Tài liệu Yêu cầu Kỹ thuật (Technical Requirement)

RFID Door

1. Giới thiệu

+ Mô tả cơ bản: Bao gồm màn hình LCD với chức năng hiển thị, bàn phím số từ 1 – 9 có phím Enter và Delete để người dùng nhập mật khẩu, bộ cảm biến thẻ từ RFID để người dùng quẹt thẻ, relay và solenoid cho chức năng khóa cửa, vi điều khiển STM32 xử lý các tác vụ.

+ **Ứng dụng:** RFID Door là một hệ thống kiểm soát ra vào cho cửa sử dụng công nghệ nhận dạng qua tần số vô tuyến. Về cơ bản, nó cho phép mở khóa cửa mà không cần chìa khóa vật lý, tạo nên sự tiện lợi và hiệu quả.

2. Yêu cầu kỹ thuật

2.1. Ngoại hình

- Nhìn đẹp, không xấu…

2.2. Điều khiển

- Sử dụng kiến trúc ARM phổ biến.
- Tần số hoạt động lớn đảm bảo các tác vụ xác thực.
- Bộ nhớ Flash tối thiểu 64 Kb để lưu firmware hệ thống.
- Có bộ nhớ không bay hơi (Flash) với khả năng lưu dữ liệu như mật khẩu, UID của thẻ hợp lệ.
- Có các chuẩn giao tiếp I2C, SPI.
- Số chân GPIO có thể sử dụng >= 8.
- Tiêu thụ năng lượng thấp.
- Hoạt động trên điện áp 3.3V

2.3. Hiển thị

- Trang bị màn hình LCD 16x2 (16 ký tự, 2 dòng) giao tiếp I2C
- Có đèn nền để sử dụng trong điều kiện ánh sáng kém.
- Điện áp hoạt động 5V.

2.4. Chức năng

- **Chức năng nhập mật khẩu:**
  + Bàn phím ma trận 4x3 hoặc các phím bấm riêng lẻ.
  + Bàn phím phải có đủ 1-9, có phím Enter và Delete.
  + Phím cứng, có độ nảy cao.

+ Trang bị còi kêu sau mỗi nút được nhấn.
+ Giao tiếp với vi điều khiển qua GPIO.

- **Chức năng quét RFID:**
  + Sử dụng RC522.
  + Tần số hoạt động 13.56 MHz
  + Khoảng cách đọc tối thiểu 3 cm
  + Nhận diện chính xác các thẻ RFID khác nhau.
- **Chức năng điều khiển khóa từ:**
  + Relay 1 kênh, điện áp kích 3.3V – 5V. Công suất tiếp điểm phải chịu được điện áp và dòng điện của khóa solenoid.
  + Khóa solenoid loại Fail-secure (vẫn khóa khi mất điện). Hoạt động trên điện áp >12V.
  + Relay phải kích mở solenoid lập tức < 1s.
  + Chỉ mở solenoid khi nhập đúng mật khẩu hoặc đúng thẻ hợp lệ.
  + Tự động đóng solenoid sau 7s.

2.5. Bảo mật

- Chỉ chấp nhận đặt mật khẩu tối thiểu 6 ký tự**.**
- Nhập sai quá 5 lần sẽ khóa chức năng trong 1 tiếng.
- REQ-SEC-DATA-01 (Lưu trữ Mật khẩu An toàn): Hệ thống phải sử dụng thuật toán băm (cryptographic hash) tiêu chuẩn (ví dụ: SHA-256) để lưu trữ mật khẩu.
- REQ-SEC-DATA-02 (Bảo vệ Dữ liệu Người dùng): Danh sách các mã định danh (UID) của thẻ RFID hợp lệ và chuỗi hash của mật khẩu phải được lưu trữ trong bộ nhớ không bay hơi (non-volatile memory) của vi điều khiển.
- REQ-SEC-PHY-01 (Kiến trúc Phân tách): Thiết kế vật lý của hệ thống **phải** tuân thủ nguyên tắc kiến trúc phân tách gồm khu vực an toàn cho thiết bị bên trong và khu vực tương tác với người dùng.
- REQ-SEC-PHY-02 (Bảo vệ Dây dẫn): Dây tín hiệu kết nối giữa các thành phần bên ngoài và bo mạch xử lý bên trong phải được che chắn và bảo vệ để chống lại các hành vi cắt, chập hoặc can thiệp vật lý.

2.6. Yêu cầu phi chức năng

- Thời gian đọc và xác thực thẻ RFID < 1s.
- Thời gian xác thực mật khẩu sau khi nhấn Enter phải dưới **<** 1s.
- Hệ thống phải hoạt động ổn định 24/7.

- Cần có cơ chế xử lý khi mất điện: Khóa loại Fail-secure, có nguồn điện dự phòng.
- Giao diện người dùng trên LCD phải rõ ràng, dễ hiểu.
- Các thao tác phải trực quan, không yêu cầu hướng dẫn phức tạp.

2.7. Kiểm chứng và xác nhận

3. Use case

UC-01 — Tap thẻ RFID để mở cửa

- Actor: Người dùng
- Mục tiêu: Mở khóa nhanh bằng thẻ hợp lệ.
- Tiền điều kiện: Hệ thống sẵn sàng; đầu đọc RFID hoạt động; danh sách UID hợp lệ đã nạp.
- Trigger: Người dùng đưa thẻ sát đầu đọc.
- Dòng chính:
    1. Hệ thống phát hiện thẻ và đọc UID.
    2. So khớp UID với danh sách cho phép.
    3. Hiển thị “Access Granted”; cửa mở.
- Ngoại lệ/nhánh: UID không hợp lệ → “Access Denied”, beep ngắn; yêu cầu thử lại.
- Hậu điều kiện: Cửa mở trong khoảng thời gian cho phép rồi tự đóng.
- KPI/UI: Phản hồi < 1 giây; LCD hiển thị rõ ràng kết quả.

UC-02 — Nhập PIN để mở cửa

- Actor: Người dùng
- Mục tiêu: Mở cửa khi không có thẻ hoặc thẻ lỗi.
- Tiền điều kiện: PIN đã được thiết lập; bàn phím hoạt động.
- Trigger: Người dùng bấm phím bất kỳ để bắt đầu nhập.
- Dòng chính:
    1. Người dùng nhập chuỗi số PIN.

2. Nhấn Enter để xác nhận.
3. Hệ thống kiểm tra → “Access Granted”; cửa mở.

- Ngoại lệ/nhánh:
  - Nhấn Delete để xóa ký tự cuối.
  - PIN sai → “Wrong PIN”, tăng bộ đếm sai.
  - Đang bị lockout → hiển thị thời gian chờ còn lại.
- Hậu điều kiện: Cửa mở trong thời hạn rồi tự đóng.
- KPI/UI: Xử lý sau Enter < 1 giây; beep mỗi lần bấm phím; che PIN trên LCD.

UC-03 — Xem hướng dẫn & phản hồi trên LCD

- Actor: Người dùng
- Mục tiêu: Biết phải làm gì và biết trạng thái hiện tại.
- Tiền điều kiện: LCD hiển thị bình thường.
- Trigger: Người dùng nhìn màn hình ở trạng thái chờ hoặc trong khi thao tác.
- Dòng chính:
  1. Ở trạng thái chờ, LCD hiển thị “Tap card or Enter PIN”.
  2. Khi đang nhập → hiển thị tiến trình (ví dụ: “PIN: ****”).
  3. Khi xác thực xong → hiển thị kết quả và đếm lùi thời gian mở cửa.
- Ngoại lệ/nhánh: Cảnh báo lỗi nhập hoặc lockout (thời gian chờ).
- Hậu điều kiện: Người dùng nhận được phản hồi rõ ràng để hoàn tất tác vụ.
- KPI/UI: Thông điệp ngắn gọn, dễ hiểu; cập nhật theo thời gian thực.

UC-04 — Thử lại sau khi bị từ chối

- Actor: Người dùng
- Mục tiêu: Có thể sửa lỗi và thao tác lại nhanh chóng.
- Tiền điều kiện: Lần xác thực trước thất bại (thẻ sai hoặc PIN sai).
- Trigger: Người dùng thao tác lại (đưa thẻ khác/nhập lại PIN).

- Dòng chính:
    1. Hệ thống cho phép nhập lại ngay lập tức.
    2. Thực hiện lại UC-01 hoặc UC-02.
- Ngoại lệ/nhánh: Đạt số lần sai tối đa → chuyển sang lockout (thông báo thời gian chờ).
- Hậu điều kiện: Thành công thì mở cửa; thất bại tiếp tục hiển thị hướng dẫn.
- KPI/UI: Không quá 1 thao tác phụ để quay lại màn hình chờ; thông báo lý do từ chối.

UC-05 — Quản trị: Thêm/Xóa thẻ hợp lệ

- Actor: Quản trị viên
- Mục tiêu: Cấp quyền hoặc thu hồi quyền truy cập bằng thẻ.
- Tiền điều kiện: Đã vào chế độ quản trị (đăng nhập/nhập mã admin).
- Trigger: Admin chọn chức năng “Quản lý thẻ” trên giao diện bảo trì.
- Dòng chính:
    1. Thêm thẻ: Yêu cầu quét thẻ mới → hiển thị UID → xác nhận lưu.
    2. Xóa thẻ: Chọn UID trong danh sách → xác nhận xóa.
    3. Lưu thay đổi và hiển thị kết quả.
- Ngoại lệ/nhánh: Thẻ/UID trùng; lỗi ghi bộ nhớ → thông báo và hủy thao tác.
- Hậu điều kiện: Danh sách thẻ hợp lệ được cập nhật.
- KPI/UI: Thao tác ≤ 3 bước cho mỗi thêm/xóa; xác nhận rõ ràng trước khi ghi.

UC-06 — Quản trị: Đặt/Đổi PIN hệ thống

- Actor: Quản trị viên
- Mục tiêu: Thiết lập hoặc thay đổi PIN mở cửa cho người dùng.
- Tiền điều kiện: Đã vào chế độ quản trị.
- Trigger: Admin chọn “Cài đặt PIN”.
- Dòng chính:

1. Nhập PIN mới (đảm bảo tối thiểu độ dài quy định).
2. Nhập lại để xác nhận.
3. Lưu và hiển thị “PIN updated”.

- Ngoại lệ/nhánh: PIN quá ngắn/không khớp khi xác nhận → yêu cầu nhập lại.
- Hậu điều kiện: PIN mới có hiệu lực; có thông báo thành công.
- KPI/UI: Quy trình ≤ 2 phút; không hiển thị PIN rõ trên màn hình.

UC-07 — Quản trị: Gỡ khóa lockout (khẩn cấp)

- Actor: Quản trị viên
- Mục tiêu: Cho phép người dùng tiếp tục truy cập khi cần (ví dụ quên PIN, nhập sai nhiều).
- Tiền điều kiện: Hệ thống đang ở trạng thái lockout do quá số lần sai.
- Trigger: Admin chọn “Gỡ lockout” trong menu bảo trì.
- Dòng chính:
    1. Xác thực admin.
    2. Chọn “Gỡ lockout ngay”.
    3. Hệ thống xóa trạng thái khóa và trở về màn hình chờ.
- Ngoại lệ/nhánh: Không đủ quyền admin → từ chối thao tác.
- Hậu điều kiện: Người dùng có thể thực hiện lại UC-01/UC-02.
- KPI/UI: Thao tác ≤ 30 giây; hiển thị thông báo “Lockout cleared”.