice
- contrastul
- orientarea imaginii
- activarea sursei interne de tensiune pentru panou

După inițializare, ecranul este șters complet.

C. Afișarea informațiilor

Afișajul este utilizat pentru:

- afișarea textului **„PIN:”** urmat de caractere mascate sau cifre
- afișarea mesajelor temporare: **„PIN OK”** sau **„PIN WRONG”**

Mesajele temporare sunt afișate pentru o durată limitată, gestionată printr-un timer software bazat pe SysTick, după care sunt șterse automat fără a afecta restul interfeței.

VI. Semnalizarea vizuală cu LED-uri

Sistemul utilizează două LED-uri pentru semnalizarea rapidă a stării autentificării:

- **LED roșu** – indică starea de repaus / acces blocat
- **LED verde** – indică autentificare reușită

LED-urile sunt conectate la pinii PTB18 (roșu) și PTB19 (verde) și sunt configurate în mod *active LOW*. Astfel, aprinderea LED-ului se face prin setarea pinului la nivel logic LOW.

După o autentificare reușită, LED-ul verde rămâne aprins timp de 3 secunde, temporizare realizată cu ajutorul unui contor incrementat de întreruperea SysTick.

VII. Controlul electromagnetului de blocare

Mecanismul fizic de blocare a ușii este realizat cu ajutorul unui electromagnet comandat de microcontroler.

A. Conectarea hardware

Electromagnetul este controlat prin pinul **PTC2**, conectat la un tranzistor de putere (MOSFET) care permite alimentarea sarcinii de curent mai mare. Această configurație protejează microcontrolerul și permite comanda unei sarcini inductive.

B. Modul de operare

Electromagnetul este activat simultan cu LED-ul verde, în cazul unei autentificări valide. El rămâne activ pe durata ferestrei de acces (3 secunde), după care este dezactivat automat. Sincronizarea este realizată prin același mecanism de temporizare utilizat pentru LED-uri.

VIII. Butonul fizic de deschidere

Pe lângă autentificarea electronică, sistemul include un buton fizic conectat la pinul **PTC3**, configurat ca intrare cu rezistență internă de pull-up.

Apăsarea butonului aduce pinul la nivel logic LOW și este interpretată ca o cerere de deschidere manuală. La detectare, sistemul activează LED-ul verde și electromagnetul pentru aceeași perioadă temporizată, oferind o metodă alternativă de acces (de exemplu pentru personal autorizat).

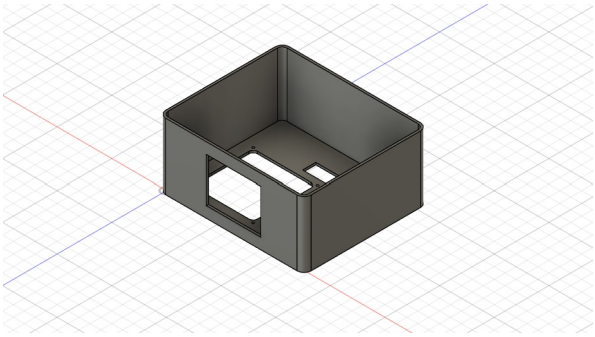

Figura 3. Model 3D al carcasei realizat în Autodesk Fusion 360 pentru integrarea sistemului de control al accesului

IX. Gestionarea timpului cu SysTick

Pentru implementarea temporizărilor fără a bloca execuția principală, sistemul utilizează timerul **SysTick** al microcontrolerului. Acesta generează o întrerupere la fiecare 1 ms, incrementând un contor global de milisecunde.

Această bază de timp este utilizată pentru:

- menținerea LED-ului verde activ pentru o perioadă fixă
- controlul duratei de activare a electromagnetului
- afișarea temporară a mesajelor pe OLED
- implementarea întârzierilor scurte pentru debounce

Această abordare permite realizarea unui sistem reactiv, fără utilizarea buclelor lungi de tip delay blocant.

X. Proiectarea componentelor mecanice în Autodesk Fusion 360

Pe lângă partea electronică și software, proiectul a inclus și realizarea componentelor mecanice necesare montării sistemului de control al accesului. Pentru modelarea 3D a acestor componente a fost utilizat software-ul Autodesk Fusion 360, un mediu profesional de proiectare asistată de calculator (CAD), utilizat pentru dezvoltarea de ansambluri mecanice și prototipuri, cum se poate observa in Figura 3 si Figura 4.

Au fost proiectate elemente precum carcasa principală a sistemului, suporturile pentru modulele electronice (RFID, OLED, tastatură, placă FRDM-KL25Z), precum și elementele de fixare și ghidare a cablurilor. Modelarea 3D a permis verificarea poziționării corecte a componentelor, optimizarea spațiului interior și asigurarea unei integrări mecanice stabile și sigure.

Utilizarea Fusion 360 a facilitat simularea ansamblului complet înainte de realizarea fizică a prototipului, reducând riscul de erori de montaj și permițând ajustări rapide ale designului.

A. Designul interfeței fizice a utilizatorului

O atenție specială a fost acordată zonei de interacțiune cu utilizatorul. Carcasa frontală a fost proiectată pentru a integra cititorul RFID, tastatura pentru introducerea codului PIN și afișajul OLED într-un mod intuitiv și ergonomic.

Dispunerea elementelor a fost gândită astfel încât utilizatorul să poată apropia cardul, introduce codul și vizualiza

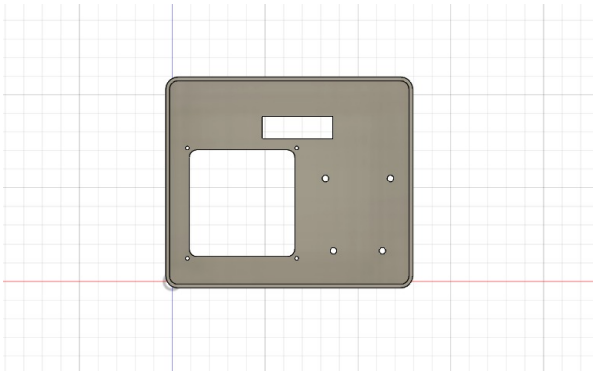

Figura 4. Model 3D al structurii mecanice realizat în Autodesk Fusion 360 pentru integrarea sistemului de control al accesului din fata

Figura 5. Randare ilustrativă a interfeței fizice a sistemului de acces cu RFID și tastatură PIN

mesajele de stare într-o succesiune naturală a acțiunilor. În Figura 5 este prezentată o randare ilustrativă a modului în care este organizată interfața fizică a sistemului de control al accesului.

XI. Fluxul complet de funcționare al sistemului

Funcționarea sistemului poate fi descrisă ca o buclă continuă de monitorizare a intrărilor și actualizare a ieșirilor.

A. Starea de repaus

În mod normal:

- LED-ul roșu este aprins
- electromagnetul este dezactiv

B. Scenariul de autentificare

1) Sistemul detectează apropierea unui card RFID.
2) LED-ul verde și electromagnetul sunt activate temporar.
3) Utilizatorul introduce codul PIN pe tastatură.
4) PIN-ul este afișat pe OLED în timp real.
5) La apăsarea tastei ENTER:
   - dacă PIN-ul este corect → se afișează „PIN OK”, acces permis
   - dacă PIN-ul este greșit → se afișează „PIN WRONG”, acces refuzat

C. Sincronizarea componentelor

Interfața fizică a utilizatorului reprezintă punctul principal de interacțiune dintre sistemul de control al accesului și persoana care solicită accesul. Din acest motiv, proiectarea acestei zone a avut un rol esențial atât din punct de vedere funcțional, cât și ergonomic. Obiectivul a fost realizarea unei interfețe intuitive, ușor de utilizat și clară din punct de vedere vizual, astfel încât utilizatorul să poată parcurge procesul de autentificare într-un mod natural și fără ambiguități.

Carcasa frontală a fost concepută pentru a integra cele trei elemente principale ale interacțiunii cu utilizatorul: cititorul RFID, tastatura pentru introducerea codului PIN și afișajul OLED pentru feedback vizual. Dispunerea acestor componente a fost realizată ținând cont de ordinea logică a pașilor de autentificare. Astfel, zona de apropiere a cardului RFID este poziționată în partea superioară, urmată de afișajul OLED, iar tastatura numerică este amplasată în partea inferioară, într-o zonă ușor accesibilă pentru introducerea codului PIN.

Această organizare verticală reflectă fluxul real de utilizare al sistemului: utilizatorul apropie mai întâi cardul de cititor, apoi privește afișajul pentru instrucțiuni sau confirmări, iar ulterior introduce codul PIN folosind tastatura. Prin această abordare, mișcările utilizatorului sunt naturale, iar interacțiunea cu sistemul devine intuitivă chiar și pentru persoane care nu sunt familiarizate cu dispozitivele electronice.

În proiectarea carcasei s-a acordat o atenție deosebită dimensiunilor și spațiului necesar fiecărei componente. Afișajul OLED necesită o fereastră frontală precis decupată, astfel încât informațiile afișate să fie vizibile fără a expune componentele interne. Tastatura a fost poziționată într-o zonă plană, pentru a asigura apăsarea confortabilă a tastelor, iar zona cititorului RFID a fost lăsată liberă de obstacole pentru a nu afecta câmpul electromagnetic necesar detectării cardurilor.

Din punct de vedere estetic, interfața fizică a fost gândită să aibă un aspect compact și ordonat, cu o separare clară între zonele funcționale. Carcasa oferă protecție mecanică componentelor electronice, ascunzând cablurile și circuitele interne, ceea ce contribuie la un aspect profesional al prototipului. În același timp, designul permite accesul facil la componente pentru mentenanță sau modificări ulterioare.

Ergonomia a fost un alt factor important în procesul de proiectare. Înălțimea și înclinarea panoului frontal au fost alese astfel încât utilizatorul să poată citi ușor mesajele de pe afișaj și să introducă PIN-ul fără efort, indiferent de poziția în care este montat sistemul (de exemplu, pe un perete sau lângă o ușă). Butoanele tastaturii sunt suficient de distanțate pentru a preveni apăsările accidentale, iar feedback-ul vizual oferit de afișaj și LED-uri completează experiența de utilizare.

În Figura 5 este prezentată o randare ilustrativă a modului în care este organizată interfața fizică a sistemului de control al accesului. Această reprezentare evidențiază integrarea componentelor într-un ansamblu coerent, precum și modul în care

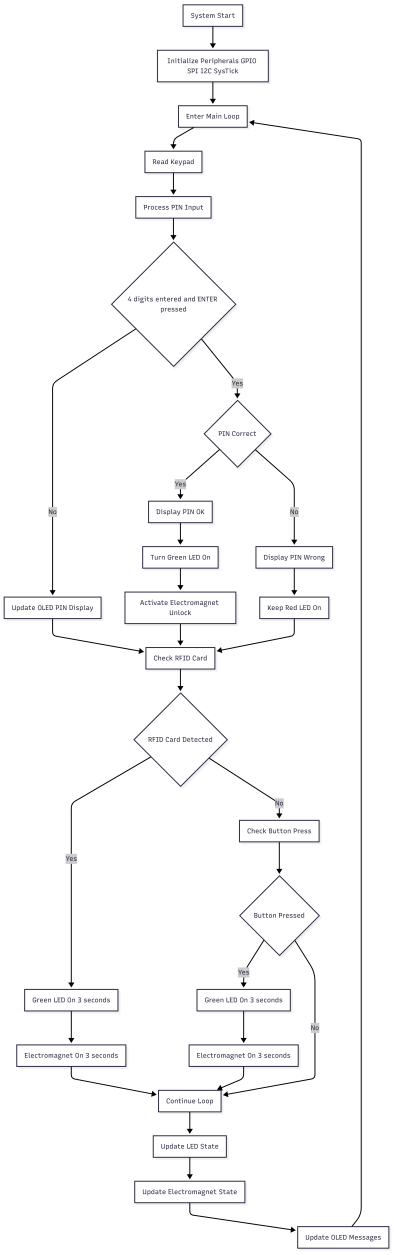

Figura 6. Diagrama de flux a buclei principale a sistemului de control al accesului

utilizatorul interacționează cu dispozitivul în timpul procesului de autentificare.

Pe lângă rolul funcțional, interfața fizică contribuie și la percepția de securitate a sistemului. Un panou clar organizat, cu elemente bine delimitate și feedback vizual constant, inspiră încredere utilizatorului și reduce posibilitatea utilizării greșite a dispozitivului. Astfel, designul interfeței fizice nu este doar un aspect estetic, ci o componentă esențială în asigurarea unei experiențe de utilizare sigure și eficiente.

XII. Modul de comunicație FRDM–Wi-Fi și afișare loguri în interfață web

Această componentă software are rolul de a asigura preluarea mesajelor de stare generate de sistemul implementat pe placa FRDM, transmiterea acestora către un modul Wi-Fi și publicarea lor sub formă de loguri într-o interfață web accesibilă din rețeaua locală.

Comunicarea dintre placa FRDM și modulul Wi-Fi se realizează indirect, prin intermediul unei plăci Arduino, care funcționează ca unitate de interconectare și procesare a mesajelor. Legătura FRDM–Arduino este realizată prin interfață UART, iar Arduino controlează modulul ESP8266 folosind comenzi AT, printr-o a doua interfață serială.

Placa FRDM transmite mesaje text reprezentând rezultatul operațiilor efectuate de sistem, precum validarea unui card RFID sau verificarea unui cod PIN. Aceste mesaje sunt trimise prin UART la un baud rate de 9600 bps și sunt recepționate de Arduino sub formă de șiruri de caractere terminate cu caracter de linie nouă. La recepție, mesajele sunt procesate și stocate într-o structură de tip buffer, care păstrează ultimele evenimente generate de sistem.

Pentru expunerea informațiilor către utilizator, Arduino configurează modulul ESP8266 în mod stație și îl conectează la o rețea Wi-Fi existentă. Ulterior, modulul este configurat să funcționeze ca server TCP/IP pe portul 80, permițând accesarea interfeței web printr-un browser standard. La detectarea unei cereri HTTP, sistemul generează dinamic o pagină HTML care conține logurile curente, afișate sub formă de tabel.

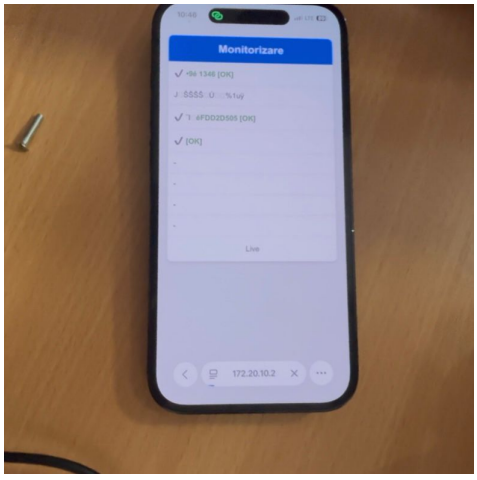

Figura 7. Interfața web pentru monitorizarea în timp real a evenimentelor sistemului

Pagina web este transmisă direct către client prin conexiunea deschisă, folosind comenzi AT de trimitere a datelor. Evenimentele sunt evidențiate vizual pentru a permite identificarea rapidă a stărilor de succes sau eșec. După trimiterea conținutului, conexiunea este închisă, iar sistemul rămâne disponibil pentru cereri ulterioare.

Prin această abordare, sistemul oferă o soluție de monitorizare în timp real, fără a necesita infrastructură suplimentară sau servicii externe, permițând vizualizarea stării sistemului

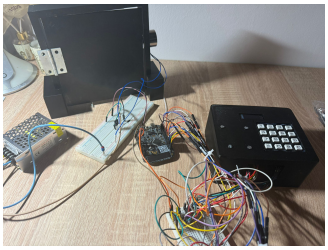

Figura 8. Prototipul fizic al sistemului – vedere frontală

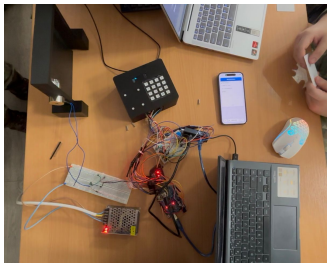

Figura 9. Prototipul fizic – integrarea componentelor hardware

direct dintr-un browser web, utilizând exclusiv comunicație serială și rețea locală Wi-Fi, conform exemplului ilustrat în Figura 7.

XIII. Concluzie asupra integrării sistemului

Integrarea modulelor hardware și software demonstrează realizarea unui sistem embedded complet, capabil să implementeze un mecanism de control al accesului în doi pași. Fiecare componentă contribuie la funcționalitatea globală:

- RFID — identificare fără contact
- Tastatură — autentificare suplimentară prin PIN
- OLED — interfață om–mașină
- LED-uri — feedback vizual instant
- Electromagnet — acționare fizică a mecanismului de acces
- Buton — metodă alternativă de acces

Prin coordonarea acestora prin firmware-ul microcontrolerului FRDM-KL25Z, sistemul obține un echilibru între securitate, fiabilitate și simplitate arhitecturală, reprezentând o soluție eficientă pentru aplicații reale de control al accesului.

Pentru validarea designului mecanic realizat în Autodesk Fusion 360, a fost construit prototipul fizic al sistemului. În figurile următoare este prezentată implementarea reală a sistemului de control al accesului, evidențiind integrarea componentelor electronice în carcasa proiectată.

Referințe

Bibliografie

[1] J. J. Mortensen, M. Gjerding, and K. S. Thygesen, “MyQueue: Task and workflow scheduling system,” *Journal of Open Source Software*, vol. 5, no. 45, p. 1844, 2020.

[2] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[3] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[4] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[5] K. Elissa, “Title of paper if known,” unpublished.

[6] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[7] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[8] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[9] Trace-ID, ”Understanding an RFID tag datasheet.” https://www.trace-id.com/en/understanding-an-rfid-tag-datasheet/