

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



BÁO CÁO ĐỒ ÁN THIẾT KẾ LUẬN LÝ

Đề tài
Ở KHÓA ĐIỆN TỬ

GVHD: Nguyễn Thành Lộc

Thành phố Hồ Chí Minh, 12/2025

Danh sách thành viên và công việc

Họ và tên	MSSV	Nhiệm vụ	Hoàn thành
Dương Khôi Nguyên	2312333	Lên ý tưởng, cấu trúc báo cáo Tổng hợp, chỉnh sửa và hoàn thiện nội dung cuối Hiện thực thao tác và quy trình xử lý dữ liệu đầu vào	100%
Trần Hoàng Bá Huy	2311249	Nghiên cứu và lựa chọn các thiết bị phù hợp Hiện thực tính năng hiển thị và tương tác người dùng Hiện thực, điều chỉnh và sửa lỗi phần cứng	100%
Nguyễn Hảo Khang	2311444	Hiện thực quy trình luận lý Điều chỉnh, tổng hợp mã nguồn Quản lý quy trình làm việc và tiến độ các thành viên	100%



Mục lục

1 Giới thiệu	2
1.1 Tính năng của sản phẩm	2
1.2 Phạm vi đề tài	3
2 Cấu tạo và Nguyên lý hoạt động	4
2.1 Nguyên lý hoạt động	4
2.2 Linh kiện phần cứng	4
2.3 Giải thuật Knutt-Morris-Pratt	9
3 Thiết kế	11
3.1 Khối xử lý trung tâm	11
3.2 Khối giao diện người dùng	12
3.3 Khối truyền động và cảm biến	13
3.4 Khối quản lý năng lượng:	13
4 Hiện thực	15
4.1 Sơ lược thiết kế	15
4.2 Chi tiết các trạng thái	16
4.3 Hiện thực mã nguồn	19
4.4 Sơ đồ máy trạng thái	19
5 Kiểm thử đề tài	21
6 Kết luận	23
6.1 Kết quả đạt được	23
6.2 Khó khăn - hướng giải quyết	24
6.3 Phát triển trong tương lai	25

1 Giới thiệu

Khóa cửa là công cụ hữu dụng nhất trong việc đảm bảo nơi cư trú của một cá nhân an toàn với thế giới bên ngoài. Từ thô sơ đến phức tạp, khóa cửa biến đổi từ những then gỗ đơn giản cho đến hiện tại, trong bối cảnh an ninh và tiện lợi được phép tồn tại song song, các giải pháp khóa cửa thông minh đang dần thay thế các loại khóa cơ truyền thống sử dụng chìa. Đây là lý do nhóm chọn đề tài "**Ô khóa điện tử**"

Dề tài tập trung vào việc nghiên cứu và xây dựng một hệ thống khóa cửa tự động sử dụng vi điều khiển. Sản phẩm sử dụng bo mạch STM32F103C8T6, với họ vi điều khiển lõi Arm® Cortex®-M3 STM32F1 làm đơn vị xử lý trung tâm. Hệ thống được thiết kế để cung cấp một giải pháp an ninh linh hoạt, kết hợp giữa việc xác thực bằng mật khẩu số và khả năng dự phòng bằng chìa khóa cơ.

1.1 Tính năng của sản phẩm

- **Mở khóa bằng mật khẩu:** Người dùng nhập mật khẩu qua một bàn phím. Hệ thống cho phép nhập một lượng tối đa các ký tự và tìm mật khẩu dựa trên những ký tự nhập vào.
 - **Mở khóa bằng phương thức vật lý:** Hệ thống tích hợp một ổ khóa cơ học truyền thống. Khi sử dụng chìa khóa cơ, một cảm biến sẽ được kích hoạt để mở khóa và khởi động lại hệ thống nếu đang bị vô hiệu hóa tạm thời. Ngoài ra, khóa được trang bị một nút bấm ở mặt trong ổ khóa để mở khóa cửa từ bên trong.
 - **Quản lý mật khẩu:** Cho phép người dùng tạo lập và thay đổi mật khẩu bên trong ổ khóa theo các quy trình phổ biến hiện nay.
 - **Cảnh báo an ninh:** Nhập sai mật khẩu nhiều lần liên tiếp, hệ thống sẽ phát cảnh báo và vô hiệu hóa bàn phím, trước khi vô hiệu hóa hoàn toàn bàn phím sau một số lần nhập cũ thẻ và phải sử dụng chìa khóa cơ để mở lại.
 - **Giao diện người dùng:** Thông tin về trạng thái của khóa và mật khẩu đang được nhập sẽ được hiển thị qua một màn hình LED.



1.2 Phạm vi đề tài

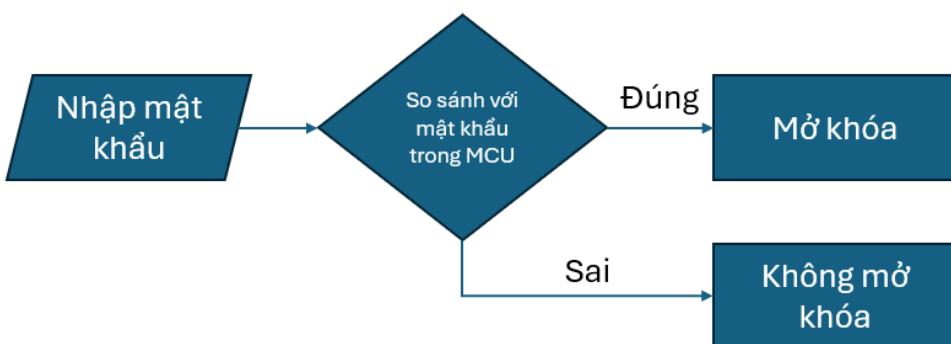
Phạm vi của đề tài được giới hạn trong các khía cạnh kỹ thuật sau:

- **Nền tảng phần cứng:** Thiết kế tập trung vào vi điều khiển STM32F103C8T6. Các linh kiện ngoại vi được lựa chọn cẩn thận bao gồm LCD 16x2 (giao tiếp I²C) , khóa Solenoid 12V LY - 03 , và Keypad 4 × 4.
- **Phạm vi xác thực mật khẩu:** Mật khẩu được lưu có độ dài cố định là bốn ký tự. Người dùng có thể nhập chuỗi dài hơn, cơ chế xác thực chỉ dựa trên việc tìm kiếm chuỗi bốn ký tự này bằng thuật toán Knuth - Morris - Pratt , không sử dụng các phương thức mã hóa phức tạp.
- **Hệ thống cấp nguồn cố định:** Hệ thống sử dụng đồng thời các bộ biến áp để cấp nguồn cho các khối linh kiện khác nhau.
- **Giới hạn trong hiện thực mạch:** Việc sử dụng đồng thời các bộ biến áp trên nền tảng breadboard gây khó khăn trong việc quản lý nhiễu điện từ khi relay đóng ngắt, dễ làm ảnh hưởng đến tính ổn định của vi điều khiển. Ngoài ra, các kết nối bằng dây cắm (jumper) không mang tính bền vững cao, dễ xảy ra tình trạng lỏng mối nối hoặc sụt áp cục bộ khi cung cấp dòng điện lớn cho khóa Solenoid.

2 Cấu tạo và Nguyên lý hoạt động

2.1 Nguyên lý hoạt động

Ổ khóa điện tử cho phép người dùng mở khóa cửa bằng cách sử dụng mật khẩu hoặc sử dụng chìa khóa cơ. Quy trình xử lý đơn giản của ổ khóa được mô tả trong sơ đồ sau:



Hình 1: Sơ đồ hoạt động của ổ khóa điện tử

Người dùng sẽ nhập một chuỗi hai mươi ký tự trong đó có chuỗi con bốn ký tự là mật khẩu của hệ số thập lục phân. Sau đó, vi xử lý trung tâm sẽ tìm kiếm mật khẩu trong chuỗi vừa nhập bằng thuật toán Knutt - Morris - Pratt và so sánh với dữ liệu được lưu trong bộ nhớ của vi. Nếu đúng, vi xử lý trung tâm sẽ gửi tín hiệu để mở chốt khóa và ngược lại. Để thao tác dễ dàng hơn, người sử dụng cũng sẽ được thấy và được cảnh báo các trạng thái của ổ khóa thông qua một màn hình LCD.

2.2 Linh kiện phần cứng

2.2.1 Vi điều khiển STM32F103C8T6

Vi điều khiển STM32F103C8T6 thuộc dòng STM32F1 của STMicroelectronics, là một lựa chọn phổ biến cho các dự án hệ thống nhúng đòi hỏi sự cân bằng giữa hiệu năng, bộ nhớ, và chi phí. Thiết bị được tích hợp lõi Arm® Cortex®-M3 32-bit RISC hiệu năng cao hoạt động ở tần số 72MHz, bộ nhớ nhúng tốc độ cao và có nhiều chân



I/O ngoại vi mở rộng, được kết nối qua hai bus APB. Vi điều khiển đóng vai trò chính trong việc nhận, xử lý và truyền dữ liệu thông qua giao thức GPIO và I²C.

Đặc điểm kỹ thuật:

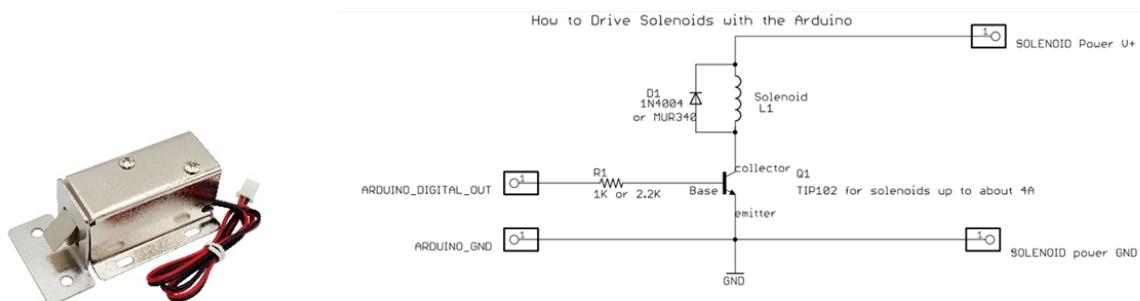
- Lõi xử lý trung tâm: Arm® Cortex®-M3
 - Tần số tối đa 72 MHz, hiệu suất truy cập bộ nhớ đạt 1.25 DMIPS/MHz (Dhrystone 2.1) khi không có chu kỳ đằng chờ.
- Bộ nhớ:
 - Flash: 64KB
 - SRAM: 20KB
- Giao tiếp ngoại vi
 - Tối đa 2 giao diện I²C (hỗ trợ SMBus/PMBus).
 - Tối đa 3 bộ USART (hỗ trợ giao diện ISO 7816, LIN, hồng ngoại IrDA, điều khiển modem).
 - Tối đa 2 giao diện SPI (tốc độ lên đến 18 Mbit/s).
 - Giao diện CAN (chuẩn 2.0B Active).
 - Giao diện USB 2.0 tốc độ tối đa.
- 51 cổng giao tiếp I/O.



Hình 2: Hình ảnh thực tế vi điều khiển STM32F103C8T6

2.2.2 Khóa chốt điện tử LY-03

Solenoid Lock LY-03, hoạt động như một ổ khóa cửa sử dụng Solenoid để kích đóng mở bằng dòng điện. Trong đề tài này, nhóm sử dụng biến áp và relay 5V để cấp, ổn áp dòng điện để truyền tín hiệu từ vi điều khiển tới khóa chốt.



Hình 3: Hình ảnh thực tế (trái) và nguyên lý hoạt động (phải) của Solenoid

Thông số	Giá trị
Điện áp sử dụng	12V DC
Dòng điện tiêu thụ	0.8A
Công suất tiêu thụ	9.6W
Loại Solenoid	Solenoid từ
Tốc độ phản ứng	dưới 1s
Thời gian kích liên tục	dưới 10s

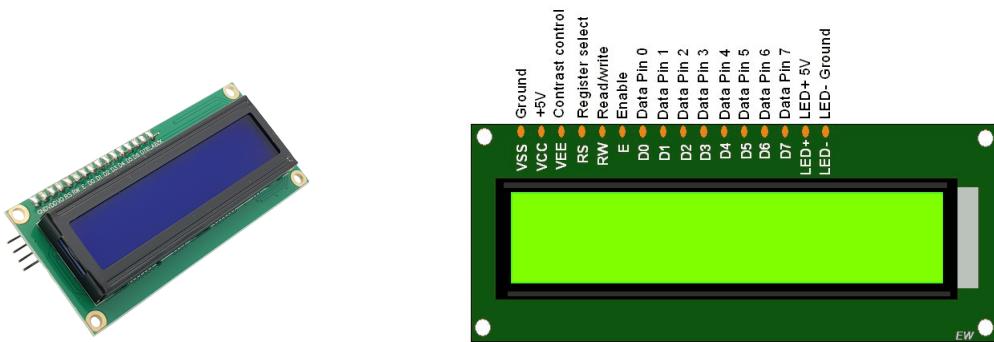
Bảng 1: Thông số khóa điện LY-03

2.2.3 Màn hình LED LCD 16 × 2

Màn hình với nền xanh dương sử dụng driver HD44780, có khả năng hiển thị 2 dòng với mỗi dòng 16 ký tự. Kết hợp với mạch chuyển giao tiếp I²C để dễ dàng truyền nhận dữ liệu với bộ xử lý trung tâm.

Thông số	Giá trị
Điện áp sử dụng	5V DC
Kích thước	80 × 36 × 12.5 mm
Hiển thị	Chữ trắng, nền xanh dương

Bảng 2: Thông số của màn hình LED 16 × 2

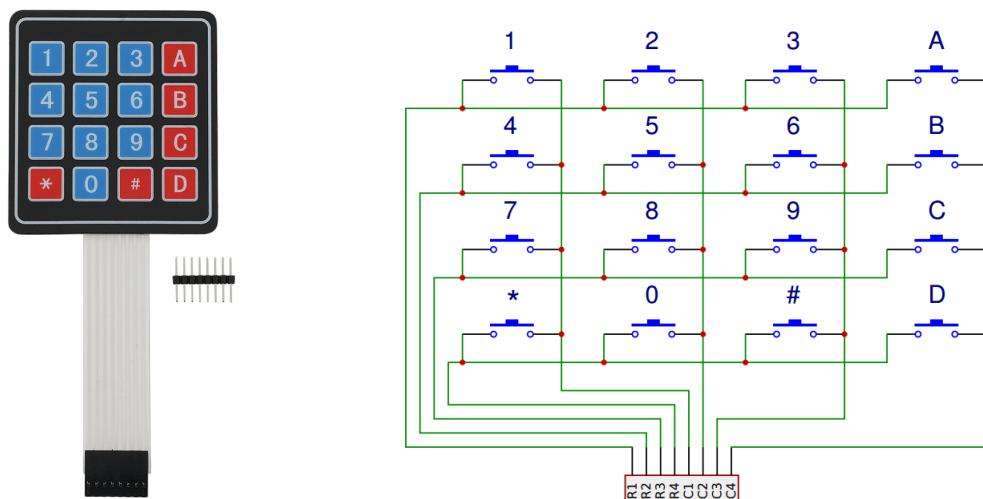


Hình 4: Hình ảnh thực tế (trái) và sơ đồ chân cắm (phải) của màn hình LED

2.2.4 Bàn phím ma trận 4 × 4

Bàn phím ma trận (Matrix Keypad) 4 × 4 là một giải pháp nhập liệu rời rạc phổ biến, cung cấp khả năng nhập dữ liệu số và lệnh điều khiển thông qua mười sáu phím bấm vật lý, được sắp xếp theo cấu trúc lưới không gian hai chiều. Ưu điểm cốt lõi của kiến trúc này là khả năng tối ưu hóa tài nguyên phần cứng (GPIO Optimization), cho phép quản lý mươi sáu trạng thái logic độc lập với số đường tín hiệu chỉ bằng một nửa số trạng thái.

Các phím bấm không có nguồn điện riêng và chia sẻ đường tín hiệu chung, vì điều khiển không thể đọc trực tiếp trạng thái của tất cả mươi sáu phím cùng một lúc. Thay vào đó, hệ thống phải sử dụng kỹ thuật quét lên toàn bộ bàn phím, với mỗi lần quét được thực thi cách nhau một khoảng thời gian rất ngắn cố định để đảm bảo ghi nhận được mọi dữ liệu mà người dùng đưa vào từ bàn phím.



Hình 5: Hình ảnh thực tế và sơ đồ nút (từ trái qua phải) của bàn phím

Thông số	Giá trị
Độ dài dây cắm	88mm
Số đầu nối	8 chân
Kích thước bàn phím	77 × 69 mm
Nhiệt độ hoạt động	0 °C đến 70 °C

Bảng 3: Thông số của bàn phím ma trận



2.2.5 Các thành phần khác

Tên linh kiện	Công dụng
Jumper đực-đực, đực-cái, cái-cái	Kết nối các linh kiện
Relay 5V	Ôn định điện áp cho Solenoid, nhận tín hiệu từ vi điều khiển
Mạch giao tiếp I ² C	Hiện thực giao tiếp giữa màn hình LCD và vi điều khiển
Buzzer 3V	Đơn vị phát âm thanh báo động
Nút bấm	Hỗ trợ nhập liệu, xác thực và mô phỏng tác nhân người dùng

Bảng 4: Các thành phần khác của ổ khóa

2.3 Giải thuật Knutt-Morris-Pratt

Thuật toán Knuth-Morris-Pratt (KMP) được phát triển bởi Donald Knuth, Vaughan Pratt, và James Morris vào năm 1977. Nó được ứng dụng rộng rãi trong các công cụ tìm kiếm, trình biên dịch, và trình soạn thảo văn bản. Đây là một thuật toán tìm kiếm chuỗi hiệu quả, được dùng để tìm một mẫu trong một đoạn văn bản. Thuật toán này sử dụng bước tiền xử lý để xử lý các trường hợp không khớp, nhờ đó đạt được độ phức tạp thời gian tuyến tính $O(n)$.

Thuật toán được triển khai với hai bước như sau:

Bước 1: Tiền xử lý - Xây dựng mảng LPS (Longest Prefix Suffix)

Ta xử lý chuỗi mẫu để tạo ra một mảng LPS. Mảng có ý nghĩa là: “Nếu ký tự không khớp tại vị trí này, ta có thể lùi lại bao nhiêu ký tự trong mẫu mà vẫn không bỏ lỡ khả năng khớp nào?” Nhờ đó, ta không cần phải quay lại đầu mẫu mỗi khi gặp lỗi không khớp. Bước này chỉ được thực hiện một lần duy nhất, trước khi bắt đầu tìm kiếm trong chuỗi văn bản.

Bước 2: So sánh - Tìm chuỗi con trong đoạn chuỗi

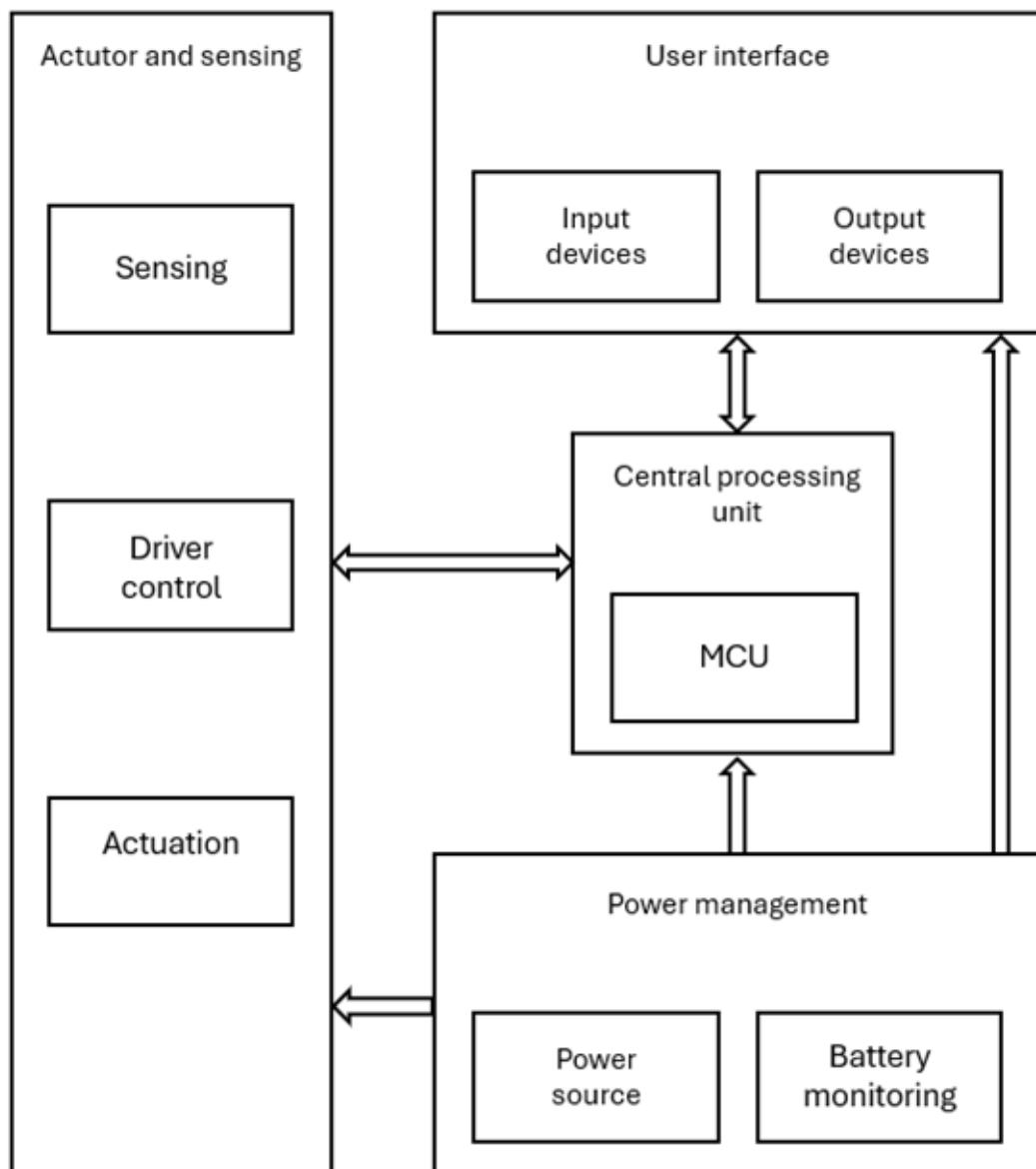
Ta sẽ bắt đầu so sánh các ký tự trong chuỗi nhập vào lần lượt một ký tự:



- Nếu ký tự khớp: di chuyển tiếp đến vị trí tiếp theo của cả chuỗi mẫu và chuỗi nhập vào.
- Nếu ký tự không khớp, sẽ có hai trường hợp:
 - Nếu không bắt đầu ở ký tự đầu tiên ở ký tự mẫu, ta dùng giá trị mảng LPS ở vị trí trước để đưa con trỏ chuỗi mẫu về vị trí đó. Điều đó có nghĩa là: nhảy về đến tiền tố dài nhất đồng thời cũng là hậu tố - không phải kiểm tra lại các ký tự đó.
 - Nếu đó là ký tự đầu, ta chỉ cần chuyển tới vị trí tiếp theo của chuỗi vào để kiểm tra.
- Nếu tới cuối chuỗi mẫu, thì ta đã tìm thấy chuỗi đó. Ta sẽ ghi nhận lại vị trí bắt đầu và tiếp tục kiểm tra.

3 Thiết kế

Sơ đồ bao gồm bốn khối: *Khối xử lý trung tâm*; *Khối giao diện người dùng*; *Khối truyền động và cảm biến* và *Khối quản lý năng lượng*.



Hình 6: Sơ đồ khối tổng quát

3.1 Khối xử lý trung tâm

Dây là đầu não hành vi của toàn bộ ổ khóa. Vì điều khiển thực hiện nhiệm vụ tiếp nhận tín hiệu đầu vào, xử lý thuật toán xác thực và phát lệnh điều khiển đến các thiết



bị ngoại vi.

Khi nhập mật khẩu, vi điều khiển nhận chuỗi ký tự từ bàn phím, sau đó thực hiện tìm kiếm mật khẩu thực liên tục trong chuỗi dữ liệu nhập vào bằng thuật toán xác thực và kích hoạt cơ cấu mở khóa nếu nội dung được kiểm tra là chính xác. Trong trường hợp người dùng sử dụng phương thức mở khóa bằng chìa cơ, vi điều khiển sẽ đọc trạng thái từ button gắn với ổ khóa cơ học để thực hiện hành động tương ứng để mở khóa.

Sau khi nhập mật khẩu, đơn vị xử lý trung tâm sẽ phát lệnh điều khiển đến các thiết bị đầu ra: màn hình hiển thị, còi báo động và relay kích hoạt solenoid ứng với từng trạng thái hoạt động của hệ thống như: tiến hành mở khóa khi đã nhập đúng; sai mật khẩu nhiều lần; hiển thị trực quan và bảo mật nội dung đang nhập... Song song với việc xử lý mở khóa, MCU đảm nhận cả việc giám sát và quản lý các thông số vận hành cần thiết.

3.2 Khối giao diện người dùng

Thiết bị đầu vào

- Bàn phím ma trận kích thước 4×4 cho phép người dùng nhập mật khẩu và các lệnh điều khiển thông qua các phím số từ "0" đến "9" và các ký tự chữ cái từ "A" đến "F", cùng với hai nút bấm rời hiện thực nút "Delete" và "Enter".
- Một button cơ học được lắp đặt tại vị trí ổ khóa cơ có chức năng phát hiện và thông báo cho MCU khi người dùng thực hiện thao tác mở khóa bằng chìa khóa truyền thống.
- Nút bấm được gắn ở mặt trong của cửa, khi được kích hoạt sẽ truyền tín hiệu mở khóa đến MCU.

Thiết bị đầu ra

- Màn hình LCD hiển thị các trạng thái của khóa.
- Còi báo động phát ra các tín hiệu âm thanh trong các tình huống như phát hiện nhập sai mật khẩu liên tiếp nhiều lần.



- Hệ thống đèn LED chỉ thị trạng thái được đặt ở cả hai mặt trước và sau của khóa, giúp người dùng quan sát trực quan trạng thái khóa của cửa.

3.3 Khối truyền động và cảm biến

- Khóa điện từ kiểu solenoid đóng vai trò là cơ cấu chấp hành chính, thực hiện động tác đóng và mở chốt khóa theo chỉ thị từ vi điều khiển.
- Solenoid yêu cầu nguồn cấp có công suất lớn hơn khả năng cung cấp trực tiếp của MCU, vi điều khiển sẽ điều khiển solenoid gián tiếp thông qua một relay trung gian, tín hiệu điều khiển mức logic 5V từ chân GPIO của MCU kích hoạt cuộn dây relay.
- Về phần cảm biến, hệ thống sử dụng một button cảm biến trạng thái cửa nhận biết vị trí đóng hoặc mở của cánh cửa và gửi về MCU, phục vụ cho thao tác cảnh báo người dùng.

3.4 Khối quản lý năng lượng:

Trong thiết kế hệ thống, khối quản lý năng lượng được xây dựng dựa trên phương án lý thuyết như sau:

- **Mô hình thiết kế lý thuyết (Giả lập):**

- Hệ thống được thiết kế với kịch bản sử dụng nguồn điện từ bộ bốn viên pin AA mắc nối tiếp, tạo ra điện áp khoảng 6V.
- Theo thiết kế này, nguồn pin sẽ đi qua các mạch điều chỉnh điện áp để tạo ra các mức điện áp ổn định 5V hoặc 3.3V cung cấp cho MCU cùng các linh kiện điện tử khác.
- Đồng thời, hệ thống tích hợp mạch giám sát điện áp hoạt động trên nguyên tắc đo điện áp bộ nguồn và chuyển đổi thành tín hiệu số gửi về MCU, giúp đưa ra các thông báo pin yếu đến người dùng khi điện áp thấp hơn định mức.

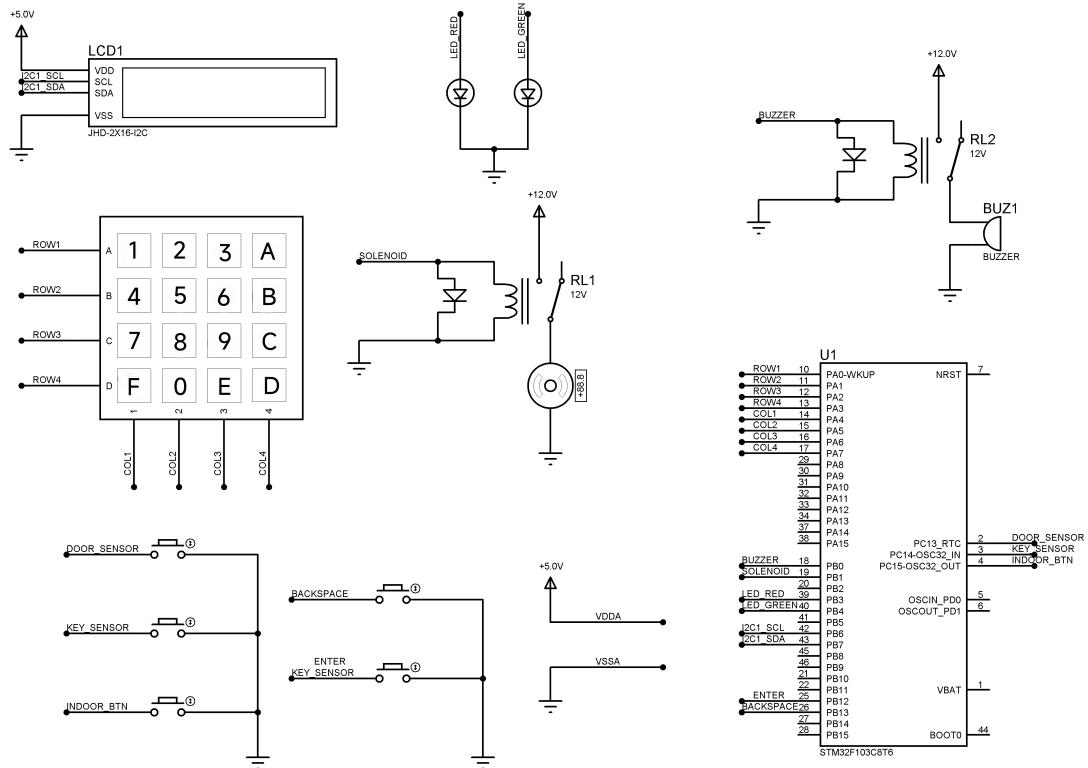
- **Hiện thực thực tế:**



- Để đảm bảo tính ổn định cao trong quá trình triển khai đồ án và đáp ứng nhu cầu năng lượng lớn của cơ cấu chấp hành, nhóm đã hiện thực nguồn cấp thông qua các bộ biến áp (adapter) rời thay vì sử dụng pin.
- **Biến áp 12V:** Cung cấp nguồn động lực trực tiếp cho khóa chốt Solenoid LY-03 thông qua relay. Nguồn này đảm bảo dòng điện tiêu thụ 0.8A và công suất 9.6W cần thiết để kích hoạt cơ chế chốt khóa.
- **Biến áp 5V:** Cung cấp nguồn nuôi cho khối xử lý trung tâm và các thiết bị hiển thị, đảm bảo hệ thống vận hành liên tục và ổn định trên nền tảng breadboard mà không phụ thuộc vào dung lượng pin trong quá trình kiểm thử.

4 Hiệu thực

4.1 Sơ lược thiết kế



Hình 7: Lược đồ thiết kế ổ khóa

Các nút bấm được sử dụng trong lược đồ đóng vai trò mô phỏng cho các tác nhân từ người dùng (mở khóa vật lý, cảnh báo người dùng về trạng thái cửa...) và hỗ trợ nhập liệu.

Hệ thống khóa điện tử nhập số được thiết kế dựa trên mô hình máy trạng thái hữu hạn (Finite State Machine - FSM) với nhiều trạng thái hoạt động riêng biệt. Máy trạng thái được triển khai thông qua ba module chính:

- **Module xử lý đầu vào (input_processing):** Đọc và phát hiện sự kiện từ bàn phím, nút nhấn và cảm biến.
- **Module xử lý trạng thái (state_processing):** Thực thi logic chuyển đổi giữa các trạng thái.



- **Module xử lý đầu ra (output_processing):** Điều khiển các thiết bị ngoại vi như đèn LED, solenoid, buzzer và màn hình LCD.

4.2 Chi tiết các trạng thái

4.2.1 LOCKED_SLEEP (Trạng thái ngủ)

- Màn hình LCD tắt; Solenoid ở trạng thái khóa.
- Bàn phím keypad 4x4 ở chế độ chờ; Hai đèn LED (Đỏ/Xanh) và Buzzer đều tắt.
- Cảm biến cửa (doorSensor) ở trạng thái 1 (cửa đóng).

Chuyển trạng thái:

- Nhấn bất kỳ phím nào → LOCKED_WAKEUP.
- Kích hoạt keySensor hoặc indoor_unlock_button → UNLOCKED_WAITOPEN.

4.2.2 LOCKED_WAKEUP (Trạng thái đánh thức)

- Bật màn hình (hiển thị "LOCK WAKE UP" trong 1 giây); LED Đỏ bật.
- Đọc ADC channel 1 để kiểm tra điện áp nguồn.

Chuyển trạng thái:

- Điện áp pin $< 4.95V \rightarrow \text{BATTERY_WARNING}.$
- Điện áp ổn định → LOCKED_ENTRY.

4.2.3 BATTERY_WARNING (Cảnh báo pin yếu)

- Hiển thị "LOW BATTERY!" trong 3 giây.
- LED Đỏ bật.
- Vô hiệu hóa bàn phím tạm thời.

Chuyển trạng thái: Sau 3 giây → LOCKED_ENTRY.



4.2.4 LOCKED_ENTRY (Nhập mật khẩu)

- Hiển thị "ENTER PASSWORD:"; Dòng 2 hiển thị cơ chế cửa sổ trượt và che dấu ký tự *.
- Nhận input từ keypad, Backspace (xóa), Enter (xác nhận). Buffer tối đa 20 ký tự.
- Bắt đầu bộ đếm 30 giây đến lúc ngưng nhận mật khẩu.

Chuyển trạng thái:

- Kết thúc 30s → LOCKED_SLEEP.
- Nhấn Enter → LOCKED_VERIFY.

4.2.5 LOCKED_VERIFY (Xác thực)

- Kiểm tra độ dài (4-20 ký tự); Chạy thuật toán KMP tìm mật khẩu.
- Quản lý biến failedAttempts.

Chuyển trạng thái:

- Mật khẩu ĐÚNG → UNLOCKED_WAITOPEN.
- Mật khẩu SAI: Nếu sai lần 3, 6, 9, 12 → PENALTY_TIMER; Nếu sai lần 15 → PERMANENT_LOCKOUT.

4.2.6 PENALTY_TIMER (Phạt tạm thời)

- Vô hiệu hóa nhập liệu.
- Buzzer kêu 10s.
- Phạt theo cấp số nhân (1, 5, 25, 125 phút).

Chuyển trạng thái:

- Hết thời gian → LOCKED_ENTRY.
- Dùng chìa khóa cơ → UNLOCKED_WAITOPEN.



4.2.7 PERMANENT_LOCKOUT (Khóa vĩnh viễn)

- Khóa toàn bộ hệ thống nhập liệu.
- Hiển thị "Use the key to unlock!".

Chuyển trạng thái: Chỉ thoát khi dùng chìa khóa cơ hoặc nút mở trong.

4.2.8 UNLOCKED_WAITOPEN (Chờ mở cửa)

- Mở chốt Solenoid và bật LED Xanh.
- Chạy bộ đếm 10 giây cho đèn khi khóa cửa.

Chuyển trạng thái:

- Cửa mở → UNLOCKED_DOOROPEN
- Quá 10s không mở → LOCKED_RELLOCK.

4.2.9 UNLOCKED_SETPASSWORD (Thiết lập mật khẩu mới)

- Cho phép nhập tối đa 4 ký tự
- Lưu vào biến toàn cục khi nhấn Enter.

Chuyển trạng thái: Thành công hoặc lỗi/timeout → Quay về trạng thái khóa hoặc chờ tương ứng.

4.2.10 UNLOCKED_DOOROPEN (Cửa đang mở)

- Giữ Solenoid mở
- Hiển thị "DOOR OPEN"; Timer 30 giây.

Chuyển trạng thái:

- Dóng cửa → UNLOCKED_WAITCLOSE.
- Quá 30s → ALARM_FORGOTCLOSE.



4.2.11 ALARM_FORGOTCLOSE (Cảnh báo quên đóng)

- Buzzer kêu 10 giây
- Nhắc nhở "Close door!" mỗi 5 phút.

Chuyển trạng thái: Cửa đóng → UNLOCKED_WAITCLOSE.

4.2.12 UNLOCKED-ALWAYSOPEN (Chế độ luôn mở)

- Vô hiệu hóa cảnh báo quên đóng
- Giữ cửa luôn ở trạng thái mở.

Chuyển trạng thái: Người dùng chủ động đóng cửa → UNLOCKED_WAITCLOSE.

4.2.13 LOCKED_RELOCK (Khóa lại)

- Dây chốt Solenoid
- LED DỎ bật Hiển thị "Locking..." .

Chuyển trạng thái: Sau 3 giây tự động chuyển về LOCKED_SLEEP.

4.3 Hiện thực mã nguồn

Mã nguồn hiện thực của nhóm được truy cập qua đường dẫn sau:

<https://github.com/Nguyen-Hao-Khang/Digital-Keypad-Lock>

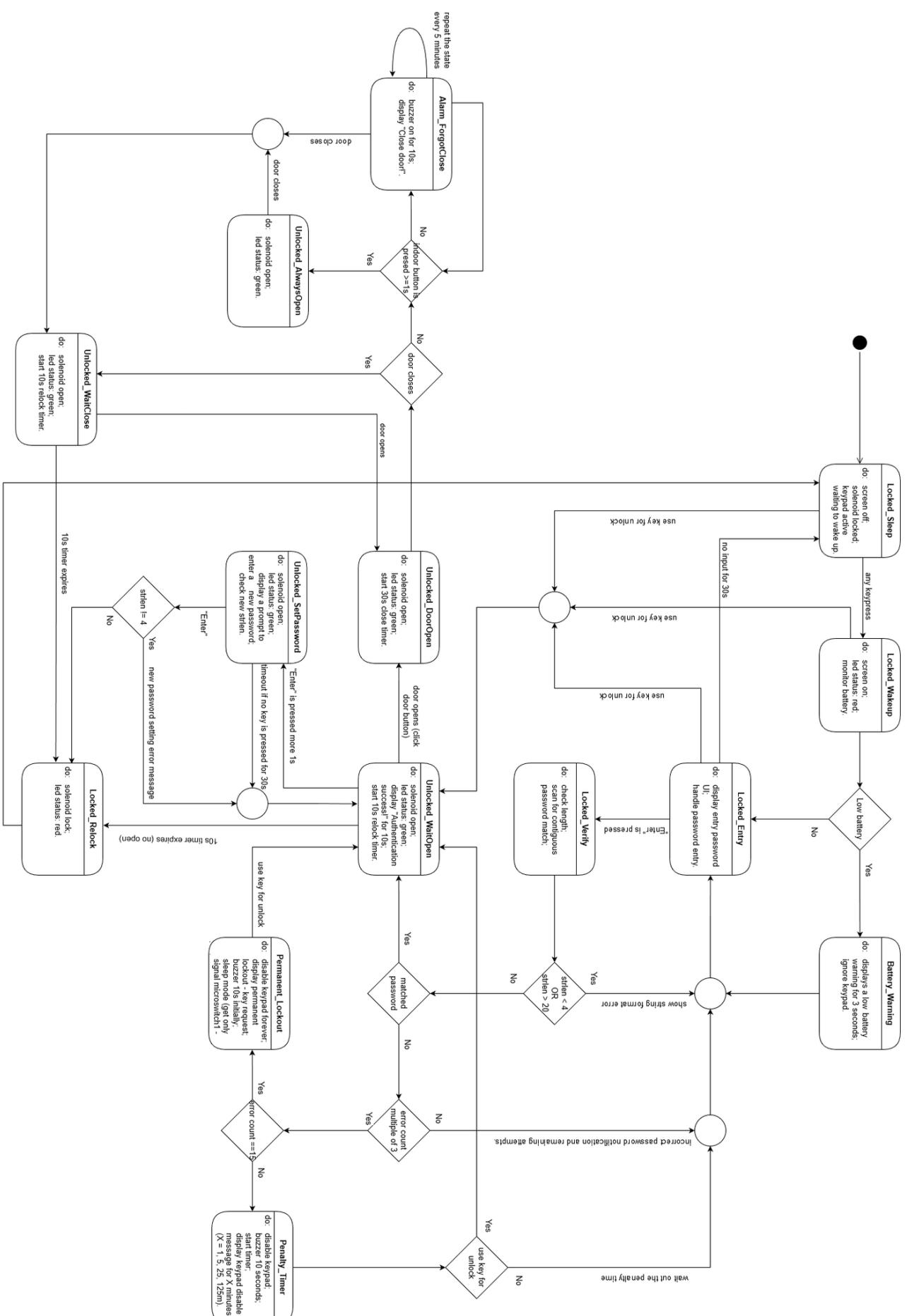
4.4 Sơ đồ máy trạng thái

Sơ đồ máy trạng thái có thể được truy cập qua đường dẫn sau:

<https://drive.google.com/file/d/1TCnZJqhzMKbLzAA-fE10va03ULszKEpr/view>

và sử dụng trang app.diagrams.net để chỉnh sửa và xem chi tiết.

Hình 8 dưới đây minh họa các điều kiện chuyển đổi và các trạng thái hoạt động của máy trạng thái:



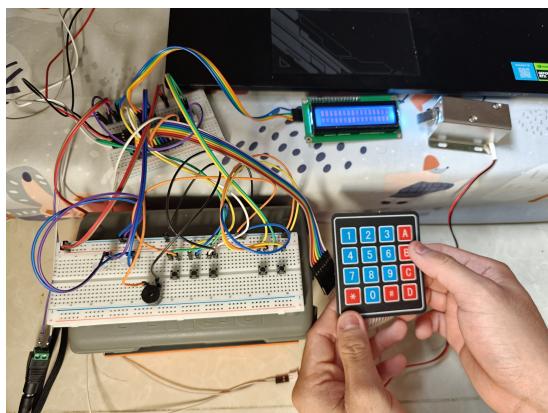
Hình 8: Sơ đồ mô tả các trạng thái của ổ khóa

5 Kiểm thử đề tài

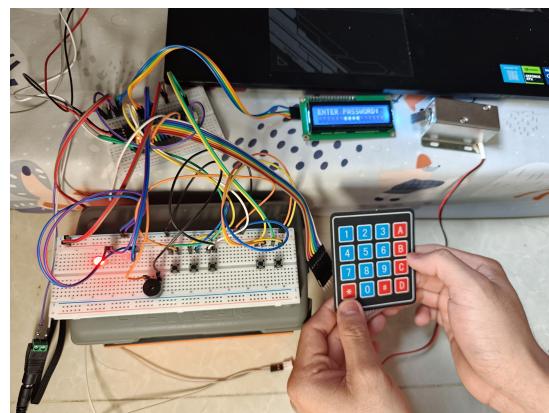
Đoạn phim sau đây mô phỏng các quy trình tương tác của người dùng với sản phẩm:

<https://drive.google.com/drive/folders/1xaC33nvBLp6ym-MlGqFftA020o0KhSRX?usp=sharing>

Các hình ảnh dưới đây minh họa một số trạng thái của hệ thống trong môi trường mô phỏng, thể hiện sự chuyển đổi linh hoạt giữa các chế độ bảo mật:

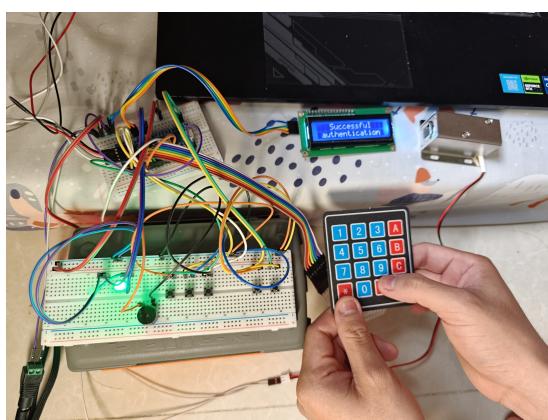


(a) Trạng thái chờ

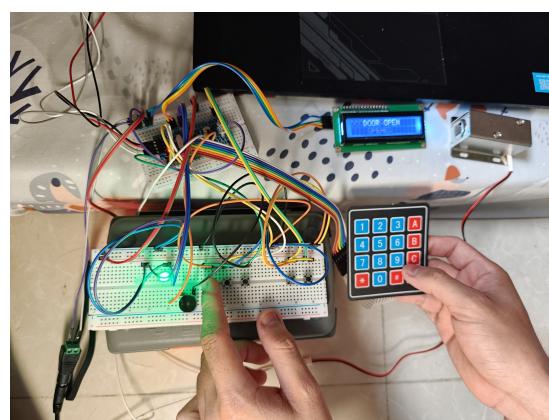


(b) Nhập mật khẩu

Hình 9

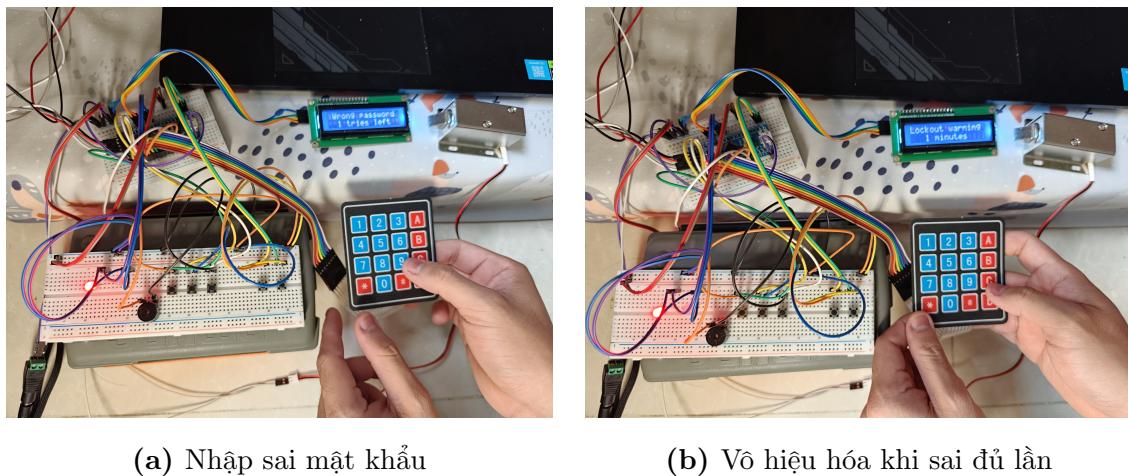


(a) Xác thực thành công



(b) Nhấn nút mở cửa

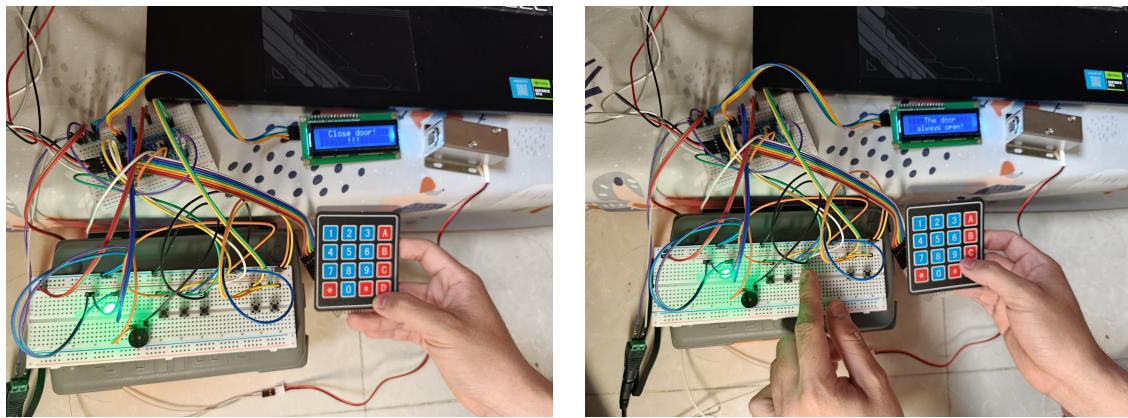
Hình 10



(a) Nhập sai mật khẩu

(b) Vô hiệu hóa khi sai đủ lần

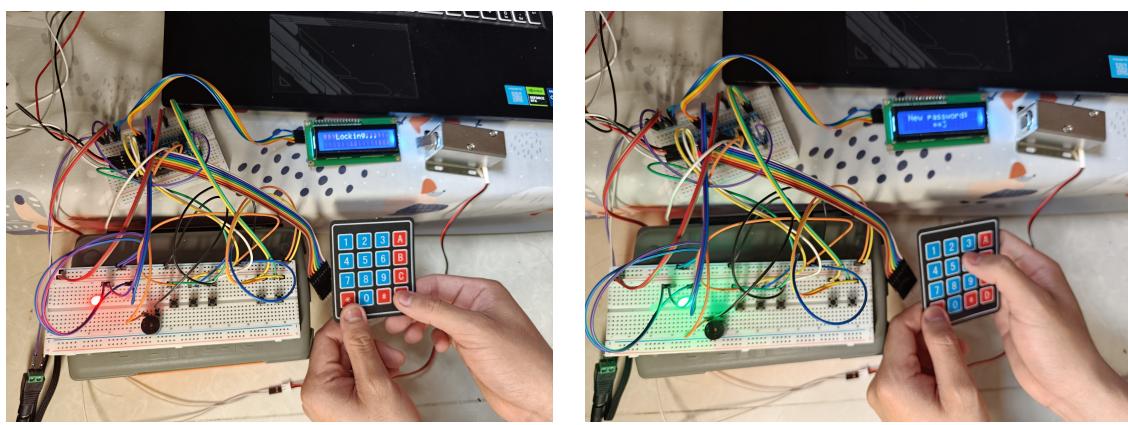
Hình 11



(a) Cảnh báo cửa mở lâu

(b) Trạng thái cửa luôn mở

Hình 12



(a) Cửa tự khóa sau 10 giây

(b) Đổi mật khẩu

Hình 13



6 Kết luận

Đề tài "Ổ khóa điện tử" đã được nhóm triển khai thành công với mục tiêu xây dựng một hệ thống khóa cửa sử dụng vi điều khiển STM32F103C8T6, kết hợp phương thức xác thực bằng mật khẩu 16 ký tự và cơ chế dự phòng bằng chìa khóa cơ hoặc nút mở khóa trong. Qua quá trình nghiên cứu, thiết kế và hiện thực, nhóm đã đạt được những kết quả quan trọng về mặt kỹ thuật cũng như tích lũy được nhiều kinh nghiệm trong lĩnh vực hệ thống nhúng.

6.1 Kết quả đạt được

Hệ thống ổ khóa điện tử đã được hoàn thiện với đầy đủ các tính năng theo đúng phạm vi và chức năng đề tài đã đề ra:

- Xác thực mật khẩu thông qua bàn phím ma trận 4×4 với hai phím hỗ trợ Backspace và Enter để xác thực.
- Mở khóa bằng phương thức vật lý sử dụng chìa khóa cơ và nút bấm bên trong.
- Quản lý mật khẩu cho phép người dùng tạo lập và thay đổi.
- Cơ chế cảnh báo an ninh với các mức phạt thời gian tăng dần theo cấp số nhân.
- Giao diện người dùng trực quan thông qua màn hình LCD 16×2 .

Về mặt kiến trúc hệ thống, nhóm đã thiết kế và triển khai thành công mô hình máy trạng thái chi tiết, đảm bảo logic chuyển đổi chặt chẽ giữa các trạng thái. Việc quản lý nhiều trạng thái với logic chuyển đổi đa dạng gây không ít khó khăn, nhưng qua quá trình nghiên cứu và tối ưu, nhóm đã xây dựng được một kiến trúc FSM rõ ràng, dễ bảo trì và mở rộng. Việc chia tách module thành các khối xử lý độc lập (`input_processing`, `state_processing`, `output_processing`) không chỉ giúp mã nguồn dễ đọc hơn mà còn tạo điều kiện thuận lợi cho việc debug và phát triển thêm tính năng mới trong tương lai.

Ở phương thức xác thực mật khẩu, áp dụng thuật toán Knuth-Morris-Pratt cho cơ chế dò tìm mật khẩu trong chuỗi ký tự nhập giúp tối ưu hiệu suất xử lý với độ phức



tạp O(n) và khả năng bảo mật đáng kể khi có kẻ gian cố tình theo dõi khi người dùng nhập mật khẩu (tính năng xác thực trên chuỗi nhập được nhóm tham khảo ở các sản phẩm thực tế trong thị trường).

Về mặt kỹ thuật phần cứng, nhóm đã có cơ hội hiện thực trên nhiều thiết bị khác nhau, từ các nút nhấn, LED đơn giản đến các thiết bị khá phức tạp như màn hình LCD và keypad. Thông qua quá trình tìm kiếm các linh kiện và video hướng dẫn liên quan đã nâng cao kiến thức và khả năng áp dụng thực tế các linh kiện của các thành viên.

6.2 Khó khăn - hướng giải quyết

Trong quá trình thực hiện đồ án, nhóm đã gặp phải nhiều thách thức liên quan đến cả khía cạnh quản lý dự án lẫn thiết kế kỹ thuật"

- **Phân tích và làm rõ yêu cầu hệ thống:** Đề tài được đưa ra ở mức độ tổng quát. Để có được chi tiết hóa đầy đủ các chức năng, ràng buộc và kịch bản hoạt động của hệ thống khóa điện tử, nhóm đã tiến hành phân tích hành vi người dùng thực tế thông qua phương pháp quan sát và đặt giả thuyết, từ đó xác định các trường hợp sử dụng cụ thể.
- **Phối hợp và quản lý tiến độ nhóm:** Nhóm sử dụng các nền tảng họp trực tuyến và duy trì kênh giao tiếp liên tục nhằm đảm bảo tiến độ dự án, cập nhật và giải quyết các vấn đề phát sinh kịp thời. Việc này giải quyết được vấn đề di chuyển của các thành viên khi sự khác biệt về khoảng cách địa lý giữa các thành viên là rất lớn.
- **Thiết kế nguồn ngoại vi cho các thiết bị:** Vì điều khiển hoạt động ở mức logic 3.3V/5V không thể điều khiển trực tiếp tải 12V cao áp dành cho Solenoid. Giải pháp được nhóm áp dụng là thiết kế mạch điều khiển hai tầng: vi điều khiển điều khiển relay 5V, relay đóng vai trò công tắc để kết nối nguồn 12V riêng biệt với solenoid. Kiến trúc này đảm bảo sự cách ly điện áp giữa mạch logic và mạch công suất, bảo vệ vi điều khiển khỏi dòng điện lớn.



- **Quản lý trạng thái phức tạp:** Thiết kế máy trạng thái ban đầu có quá nhiều trạng thái dư thừa. Việc triển khai logic này bằng cấu trúc if - else lồng nhau truyền thống dễ dẫn đến lỗi luận lý và vô cùng khó bảo trì. Để giải quyết vấn đề này, nhóm dự định sử dụng mô hình State Machine programming, trong đó mỗi trạng thái được định nghĩa tường minh cùng với các điều kiện chuyển đổi. Vấn đề timer được nhóm cân nhắc sử dụng cooperative giảm khả năng sai sót khi quản lý các timer.

6.3 Phát triển trong tương lai

Mặc dù đã đạt được những kết quả trong phạm vi dự án, hệ thống ở khóa điện tử vẫn còn nhiều tiềm năng để phát triển và cải thiện. Theo thiết kế dự án, mã nguồn đã tích hợp trạng thái cảnh báo pin yếu (kiểm tra điện áp nguồn mỗi khi hệ thống được đánh thức), tuy nhiên để thuận tiện cho việc kiểm thử trên breadboard với nguồn adapter, cờ báo pin yếu đang được giả lập (mức 0 - không cảnh báo). Trong các phiên bản tiếp theo, nhóm có thể chuyển đổi sang sử dụng pin AA hoặc pin sạc lithium-ion với mạch quản lý hoàn chỉnh, từ đó kích hoạt đầy đủ tính năng giám sát pin thực tế và cảnh báo người dùng thay pin kịp thời.

Về phương thức xác thực, hệ thống hiện tại chỉ sử dụng mật khẩu số dựa trên bàn phím. Để nâng cao tính bảo mật và trải nghiệm người dùng, hệ thống có thể được mở rộng với các phương thức sinh trắc học như:

- Cảm biến vân tay cho phép xác thực nhanh chóng và chính xác.
- Nhận dạng khuôn mặt thông qua cảm biến hồng ngoại và thuật toán xử lý ảnh.
- Nhận dạng giọng nói để tạo trải nghiệm xác thực tự nhiên hơn.

Việc tích hợp đa phương thức xác thực sẽ tăng đáng kể mức độ an ninh của hệ thống, đồng thời mang lại sự tiện lợi cho người dùng.

Về cơ chế dự phòng, dự án hiện tại sử dụng chìa khóa cơ truyền thống có thể được thay thế bằng các giải pháp hiện đại hơn như thẻ từ RFID hoặc NFC. Điều này cho phép quản lý quyền truy cập linh hoạt hơn, ví dụ như cấp thẻ tạm thời cho khách hoặc vô hiệu hóa thẻ bị mất mà không cần thay đổi ổ khóa.



Cuối cùng, xu hướng phát triển hướng tới tích hợp khả năng kết nối IoT. Bằng cách trang bị module WiFi hoặc Bluetooth, hệ thống có thể được điều khiển và giám sát từ xa thông qua ứng dụng di động. Người dùng có thể nhận thông báo khi có người mở khóa, xem lịch sử truy cập, thay đổi mật khẩu từ xa, hoặc cấp quyền mở cửa tạm thời cho khách mà không cần có mặt tại nhà. Hơn nữa, việc lưu trữ dữ liệu trên cloud sẽ giúp phân tích hành vi sử dụng và phát hiện các hoạt động bất thường, từ đó nâng cao khả năng bảo mật tổng thể của hệ thống.