Table of Contents

1. Preface ……4

1.1 Expected Readership
1.2 Version History
1.3 Rationale for new versions
1.4 Summary of changes in versions

2. Introduction……5

2.1 Introduction to the Need for the System
2.2 System Functions
2.3 Integration with Other Systems
2.4 Alignment with Business or Strategic Objectives

3. Glossary……6

3.1 Door Locker Security System
3.2 HMI_ECU (Human Machine Interface)
3.3 CONTROL_ECU
3.4 2x16 LCD
3.5 4x4 Keypad
3.6 DC Motor
3.7 EEPROM
3.8 I2C (Inter-Integrated Circuit)
3.9 UART (Universal Asynchronous Receiver-Transmitter)
3.10 GPIO (General Purpose Input/Output)
3.11 Buzzer
3.12 Timer 1
3.13 Terms Specific to Door Locker Security System Operations

4. User Requirements Definition……8

4.1 User Services
4.2 Non-functional System Requirements
4.3 Product and Process Standards

5. System Architecture……10

5.1 Architecture of HMI_MC1
5.2 Architecture of CONTROL_MC2
5.3 Architecture of The Whole System

6. System Requirements Specification……...12
6.1 Functional Requirements
6.1.1 Password Management
6.1.1.1 Password Creation
6.1.1.2 Password Verification
6.1.1.3 Password Change
6.1.2 Door Control
6.1.2.1 Door Unlocking
6.1.2.2 Door Locking
6.1.3 System Feedback
6.1.3.1 Information Display LCD
6.1.3.2 Security Alert Buzzer
6.2 Non-Functional Requirements
6.2.1 Performance Requirements
6.2.1.1 Response Time
6.2.1.2 Motor Rotation Time
6.2.1.3 LCD display Refresh Rate
6.2.2 Reliability Requirements
6.2.2.1 Password Verification Accuracy
6.2.2.2 Motor Reliability
6.2.3 Usability Requirements
6.2.3.1 User Guidance
6.2.3.2 Keypad Responsiveness
6.2.4 Security Requirements
6.2.4.1 Password Storage
6.2.4.2 Buzzer Activation
6.3 Interfaces to Other Systems
6.3.1 HMI_ECU to CONTROL_ECU Communication (UART)
6.3.2 CONTROL_ECU to External EEPROM (I2C)
7. System Model……16
7.1 Object Model
7.1.1 Purpose
7.1.2 Description
7.2 Data-Flow Model
7.2.1 Purpose
7.2.2 Description
7.2.3 Example Data-Flow Model

7.3 Semantic Data Model
7.3.1 Purpose
7.3.2 Description
7.4 State Diagram to our Project
8. System Evolution……..…21
8.1 Fundamental Assumptions
8.1.1 Purpose
8.1.2 Assumptions
8.2 Anticipated Changes
8.2.1 Purpose
8.2.2 Anticipated Changes
8.2.3 Mitigation Strategies
9. Appendices……23
9.1 Hardware Requirements
9.1.1 Minimal Configuration
9.1.2 Optimal Configuration
9.2 Database Requirements
9.2.1 Logical Organization
9.2.2 Database Scalability
9.2.3 Database Access Control
9.3 Database and Hardware Integration
10. Index…….25
10.1 Alphabetical Index
10.2 Diagram Index
10.3 Function Index

1. Preface

1.1 Expected Readership

This documentation is designed for developers and end-users who wish to understand, install, and utilize the Door Locker Security System.

1.2 Version History

- Version 1.0 (Release Date: 1/10/2023)
    - Initial release of the Door Locker Security System documentation.
- Version 1.1 (Release Date: 20/10/23)
    - Bug fixes and minor updates to improve user experience.
- Version 2.0 (Release Date: 8/11/2023)
    - Add Buzzer feature for more security.
    - Change the password feature.

1.3 Rationale for New Versions

New versions are created to continually enhance the Door Locker Security System, introducing new features, and ensuring the security and reliability of the system.

1.4 Summary of Changes in Version 2.0

- Added buzzer feature since if the person entered the password 3 times wrong in row it will be activated.
- Add Change password feature since you can change your password but after you enter the old password correctly.

2. Introduction

2.1 Introduction to the Need for the System

The Door Locker Security System addresses the critical need for a robust and intelligent access control solution. In modern environments where security is paramount, the system provides an effective means to enhance physical access, security and control.

2.2 System Functions

- HMI_ECU (Human Machine Interface) - Mc1:

  Responsible for user interaction, HMI_ECU utilizes a 2x16 LCD and a 4x4 keypad. It guides users through password creation, entry, and system options display.

- CONTROL_ECU - Mc2:

  Handles core processing and decisions:

  - Creates and stores system passwords securely in EEPROM.
  - Controls a DC motor for physical door locking/unlocking.
  - Manages the overall system logic and responses.

2.3 Integration with Other Systems

The Door Locker Security System seamlessly integrates with other systems:

- HMI_ECU to CONTROL_ECU: Communication via UART allows HMI_ECU to send user-entered passwords to CONTROL_ECU for processing.
- CONTROL_ECU to External EEPROM: I2C facilitates secure storage of system passwords in an external EEPROM.
- CONTROL_ECU to Buzzer and DC Motor: GPIO and Timer1 drive the Buzzer and DC motor for audio alerts and door control.

2.4 Alignment with Business or Strategic Objectives

The implementation of the Door Locker Security System aligns strategically with the organization's goals by:

Enhancing Security Measures: Mitigating risks associated with unauthorized access.

Technological Innovation: Providing a modern, user-friendly solution in line with technological advancements.

Comprehensive Security Strategy: Contributing to a broader security strategy by integrating with existing systems.

This system plays a pivotal role in achieving the organization's objectives by offering enhanced security, user convenience, and adaptability to evolving technological landscapes.

3. Glossary

To enhance clarity and understanding, the following terms are defined as they are used in this document:

3.1 Door Locker Security System:

The comprehensive security solution is designed to control and monitor physical access to doors. It includes a Human Machine Interface (HMI_ECU) for user interaction and a Control Electronic Control Unit (CONTROL_ECU) for core processing.

3.2 HMI_ECU (Human Machine Interface):

The interface was responsible for user interaction with the Door Locker Security System. It incorporates a 2x16 LCD for displaying information and a 4x4 keypad for user input.

3.3 CONTROL_ECU:

The Control Electronic Control Unit is the core processing unit of the Door Locker Security System. It manages password creation, verification, door control, and overall system logic.

3.4 LCD 2x16:

A Liquid Crystal Display with a capacity of 2 rows and 16 characters per row, utilized in the HMI_ECU for presenting information to the user.

3.5 Keypad 4x4:

A keypad with four rows and four columns is used in the HMI_ECU for user input, particularly in the process of entering and confirming passwords.

3.6 DC Motor:

A Direct Current motor is used for physically controlling the locking and unlocking of doors within the Door Locker Security System.

3.7 EEPROM (Electrically Erasable Programmable Read-Only Memory):

An external memory storage device is used in the CONTROL_ECU for securely storing system passwords.

3.8 I2C (Inter-Integrated Circuit):

A communication protocol utilized in the Door Locker Security System for interfacing with the EEPROM.

3.9 UART (Universal Asynchronous Receiver-Transmitter):

A communication protocol is used for serial communication between the HMI_ECU and CONTROL_ECU.

3.10 GPIO (General Purpose Input/Output):

A set of pins on a microcontroller is used for both input and output operations. In the Door Locker Security System, GPIO is employed for various tasks, including interfacing with the DC Motor and Buzzer.

3.11 Buzzer:

An audio signaling device integrated into the CONTROL_ECU for generating sound alerts in response to specific events.

3.12 Timer1:

A timer module is employed in the CONTROL_ECU for time-related operations, such as controlling the duration of motor rotations and managing system timing.

3.13 Terms Specific to Door Locker Security System Operations:

Password Creation: The process of setting up a unique access code for the Door Locker Security System.
Password Verification: Confirm that the entered password matches the stored password.
Door Unlocking: The act of allowing physical access by rotating the DC Motor in a specified direction.
Door Locking: The act of securing the door by rotating the DC Motor in the opposite direction.

4. User Requirements Definition

4.1 User Services

4.1.1 Password Creation Service:

The Door Locker Security System offers a user-friendly service for creating a secure system password. Users interact with the HMI_ECU through a 4x4 keypad, entering a 5-digit password. The system guides users through the process on the 2x16 LCD.

4.1.2 Door Unlocking Service:

To unlock the door, users enter their password via the keypad. The HMI_ECU sends the entered password to the CONTROL_ECU, which verifies it against the stored password in the EEPROM. Upon successful verification, the DC Motor is activated to unlock the door. The process is displayed on the LCD in real time.

4.1.3 Password Change Service:

Users have the option to change their system password. After entering the current password, a new password can be set using the same process as the password creation service. This ensures flexibility and security for users.

4.2 Non-functional System Requirements

2.1 Performance Requirements:

Response Time: The system should respond to user inputs within 1 second.
Motor Rotation Time: The DC Motor should complete a full rotation in 15 seconds during door unlocking/locking.
LCD Display Refresh Rate: The LCD should refresh at a rate of at least 1 Hz.

2.2 Reliability Requirements:

Password Verification Accuracy: The system should have a password verification accuracy of 99.9%.
Motor Reliability: DC Motor should operate without failure for a minimum of 10,000 rotations.

2.3 Usability Requirements:

User Guidance: The LCD should provide clear and concise guidance to users during all interactions.
Keypad Responsiveness: Keypad buttons should be responsive to user input without delay.

2.4 Security Requirements:

Password Storage: Passwords should be securely stored in the EEPROM using encryption techniques.
Buzzer Activation: In the event of three consecutive failed password attempts, the Buzzer should be activated, signaling a potential security breach.

4.3 Product and Process Standards

I2C Standard:

The system adheres to the I2C communication standard for interfacing with external EEPROM.

UART Standard:

The UART communication standard is followed by communication between HMI_ECU and CONTROL_ECU.

Timer1 Configuration Standard:

Timer 1 is configured according to established standards for precise timing operations.

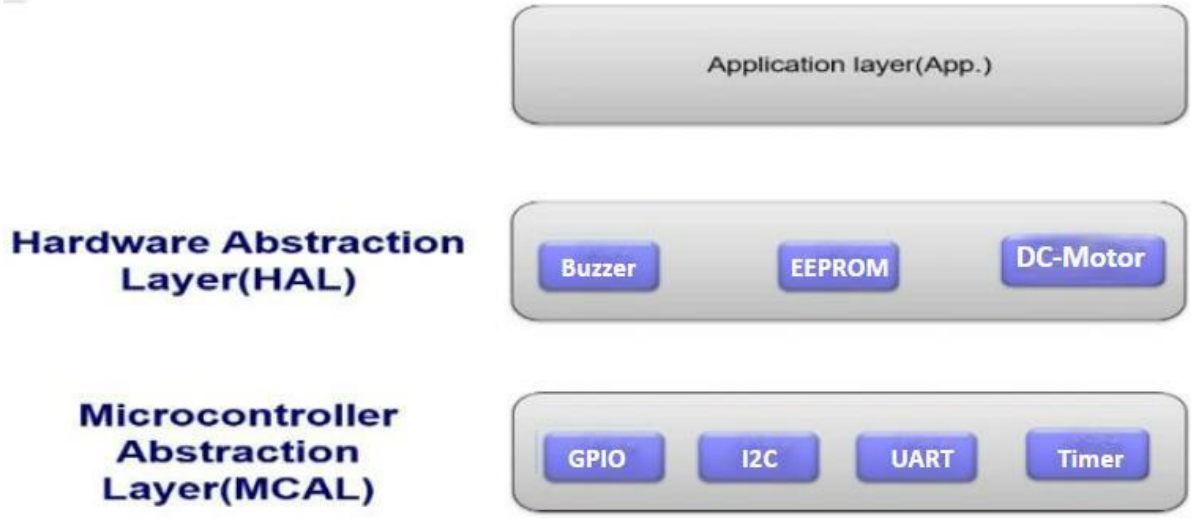
5. System Architecture

5.1 Architecture of HMI_MC1

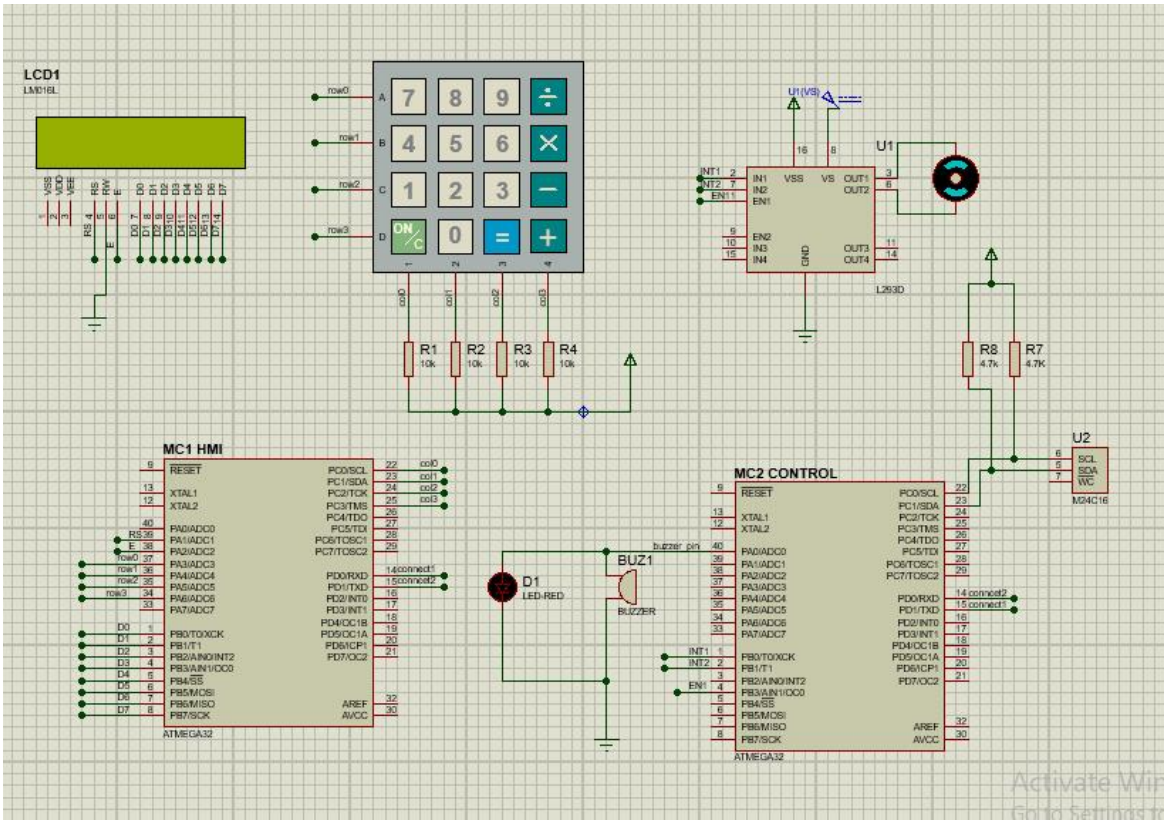
HMI_ECU (Human Machine Interface) with 2x16 LCD and 4x4 keypad.

5.2 Architecture of CONTROL_MC2

Control_ECU with EEPROM, Buzzer, and Dc-Motor.



5.3 Architecture of The Whole System



HMI_ECU (Mc1):

- Responsible for user interaction.
- Utilizes shared GPIO, LCD, and Keypad drivers.

CONTROL_ECU (Mc2):

- Manages core processing and decisions.
- Utilizes shared GPIO, Timer1, and UART drivers.
- Communicates with HMI_ECU through UART.
- Controls external components like DC Motor and Buzzer.

Shared Drivers:

- Components such as GPIO, LCD, Keypad, Timer1, and UART are designed as shared drivers.
- Reusable across both HMI_ECU and CONTROL_ECU for consistent functionality.

6. System Requirements Specification

6.1 Functional Requirements

6.1.1 Password Management

6.1.1.1 Password Creation

- User Input:
  - ✓ Users will input a 5-digit password through the 4x4 keypad on the HMI_ECU.
  - ✓ The system will display asterisks (*) on the 2x16 LCD screen for each entered digit.
- Confirmation Process:
  - ✓ After the initial password entry, users will be prompted to re-enter the same password for confirmation.
  - ✓ If the two entered passwords match, HMI_ECU will send the password to CONTROL_ECU via UART for storage in the EEPROM.
  - ✓ If not, users will go through the password creation process again.

6.1.1.2 Password Verification

- User Input:
  - ✓ To unlock the door, users will enter their password through the 4x4 keypad.
  - ✓ The HMI_ECU will send the entered password to CONTROL_ECU via UART.
- Verification Process:
  - ✓ CONTROL_ECU will compare the entered password with the stored password in the EEPROM.
  - ✓ If the passwords match, the system will proceed with door unlocking.
  - ✓ If not, users will be prompted to re-enter the password.

6.1.1.3 Password Change

- User Input:
  - ✓ Users can initiate the password change process by entering their current password through the keypad.
- Change Process:
  - ✓ If the entered password matches the stored password, users will be prompted to create a new password using the password creation process.

6.1.2 Door Control

6.1.2.1 Door Unlocking

- User Input:
  - ✓ Users enter their password via the keypad.
- Verification and Action:
  - ✓ The system verifies the entered password.
  - ✓ If successful, CONTROL_ECU activates the DC Motor to unlock the door.
  - ✓ LCDs real-time feedback on the unlocking process.

6.1.2.1 Door Locking

- User Input:
  - ✓ Users enter their password via the keypad.
- Verification and Action:
  - ✓ The system verifies the entered password.
  - ✓ If successful, CONTROL_ECU activates the DC Motor to lock the door.
  - ✓ LCDs real-time feedback on the locking process.

6.1.3 System Feedback

6.1.3.1 Information Display LCD

- ✓ The 2x16 LCD provides clear instructions and feedback during password creation, verification, and door control processes.
- ✓ Real-time status updates, error messages, and success messages are displayed.

6.1.3.2 Security Alert Buzzer

- ✓ In the event of three consecutive failed password attempts, the Buzzer is activated.
- ✓ The Buzzer provides an audible alert to signal a potential security breach.

6.2 Non-Functional Requirements

6.2.1 Performance Requirements

6.2.1.1 Response Time

- System Responsiveness
  The system should respond to user inputs within 1 second.

6.2.1.2 Motor Rotation Timing

- Door Control Timing
  The DC Motor should complete a full rotation in 15 seconds during door unlocking/locking.

6.2.1.3 LCD Display Refresh Rate

- LCD Display
  The LCD should refresh at a rate of at least 1 Hz.

6.2.2 Reliability Requirements

6.2.2.1 Password Verification Accuracy

- Verification Accuracy
  The system should have a password verification accuracy of 99.9%.

6.2.2.2 Motor Reliability

- DC-motor Operation
  The DC Motor should operate without failure for a minimum of 10,000 rotations.

6.2.3 Usability Requirements

6.2.3.1 User Guidance

- Clear Instructions
  The LCD should provide clear and concise guidance to users during all interactions.

6.2.3.2 Keypad Responsiveness

- Efficient User Input
  Keypad buttons should be responsive to user input without delay.

6.2.4 Security Requirements

6.2.4.1 Password Storage

- Secure Password Storage
  Passwords should be securely stored in the EEPROM using encryption techniques.

6.2.4.2 Buzzer Activation

- Security Breach Alert
  In the event of three consecutive failed password attempts, the Buzzer should be activated, signaling a potential security breach.

6.3 Interfaces to Other Systems

6.3.1 HMI_ECU to CONTROL_ECU Communication (UART)

- Data Exchange:
  The HMI_ECU communicates with the CONTROL_ECU using UART for sending and receiving password and control data.

6.3.2 CONTROL_ECU to External EEPROM (I2C)

- Secure Data Storage:
  CONTROL_ECU communicates with an external EEPROM using I2C for secure storage of system passwords.

7. System Model

7.1 Object Model

7.1.1 Purpose

The Object Model provides a graphical representation of the relationships between the key system components, emphasizing their interactions and dependencies.

7.1.2 Description

The Object Model will illustrate the main objects in the Door Locker Security System, including HMI_ECU, CONTROL_ECU, DC Motor, LCD, Keypad, and external components like EEPROM and Buzzer. Relationships, dependencies, and communication channels will be visually represented.

7.1.3 Example Object Model

1. HMI_ECU
   - Attributes:
     - LCD
     - Keypad
2. CONTROL_ECU
   - Attributes:
     - EEPROM
     - Buzzer
     - DC Motor
3. User
   - Attributes:
     - Password
4. System
   - Attributes:
     - Door State (Locked/Unlocked)
     - System Status

Relationships:

- HMI_ECU interacts with CONTROL_ECU through UART communication.
- CONTROL_ECU communicates with External EEPROM for password storage using I2C.
- CONTROL_ECU controls the DC Motor for door locking/unlocking.
- User interacts with HMI_ECU to input and manage passwords.
- HMI_ECU provides feedback to the User through the LCD.
- CONTROL_ECU triggers the Buzzer for security alerts.

7.2 Data-Flow Model

7.2.1 Purpose

The Data-Flow Model visually depicts the flow of data between different components of the system, emphasizing the movement and transformation of information.

7.2.2 Description

The Data-Flow Model will showcase how user inputs, passwords, and control signals flow between HMI_ECU and CONTROL_ECU. It will also illustrate how data is stored and retrieved from the external EEPROM.

1. User Input
   - Data Source: User (via Keypad)
   - Data Destination: HMI_ECU
   - Description: Represents the input of passwords from the user.

2. Password Data
   - Data Source: HMI_ECU
   - Data Destination: CONTROL_ECU
   - Description: Transmits password data from HMI_ECU to CONTROL_ECU for verification and storage.

3. Door Control Command
   - Data Source: HMI_ECU
   - Data Destination: CONTROL_ECU
   - Description: Instructs CONTROL_ECU to unlock or lock the door based on user input.

4. System Feedback
   - Data Source: CONTROL_ECU
   - Data Destination: HMI_ECU
   - Description: Sends feedback information (e.g., door status, security alerts) from CONTROL_ECU to HMI_ECU.

5. Security Alert
   - Data Source: CONTROL_ECU
   - Data Destination: Buzzer
   - Description: Activates the Buzzer for security alerts triggered by CONTROL_ECU.

6. LCD Display
- Data Source: CONTROL_ECU
- Data Destination: HMI_ECU
- Description: Informs HMI_ECU to display relevant information on the LCD.

7. Password Change Request
- Data Source: HMI_ECU
- Data Destination: CONTROL_ECU
- Description: Signals CONTROL_ECU that the user intends to change the password.

8. Password Change Data
- Data Source: HMI_ECU
- Data Destination: CONTROL_ECU
- Description: Transmits new password data from HMI_ECU to CONTROL_ECU for password change.

7.3 Semantic Data Model

7.3.1 Purpose

The Semantic Data Model provides a detailed representation of the data structures and their relationships within the system.

7.3.2 Description

The Semantic Data Model will illustrate how passwords are structured, stored, and accessed within the EEPROM. It will highlight the encryption techniques used for secure password storage.

7.3.3 Example Semantic Data Model

Semantic Data Model:

Entities:

1. User

- Attributes:

- UserID (unique identifier)

- Password

2. Door

- Attributes:

  - DoorID (unique identifier)

  - DoorState (Locked/Unlocked)

Relationships:

- A User can have multiple Passwords (one-to-many relationship).

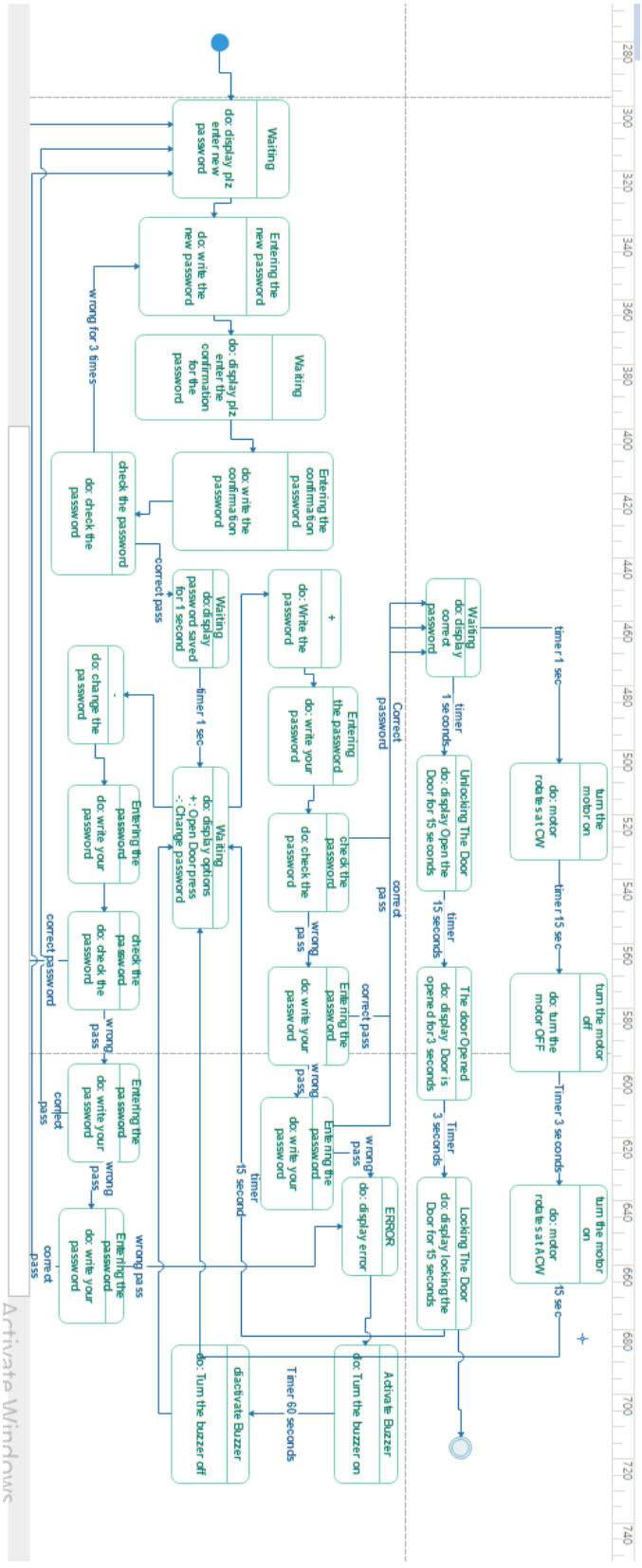
- CONTROL_ECU manages the state of the Door (one-to-one relationship).

- HMI_ECU interacts with User for input and provides feedback (association).

- CONTROL_ECU receives password data from HMI_ECU for verification (association).

- CONTROL_ECU triggers the Buzzer for security alerts (association).

7.4 State Diagram



8. System Evolution

8.1 Fundamental Assumptions

8.1.1 Purpose

This section outlines the fundamental assumptions upon which the Door Locker Security System is based. Recognizing these assumptions is crucial for system designers and developers to understand the foundational principles guiding the system's design and operation.

8.1.2 Assumptions

- User Competence:
  - Users are assumed to have basic competence in operating a keypad-based security system.
- Reliability of Components:
  - The hardware components, including the DC Motor, LCD, Keypad, and Buzzer, are assumed to operate reliably under normal conditions.
- Secure Environment:
  - The system assumes a physically secure environment where unauthorized access to the hardware components is limited.
- Stable Power Supply:
  - The system assumes a stable power supply for uninterrupted operation

8.2 Anticipated Changes

8.2.1 Purpose

This section addresses potential changes or evolutions that the Door Locker Security System may undergo in the future. Identifying these anticipated changes helps system designers avoid decisions that could impede adaptability to evolving requirements.

8.2.2 Anticipated Changes

- Hardware Evolution:

  Anticipate changes in hardware components, such as advancements in keypad technology or improvements in motor efficiency.

- User Interface Enhancements:

Future updates may involve enhancements to the user interface, possibly incorporating touchscreen technology or additional user authentication methods.

- Security Protocol Updates:

Changes in security standards or the discovery of new vulnerabilities may necessitate updates to the system's security protocols.

- Integration with Smart Home Systems:

  As smart home technologies evolve, there may be opportunities to integrate the Door Locker Security System with broader smart home ecosystems.

- User Feedback and Iterative Improvements:

Continuous user feedback may lead to iterative improvements in the system's usability and features.

8.2.3 Mitigation Strategies

- Modular Design:

Implement a modular design approach to facilitate the replacement or upgrade of individual components without affecting the entire system.

- Software Update Mechanism:

Incorporate a software update mechanism to allow for seamless updates to the system's firmware as needed.

- Open Communication Protocols:

Design communication protocols with openness to integration, ensuring compatibility with emerging technologies.

- User-Focused Development:

Prioritize user feedback and involve users in the development process to align system improvements with user needs.

9. Appendices

9.1 Hardware Requirements

9.1.1 Minimal Configuration

- **Microcontrollers**: Two ATmega32 Microcontrollers with a minimum frequency of 8MHz each.
- **Memory:** program memory and EEPROM space for storing passwords and system data.
- **Peripherals:**
  Input peripherals: 4x4 Keypad for user input.
  Output peripherals: 2x16 LCD for displaying system information.
- **Actuator:** DC Motor for controlling door lock/unlock.
- **Connectivity:**
  1. UART for communication between HMI_ECU and CONTROL_ECU.
  2. I2C for communication with external EEPROM.

9.1.2 Optimal Configuration

- **Microcontrollers**: Upgraded microcontrollers with higher processing speeds for improved system responsiveness.
- **Memory:** Increased program memory and EEPROM space to accommodate future feature enhancements.
- **Peripherals:** Upgraded LCD with enhanced display capabilities.
  Advanced keypad technology for improved user interaction.
- **Connectivity:**
  Enhanced communication interfaces for future expansion and integration with external systems.

9.2 Database Requirements

9.2.1 Logical Organization

- **Password Storage**: Passwords shall be securely stored in the EEPROM. Encryption algorithms shall be employed to ensure data security.
- **Data Relationships:** The EEPROM shall maintain a structured organization of data, including user passwords and system configuration settings.
- **Data Integrity**: Implement error-checking mechanisms to ensure the integrity of stored data.
- **Backup and Recovery:** Develop mechanisms for regular data backup to prevent data loss.
  Implement recovery procedures in case of unexpected data corruption.

9.2.2 Database Scalability

- **User Management**: Design the database to accommodate a scalable number of user profiles.

- **System Events:** Create provisions for storing and managing system events, such as door access attempts and security alerts.

9.2.3 Database Access Control

- **Read/Write Permissions**: Implement strict access control mechanisms to restrict unauthorized access to the database.
  Read and write permissions shall be defined based on user roles.
- **Audit Trails:** Maintain audit trails to track database access and modifications for security and accountability.

9.3 Database and Hardware Integration

- **Communication Protocols**: Define communication protocols between the CONTROL_ECU and the external EEPROM using I2C.
  Ensure secure data transfer between the microcontrollers and the storage device.
- **Real-Time Data Updates:**
  Establish mechanisms for real-time updates to the database as users interact with the system.

10. Index

10.1 Alphabetical Index

- 2x16 LCD
  - ✓ Information Display LCD, 6.1.3.1
- **4x4 Keypad**
  - ✓ Keypad Responsiveness, 6.2.3.2
- **Anticipated Changes**
  - ✓ Mitigation Strategies, 8.2.3
  - ✓ Purpose, 8.2.1
- **Architecture of CONTROL_MC2**
  - ✓ System Architecture, 5.2
- **Architecture of HMI_MC1**
  - ✓ System Architecture, 5.1
- **Architecture of The Whole System**
  - ✓ System Architecture, 5.3
- **Assumptions**
  - ✓ Assumptions, 6.1
  - ✓ Purpose, 6.1.1
- **Buzzer**
  - ✓ Buzzer Activation, 6.2.4.2
  - ✓ Security Alert Buzzer, 6.1.3.2
  - ✓ Buzzer Feedback, 2.3.2
- **CONTROL_ECU**
  - ✓ HMI_ECU to CONTROL_ECU Communication (UART), 6.3.1
- **Data-Flow Model**
  - ✓ Data-Flow Model, 7.2
- **DC Motor**
  - ✓ Motor Reliability, 6.2.2.2
  - ✓ Door Locking, 6.1.2.2
  - ✓ Door Unlocking, 6.1.2.1
- **Door Locker Security System**
  - ✓ Glossary, 3.1
- **EEPROM**
  - ✓ Database and Hardware Integration, 9.3
  - ✓ Database Requirements, 9.2
  - ✓ External EEPROM (I2C), 6.3.2
- **Expected Readership**
  - ✓ Preface, 1.1
- **Fundamental Assumptions**
  - ✓ Anticipated Changes, 8.2
  - ✓ Purpose, 8.1.1
- **GPIO (General Purpose Input/Output)**
  - ✓ GPIO Driver Requirements, 9.1
- **Glossary**
  - ✓ Glossary, 3
- **HMI_ECU (Human Machine Interface)**
  - ✓ HMI_ECU to CONTROL_ECU Communication (UART), 6.3.1

- ✓ Architecture of HMI_MC1, 5.1

- **I2C (Inter-Integrated Circuit)**
  - ✓ External EEPROM (I2C), 6.3.2
  - ✓ Database and Hardware Integration, 9.3
- **Integration with Other Systems**
  - ✓ Integration with Other Systems, 2.3
- **Introduction**
  - ✓ Introduction to the Need for the System, 2.1
- **Password Creation**
  - ✓ Password Creation, 6.1.1.1
- **Password Management**
  - ✓ Password Verification, 6.1.1.2
  - ✓ Password Change, 6.1.1.3
- **Performance Requirements**
  - ✓ Motor Rotation Time, 6.2.1.2
- **Preface**
  - ✓ Preface, 1
- **Product and Process Standards**
  - ✓ Non-functional System Requirements, 4.3
- **Real-Time Data Updates**
  - ✓ Database and Hardware Integration, 9.3
- **Reliability Requirements**
  - ✓ Password Verification Accuracy, 6.2.2.1
- **Rationale for new versions**
  - ✓ Preface, 1.3
- **Response Time**
  - ✓ Performance Requirements, 6.2.1.1
- **Semantic Data Model**
  - ✓ Semantic Data Model, 7.3
- **Security Alert Buzzer**
  - ✓ Security Alert Buzzer, 6.1.3.2
  - ✓ Buzzer Feedback, 2.3.2
- **Security Requirements**
  - ✓ Security Requirements, 6.2.4
- **Summary of changes in versions**
  - ✓ Preface, 1.4
- **System Architecture**
  - ✓ System Architecture, 5
- **System Evolution**
  - ✓ Fundamental Assumptions, 8.1
- **System Feedback**
  - ✓ System Feedback, 6.1.3
- **System Functions**
  - ✓ System Functions, 2.2
- **System Models**
  - ✓ System Models, 7
- **System Requirements Specification**
  - ✓ System Requirements Specification, 6

- **Terms Specific to Door Locker Security System Operations**
  - ✓ Terms Specific to Door Locker Security System Operations, 3.13
- **Timer 1**
  - ✓ Timer 1, 3.12
- **UART (Universal Asynchronous Receiver-Transmitter)**
  - ✓ HMI_ECU to CONTROL_ECU Communication (UART), 6.3.1
  - ✓ UART Driver Requirements, 9.1
- **User Guidance**
  - ✓ Usability Requirements, 6.2.3.1
- **User Requirements Definition**
  - ✓ User Requirements Definition, 4
- **User Services**
  - ✓ User Services, 4.1
- **Usability Requirements**
  - ✓ Usability Requirements, 6.2.3
- **Version History**
  - ✓ Version History, 1.2
- **Version History and Summary of Changes**
  - ✓ Preface, 1.2

10.2 Diagram Index

Object Model

Purpose: Describes the organization of system components.
Location: Section 7.1
Example: Figure 7.1.3

Data-Flow Model

Purpose: Illustrates the flow of data between system modules.
Location: Section 7.2
Example: Figure 7.2.3

Semantic Data Model

Purpose: Represents the meaning and relationships of data elements.
Location: Section 7.3
Example: Figure 7.3.3

10.3 Function Index

Password Management
- **6.1.1 Password Creation**
  - **Purpose:** Define how passwords are created.
  - **Location:** Section 6.1.1.1
- **6.1.1.2 Password Verification**
  - **Purpose:** Specify the process for verifying passwords.
  - **Location:** Section 6.1.1.2
- **6.1.1.3 Password Change**
  - **Purpose:** Describe the procedure for changing passwords.
  - **Location:** Section 6.1.1.3

Door Control
- **6.1.2.1 Door Unlocking**
  - **Purpose:** Define the steps for unlocking the door.
  - **Location:** Section 6.1.2.1
- **6.1.2.2 Door Locking**
  - **Purpose:** Specify the process for locking the door.
  - **Location:** Section 6.1.2.2

System Feedback
- **6.1.3.1 Information Display LCD**
  - **Purpose:** Describe how information is displayed on the LCD.
  - **Location:** Section 6.1.3.1
- **6.1.3.2 Security Alert Buzzer**
  - **Purpose:** Define the activation of the security alert buzzer.
  - **Location:** Section 6.1.3.2

Performance Requirements
- **6.2.1.1 Response Time**
  - **Purpose:** Specify the expected response time.
  - **Location:** Section 6.2.1.1
- **6.2.1.2 Motor Rotation Time**
  - **Purpose:** Define the time for motor rotation.
  - **Location:** Section 6.2.1.2
- **6.2.1.3 LCD Display Refresh Rate**
  - **Purpose:** Specify the refresh rate for the LCD display.
  - **Location:** Section 6.2.1.3

Reliability Requirements
- **6.2.2.1 Password Verification Accuracy**
  - **Purpose:** Define the accuracy of password verification.
  - **Location:** Section 6.2.2.1
- **6.2.2.2 Motor Reliability**
  - **Purpose:** Specify the reliability requirements for the motor.
  - **Location:** Section 6.2.2.2

Usability Requirements
- **6.2.3.1 User Guidance**

Purpose: Define how user guidance is provided.
Location: Section 6.2.3.1

6.2.3.2 Keypad Responsiveness

Purpose: Specify the responsiveness of the keypad.
Location: Section 6.2.3.2

Security Requirements

6.2.4.1 Password Storage

Purpose: Specify how passwords are stored securely.
Location: Section 6.2.4.1

6.2.4.2 Buzzer Activation

Purpose: Define the activation of the buzzer for security.
Location: Section 6.2.4.2

Interfaces to Other Systems

6.3.1 HMI_ECU to CONTROL_ECU Communication (UART)

Purpose: Describe the communication interface between HMI_ECU and CONTROL_ECU using UART.
Location: Section 6.3.1

6.3.2 CONTROL_ECU to External EEPROM (I2C)

Purpose: Describe the communication interface between CONTROL_ECU and External EEPROM using I2C.
Location: Section 6.3.2