Project 01: Home Safe

Software Requirements Specification
SRS Version 2

Team 01

Marina Seheon (Manager)
Andrei Phelps (Document Manager)
Luke McDougall (Lead Software Engineer)
Jack Vanlyssel
Spoorthi Menta
Vamsi Krishna Singara

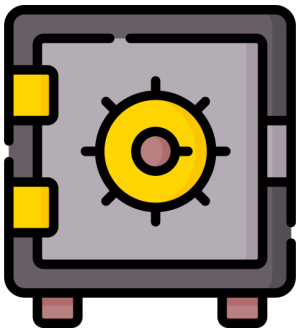

Image courtesy of Flaticon.com [3].

CS460: Software Engineering

Table of Contents

1 Introduction **2**

2 Definition of Terms **2**

3 General Description **2**

4 Specific Requirements **3**
4.1 External Interfaces 4
4.1.1 Input Events 4
4.1.2 Output Events 4
4.2 Internal Interfaces 5
4.2.1 Microcontroller 5
4.2.2 Software 5
4.2.3 Lock Mechanism 5
4.2.4 Lock Sensors 5
4.3 Control Logic 5
4.3.1 Initial Setup Process 5
4.3.2 Authorization 6

5 Design Constraints **7**

1 Introduction

In today's homes, safes have become commonplace, and digital safes are increasingly favored by Americans for their convenience and heightened security features. Our product, HomeSafe, has been meticulously designed with the vigilant consumer in mind, catering to those who value convenience, security, and reliability. It distinguishes itself through a streamlined setup process, robust biometric two-factor authentication (2FA), user monitoring for access control, and an auxiliary power source. While mirroring the user experience of a typical digital safe, HomeSafe aims to encompass a unique set of features typically associated with commercial-grade safes.

The Software Requirements Specification (SRS) provides a comprehensive insight into the features, external and internal interfaces, control logic, and design constraints of HomeSafe. The system employs a dynamic model based on the Object Modeling Technique (OMT) to direct and structure user interactions with the product, effectively governing the control flow within the system.

As previously detailed in the Requirements Definitions Document (RDD), the core requirements formulated by the marketing team encompass multi-user capability, enhanced security via 2FA, user-friendly setup and maintenance, and continuous security and access. These fundamental requirements lay the groundwork for HomeSafe's development, guiding the organization of its components to achieve these objectives. The RDD outlines the capabilities and design constraints essential for realizing HomeSafe's overarching goals.

2 Definition of Terms

This section provides definitions for critical terms recurrently utilized throughout the document. This section can be a reference point for readers engaging with the content.

I. **Administrator**: An individual with authority to establish and oversee separate user profiles within the system, regulating user access to the system's settings and contents.

II. **Auxiliary**: An additional or secondary power source that supports the main or primary power supply. An auxiliary power source is typically used to provide backup, redundancy, or temporary power when the main power source is unavailable, disrupted, or insufficient.

III. **Bio-Metric Scanner**: A technology that identifies and authenticates users based on their unique biological characteristics, typically fingerprints, retina patterns, or other traits.

IV. **Microcontroller**: A microcontroller is a small integrated circuit serving as the central processing unit (CPU) of a safe's electronic system. It contains a processor, memory, and input/output ports and can include programmable capabilities. Microcontrollers manage the safe's tasks, user input, security protocols, and control functions, including locks, interface interactions, and external device communication.

V. **Personal Identification Number (PIN)**: A numerical code that serves as a security credential used to authenticate and verify the identity of an individual. PINs are commonly used in various systems, such as electronic devices, bank accounts, and access control systems, to ensure that only authorized users can gain access.

VI. **Two-Factor Authentication (2FA)**: A security protocol that requires users to provide two distinct forms of verification to access a system. This commonly involves a combination of something known (such as a password), and something possessed (such as a generated code or biometric information), adding an extra layer of security and protection against unauthorized access [2].

3 General Description

At the core of our software architecture lies the microcontroller, serving as the pivotal component responsible for overseeing all of HomeSafe's operations. This microcontroller is the nexus, intricately linked to all the physical elements housed within HomeSafe. It adeptly manages inputs from various input devices and orchestrates the delivery of corresponding outputs to designated output devices. To enable its functionality, the microcontroller is programmed using our custom-developed software, ensuring the precise execution of desired operations.

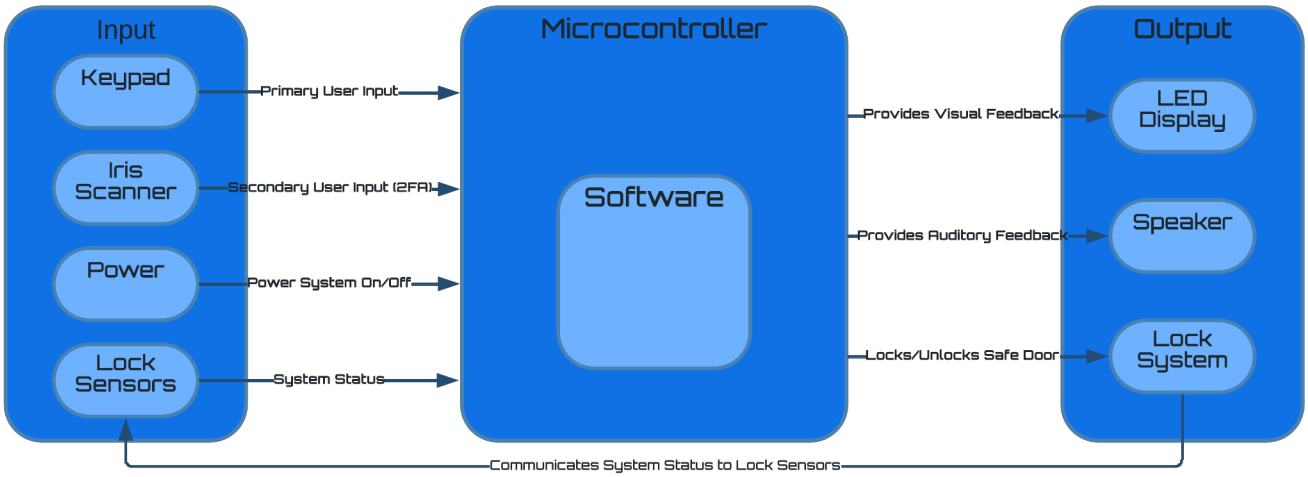

Figure 1: Block Diagram of HomeSafe System [4]

- **Keypad**: The software permits users to enter their assigned PIN using the numeric keys 0-9. Any key press triggers the LED display screen and speaker to offer visual and auditory feedback. Upon successful identity verification via the correct passkey, the software sends a signal to the microcontroller, activating the iris scanner for two-factor authentication (2FA). After inputting the entire PIN, the user must press the ENTER button to initiate password verification. In the case of an erroneous number entry during PIN input, the user can press the CANCEL button to abort the entry attempt and reset the procedure.
- **Iris Scanner**: The software allows users to input data through the Iris Scanner after successfully verifying the PIN. After completing the PIN verification, the system will prompt the user for an iris scan. Once the iris scan is completed and the user's identity is confirmed, access to the safe is granted. Visual and auditory notifications are provided through the LED Display and Speaker, and a signal is sent to the Lock System to switch the safe's status from LOCKED to UNLOCKED.
- **Power**: When you press this button, the system will initiate, showing the main menu for PIN input on the LED Display. A startup sound will also emanate from the Speaker, signaling the user that the system is operational. It's important to note that the system can only be powered off when in the LOCKED state. If the user tries to power off the procedure while in this state, a warning message will be displayed on the LED screen.
- **Lock Sensors**: The interface tasked with conveying the current status of the HomeSafe (whether in the LOCKED or UNLOCKED state) to the microcontroller.
- **LED Display**: The LED (Light Emitting Diode) display is a visual interface for user interaction. Its primary role is to initiate user input and, when input is made via the keypad, to provide feedback by indicating the current number of characters entered. Furthermore, it can convey additional information, such as system warnings or low-power notifications, to the user.
- **Speaker**: A micro-speaker is integrated into the HomeSafe to convey auditory feedback to the user when buttons are pressed.
- **Lock Mechanism**: This system's role is to authorize entry into the HomeSafe once user authentication is completed. Upon successful authentication, the microcontroller transmits a signal to the lock mechanism, releasing the latch and making the door accessible for the user to open. This system also communicates with the Lock Sensors, which transmit this information to the software and allow further operation.

4 Specific Requirements

In this section, we take a deep dive into the inner workings of the system logic and how it reacts to the full spectrum of user interactions. We'll uncover how our software interprets and handles these interactions, giving you a clear picture of how HomeSafe smoothly manages its operations in response to diverse user actions and inputs.

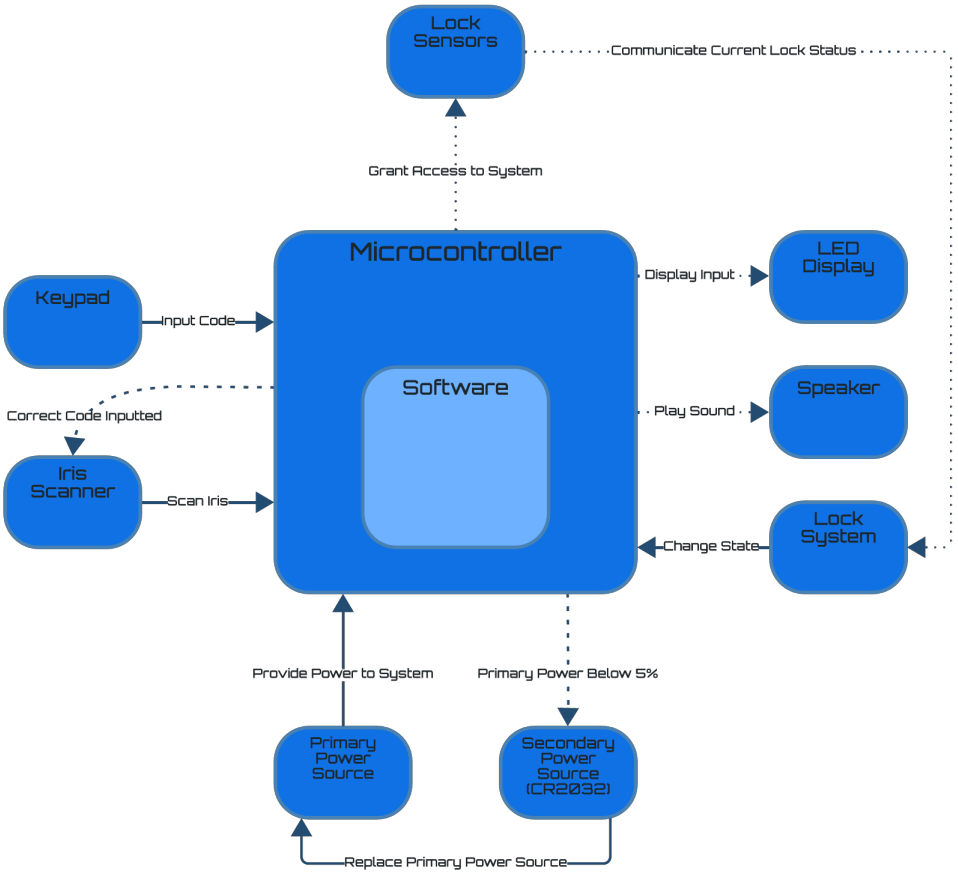

Figure 2: Logical Diagram of HomeSafe System [4]

4.1 External Interfaces

The software residing on the microcontroller governs all communication between the input and output components. Figure 2 provides a graphical representation of the physical input channels and the feasible output channels they can activate. Section 3.1 elaborates on the dynamics of interactions occurring between these inputs and outputs, while Section 3.2 illustrates the system's control flow using transition-state models.

4.1.1 Input Events

The interaction between users and the safe is facilitated through the keypad, iris scanner, and lock sensors, each serving a vital role in ensuring security and accessibility.

- **Keypad**: For user authentication, individuals can enter their assigned PIN using the software's numeric keys 0-9. Each keypress prompts both visual and auditory feedback from the LED display screen and speaker. Upon entering the correct PIN, the software interacts with the microcontroller, activating the iris scanner for enhanced two-factor authentication (2FA). To proceed with PIN verification, users should press the ENTER button after keying in their full PIN.
- **Iris Scanner**: This system represents the second user authentication layer. After successful PIN verification, the software allows users to input data through the Iris Scanner. After validating the PIN, the system prompts the user for an iris scan. Upon the successful completion of the iris scan and the subsequent confirmation of the user's identity, access to the safe is authorized. Visual and auditory notifications are provided through the LED Display and Speaker to enhance user understanding and engagement. Simultaneously, a signal is dispatched to the Lock System, orchestrating the transition of the safe's status from LOCKED to UNLOCKED, ensuring a robust and multi-tiered security approach.

4.1.2 Output Events

The channels where the safe interacts with the input mechanisms are the LED Display, Speaker, and Lock System.

- **LED Display**: The LED display serves as a visual interface for user interaction, primarily initiating input and providing character count feedback when using the keypad. Additionally, it communicates important system information, such as warnings and low-power notifications, to the user.
- **Speaker**: A micro-speaker is seamlessly integrated into the HomeSafe, designed to deliver auditory output events to the user in response to button presses.

4.2 Internal Interfaces

This subsection delves into the essential internal components that make the system function seamlessly: the microcontroller, software, locking mechanism, and lock sensors.

4.2.1 Microcontroller

Serving as the system's central intelligence hub, the microcontroller is powered by the batteries and acts as the core decision-making unit. It receives and interprets various inputs, ensuring they are processed accurately before conveying any corresponding output to the user. In addition, the microcontroller requires power to store and manage crucial user data, including PINs and biometric information, contributing to the system's robust security framework.

4.2.2 Software

The software is the critical bridge between the user and the system's hardware components. It operates with the microcontroller to manage user interactions and authentication processes. The software ensures that the user's input is processed correctly, and it facilitates communication between the various hardware components to provide a seamless and secure user experience.

4.2.3 Lock Mechanism

The lock mechanism's primary role is granting entry into the HomeSafe once user authentication is completed. Upon successful authentication, the microcontroller, in conjunction with the software, transmits a signal to the lock mechanism, effectively releasing the latch and permitting the user to access the contents of the safe.

4.2.4 Lock Sensors

Integral to the security of the HomeSafe, the lock sensors continuously monitor the status of the safe's door, accurately detecting whether the locking mechanism is in a locked or unlocked state. This crucial information is communicated to the microcontroller and software, ensuring real-time awareness of the safe's security status and allowing the system to respond promptly to user actions and the safe's condition.

4.3 Control Logic

The control flow of the system orchestrates various operations to ensure the secure and efficient functionality of the safe. This section outlines the process of setting up initial user credentials and subsequent actions within the system.

4.3.1 Initial Setup Process

This section delineates the process through which users set their PIN and input their iris scan to secure access to the safe. Upon receipt, the safe remains locked but is energized by a functioning battery and features an active keypad. The individual endowed with the master PIN, supplied with the safe, assumes the role of the administrator.

Enclosed with the safe is a user guide, the final page of which prominently displays a unique 6-digit master PIN. On powering up the safe for the first instance, users are guided to input this master PIN to kickstart their credential configuration. Post the master PIN's successful recognition, users are then ushered to determine their individual 6-digit PIN. Subsequent to setting this PIN, the system beckons for an iris scan to bolster the authentication process. After the successful capture of the iris scan, the user profile is constituted, and the data anchored securely to the microcontroller.

Having successfully registered both the personal PIN and the iris scan, the safe affords access, preserving the user's details with utmost confidentiality. Crucially, the master PIN not only facilitates the preliminary

setup but also stands as a lifeline for recovery, should a user misplace their personal PIN. Upon wrapping up the initial setup, this configuration mode is sealed within the microcontroller, and reverting or altering it demands intervention from the manufacturer.

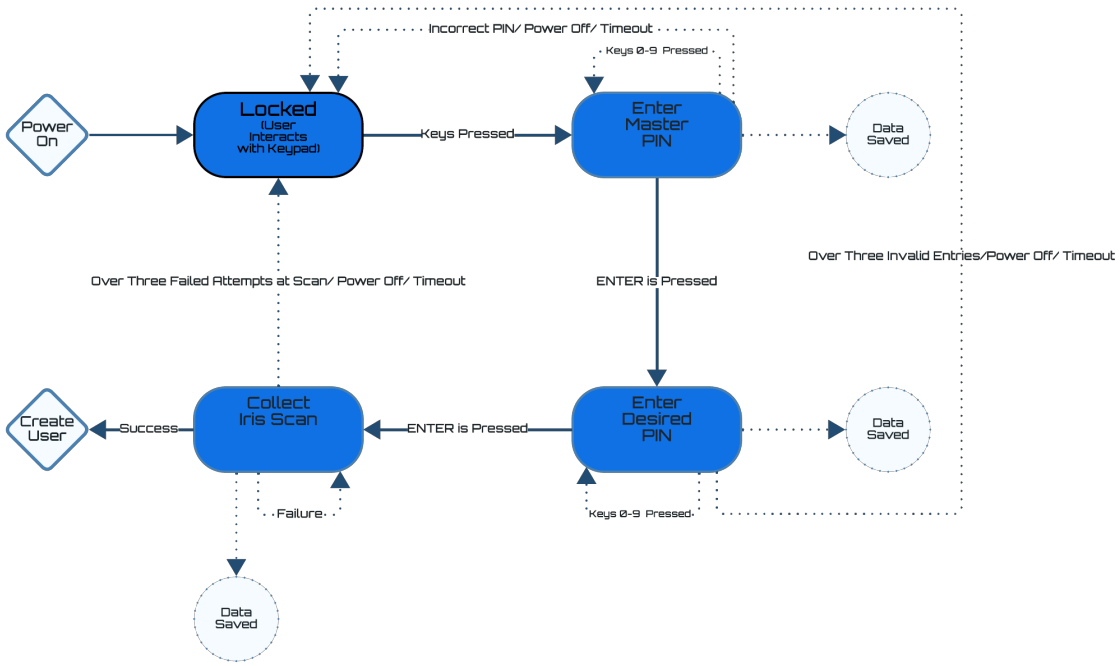

Figure 3: Dynamic OMT Diagram of the Initial Setup Process [4]

4.3.2 Authorization

In the framework of control logic, this section steers through the pivotal steps required for users to gain authorization to the safe. The process initiates with a secured door fronted by an active keypad. To kick off the authentication, users power on the safe and key in their personal 6-digit PIN. Following the system's acknowledgment of the entered PIN, the subsequent stage ushers in the Iris Scanner - a lynchpin in ensuring advanced authentication.

Users are then prompted to provide a single iris scan through the scanner interface. This captured scan is securely stored and cross-referenced by the system during subsequent access attempts. In scenarios where a user's iris scan doesn't match the saved data, or if unsuccessful matching ensues thrice in a row, the safe enforces a one-hour lockout. Persistent lockouts necessitate the intervention of the master PIN to reaccess the safe, ensuring an elevated layer of security, thereby making it virtually impregnable.

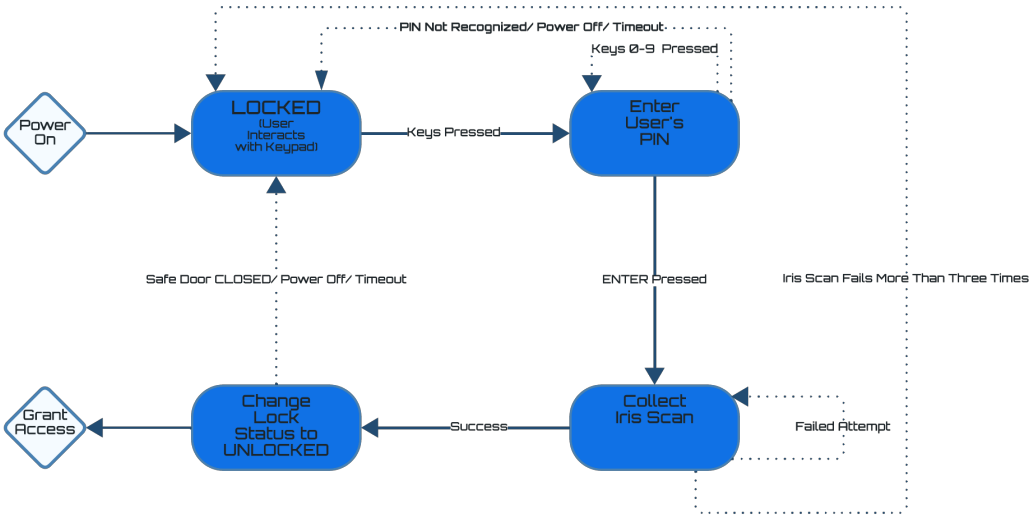

Figure 4: Dynamic OMT Diagram of the Authorization Process [4]

5 Design Constraints

- The control software for HomeSafe is crafted using Java, which means it operates within the confines and opportunities presented by an object-oriented programming language. This choice of language enables a structured and modular design approach, allowing for the efficient management of complex system behaviors. However, it also implies certain limitations associated with Java-based applications' performance and resource utilization.
- The auxiliary power supply, a single CR2032 cell battery, can sustain the system for an estimated ten years [1]. However, suppose the additional power supply depletes before the primary power source is reinstated (two non-rechargeable alkaline AA batteries). All user data will be forfeited, rendering the unit's contents inaccessible. Additionally, due to the microcontroller's exclusive control over the lock mechanism, manual operation of the safe box is not feasible. Consequently, should both the primary and secondary power sources fail, none of the users will possess the means to access HomeSafe.
- The HomeSafe is 12 x 16 x 12 inches (L x W x H). This may limit how much the customer can store inside.

References

[1] *Everything You Need To Know About The CR2032 Battery — microbattery.com.* https://www.microbattery.com/blog/post/battery-bios:-everything-you-need-to-know-about-the-cr2032-battery/. [Accessed 27-AUG-2023].

[2] Kathleen Garska. *Two-Factor Authentication (2FA) Explained: Biometric Authentication — blog.identityautomation.com* https://blog.identityautomation.com/mfa-face-off-series-biometric-authentication. [Accessed 27-AUG-2023].

[3] https://www.facebook.com/flaticon. *Safe Deposit free icons designed by Freepik — flaticon.com.* https://www.flaticon.com/free-icon/safe-deposit_3073524?term=safe&page=1&position=26&origin=search&related_id=3073524. [Accessed 25-AUG-2023].

[4] *Lucid visual collaboration suite: Log in — lucid.app.* https://lucid.app. [Accessed 09-SEP-2023].