CS350 Safehome Project
Software Requirement Specification (SRS)

Project Team #6 Members:

20140576	Geunyeong Cheon
20220809	Alan Zhainar
20220814	Yernaz Akhmetov
20256402	Arda Eren

Korea Advanced Institute of Science and Technology

Table of Contents

I. Overview

1. Introduction

Safehome is a new product for home automation. Private homeowners or small business can now think of using a Universal device that they can use to access their property with much ease, flexibility and mobility. Safehome makes this possible by bringing together all the innovative ideas relating to manage the work of a house owner using the latest technology equipments both remotely and locally. Automation has been made feasible by the widely used wireless equipments.

The product is quite comprehensible in the current market when more and more people are becoming mobile and ubiquitous. Amongst the most thought about targets, Safehome focuses on making the home absolutely safe. It provides a convenient way to secure the property for those who require both accessibility and quality of service.

To start with, the first version of Safehome will include only the security and surveillance functions. Safehome is thought to attract huge number of customers and make a high turnover over a year. Besides fulfilling the basic requirements of security and surveillance, this product will also be standardized to cope with the needs to become Universal device by adding additional functionalities like management, subscription, etc.

2. Goal

Providing all the functions for a safe, secure and managed home is the primary goal of this whole project. The customer who uses this product will be ensured that the home is safe.

Functional goal is to provide the followings:

1) Security functions
2) Surveillance functions

Non-functional goal is as follows:

1) To fulfill customer satisfaction
2) To provide highest level of assurance and guarantee
3) Timely product delivery
4) To make profit

In order to make Safehome features standardized and concurrent with user's requirements we will also have to consider the followings:

1) *Completeness* - The Safehome system we develop has all the function specified in the function requirements below.
2) *Reliability* - The Safehome system we develops provide reliable services for all the functions even in an emergency or an unexpected situation.
3) *Simplicity* - We follow the basic principle, "Keep It Simple," in the entire process framework: communication, planning, modeling, construction and deployment. So the entire development process is not very complex and the time to process the work is managed within the planned schedule.

4) *Customized service* - The Safehome system should be configured for a specific homeowners' environment considering the house, life pattern, and personal requirements.
5) *User-friendliness* - The Safehome system has user-friendly interface that homeowners can access anywhere, anytime with ease.

3. Major Functionalities

1) Security Management

The security functions in Safehome product allows the homeowner to arm/disarm system through the control panel or through the web browser and enables the homeowner to respond to an unauthorized access monitored by sensors such as window sensors, door sensors and motion sensors. It also provides functions such as creating and managing safety zone, changing the master password, and configuring system settings such as delay time, master password, guest password, phone number.

To arm/disarm the system the user has to use passwords to authenticate his identity. The home may be set to any of these statuses like away, home, extend travel, overnight travel. The user can arm/disarm specific safety zones too.

When there is an authorized access monitored by sensors, the system will raise an audible alarm and call for monitoring service to provide information about the location and report the nature of the event that has been detected. It also will display alarm message on the control panel as well as on the web application of Safehome product. The user can use panic buttons any time on the control panel to call monitoring service in emergency situations.

2) Surveillance Management

The surveillance function in Safehome product facilitates the homeowner to observe the house locally and/or remotely. The user can view cameras by selecting from a thumbnail or floor plan, zoom or pan cameras, enable/disable them, and restrict access to specific cameras. The surveillance video may be recorded to be viewed later.

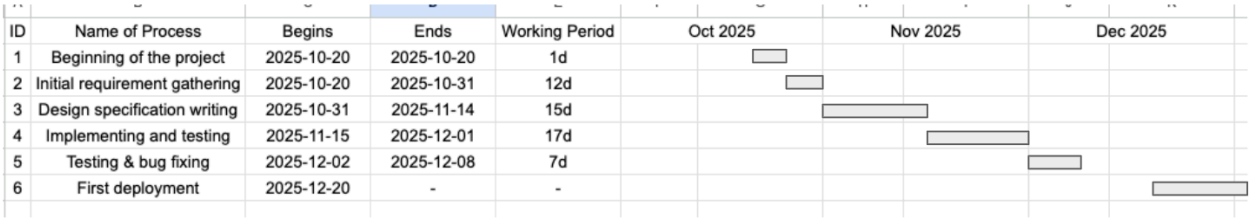
II. Project Schedule

The project will proceed following the concept of incremental software development model. The security functions, surveillance functions and the web access functions which are the core of the Safehome product will be developed in the first increment. Other functions such as home management functions - controlling the wireless electronic devices – will be developed in the later increments.

Plan for first increment

Beginning of the project	Oct 20, 2025
Initial requirement gathering	Oct 20 - Oct 31, 2025
Design specification writing	Oct 31 - Nov 14, 2025
Implementing and testing	Nov 15 - Dec 1, 2025
Testing & bug fixing	Dec 2 - Dec 8, 2025
First deployment	Dec 20, 2025 -

ID	Name of Process	Begins	Ends	Working Period
1	Beginning of the project	2025-10-20	2025-10-20	1d
2	Initial requirement gathering	2025-10-20	2025-10-31	12d
3	Design specification writing	2025-10-31	2025-11-14	15d
4	Implementing and testing	2025-11-15	2025-12-01	17d
5	Testing & bug fixing	2025-12-02	2025-12-08	7d
6	First deployment	2025-12-20	-	-



III. Prototype GUI

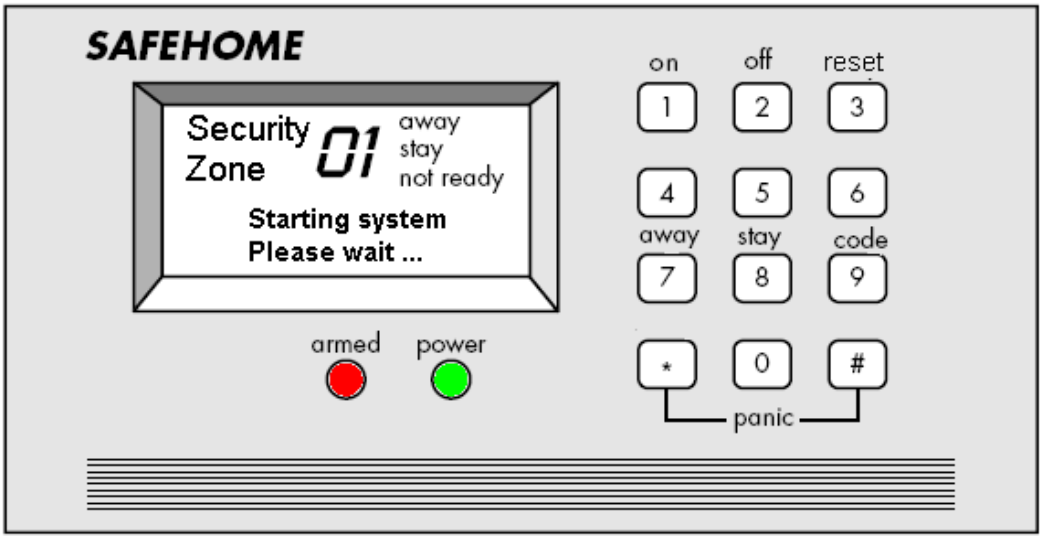


Fig 1. Control Panel

Fig 2. Login Screen

Fig 3. MainFunctions

Fig. 4 Security Function – Safety zone

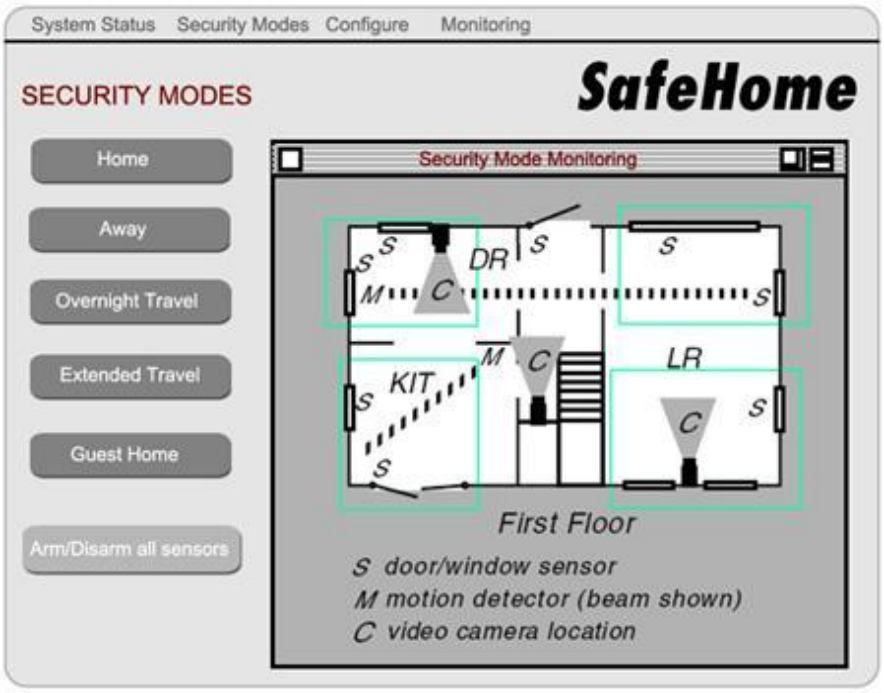


Fig. 5 Security Function – Security Mode

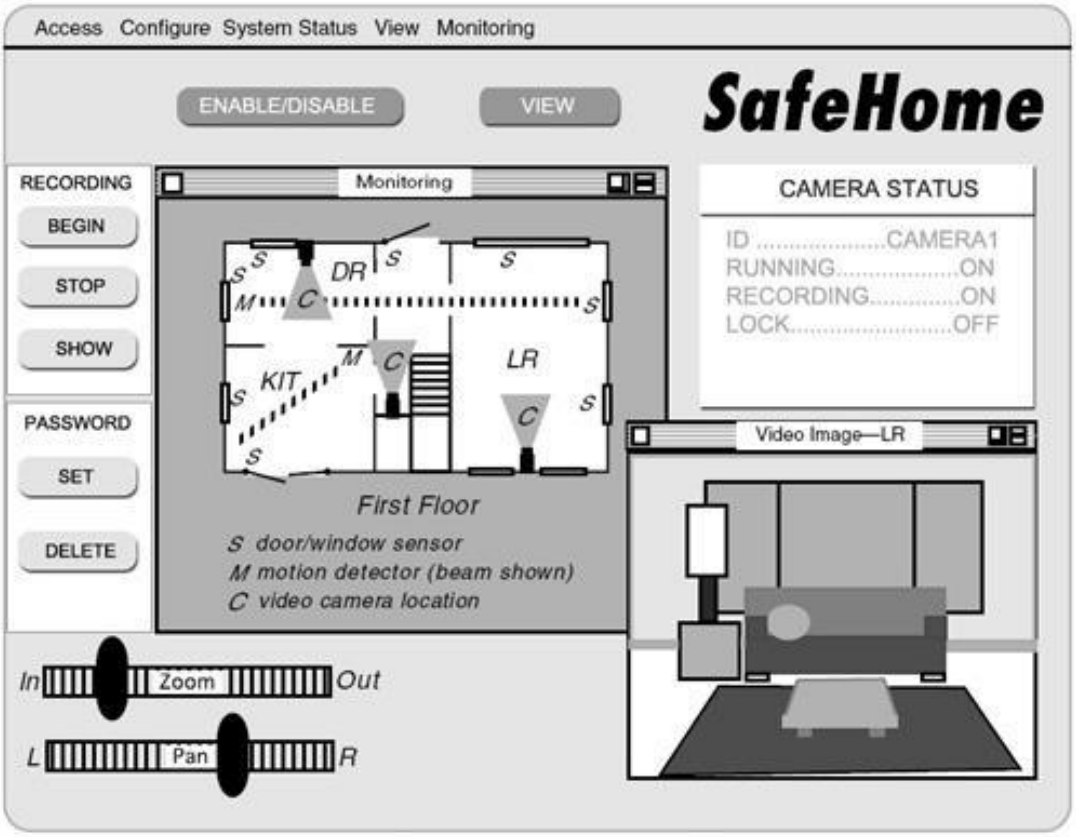


Fig. 6 Surveillance Function.

IV. Assumptions

1. Camera monitoring zone in page 30, 31 is defined as camera pan/zoom control

2. Floor plan configuration and hardware deployment is complete and out of the scope of our project.

3. Reconfiguring the floor plan or relocating the sensors or cameras are not in the scope of our project.

4. “set alarm” on slide 58 is setting delay time defined in the use case “configure system setting”

5. “configure Safehome system parameters” on page 21 is defined as “configure system setting”

6. “encounters an error condition” on slide 32-33 is not defined as an use case but is described in exceptions of each use cases

7. reconfigure sensors on page 71 is considered as setting floor plan which is not in the scope of our project.

8. “system administrator” in our use case scenarios is not a person who is in charge of managing the system. It is the system itself acting as a facilitator for the use of system functionalities.

9. Doggie angst sensor on page 59 is considered to be implemented in the next increment

10. Enable/test/read/disable sensors on page 94-95 is for test cases. We only control sensors through changing house safety situations or by arming/disarming safety zones.

11. We do not consider web pages selling product on page 73

12. We added function to view intrusion log on the web page

13. We added enabling and disabling all the cameras

14. Camera password is optional as shown on Slide 31

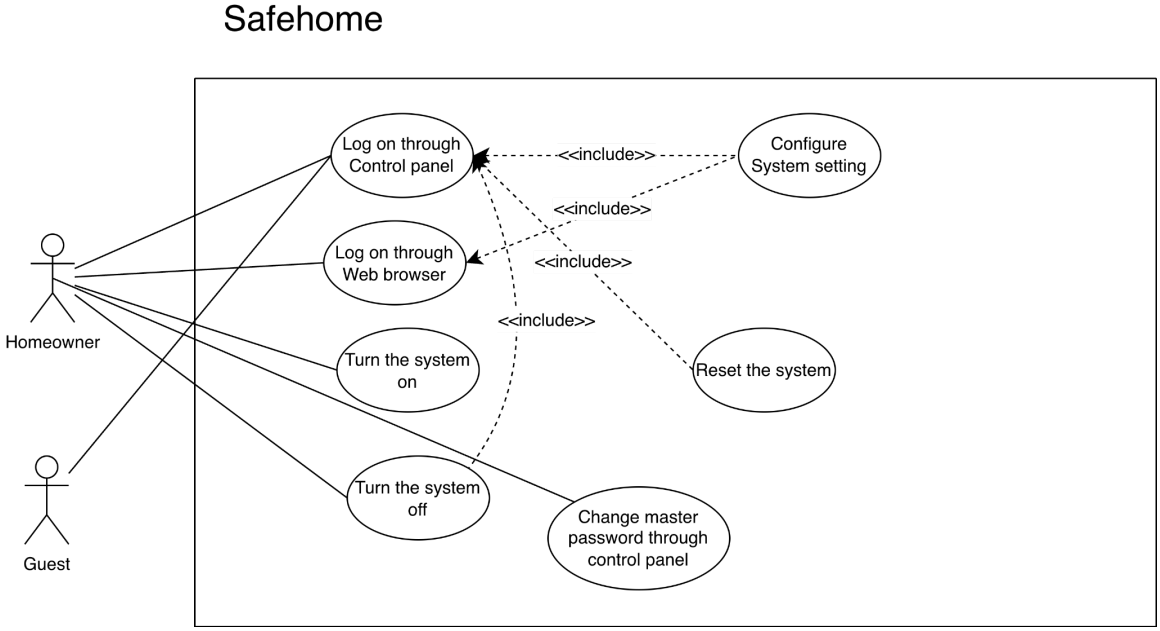
15. Internet access for security and surveillance is a mandatory feature for the first increment.This was referenced on slide 27

16. A dedicated native mobile application is out of scope for this increment. This was referenced on slide 75-77

17. The web interface will include alternate pages or views to support visually impaired users. This was referenced on slide 65

V. Use Case Diagrams

1. Common Functions



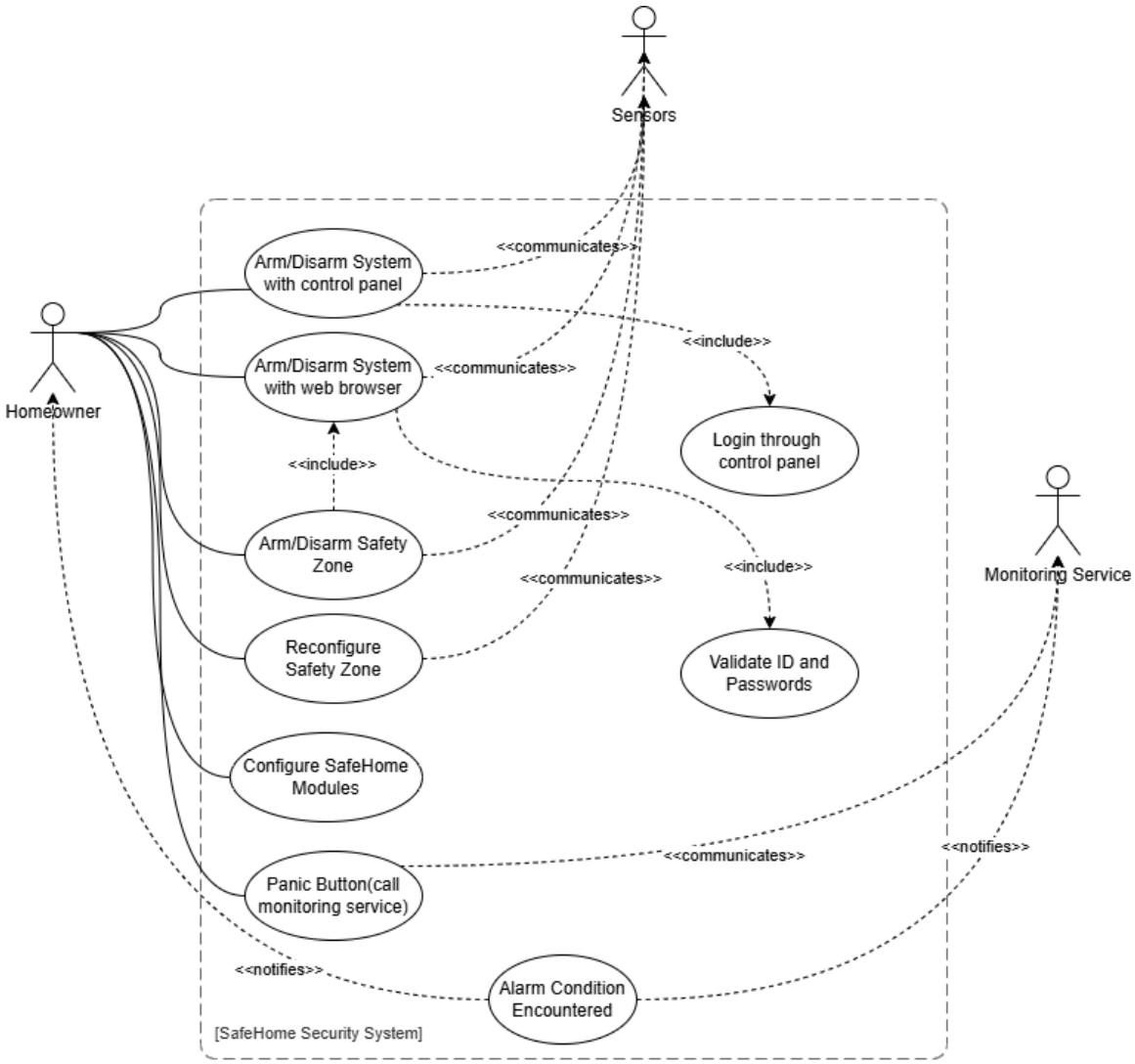
< Figure 7. Common Functions [CM]>

Here guests can log on through the Control panel but it doesn't mean that guests can configure or reset the system. Guests got a temporary password to enter the home.

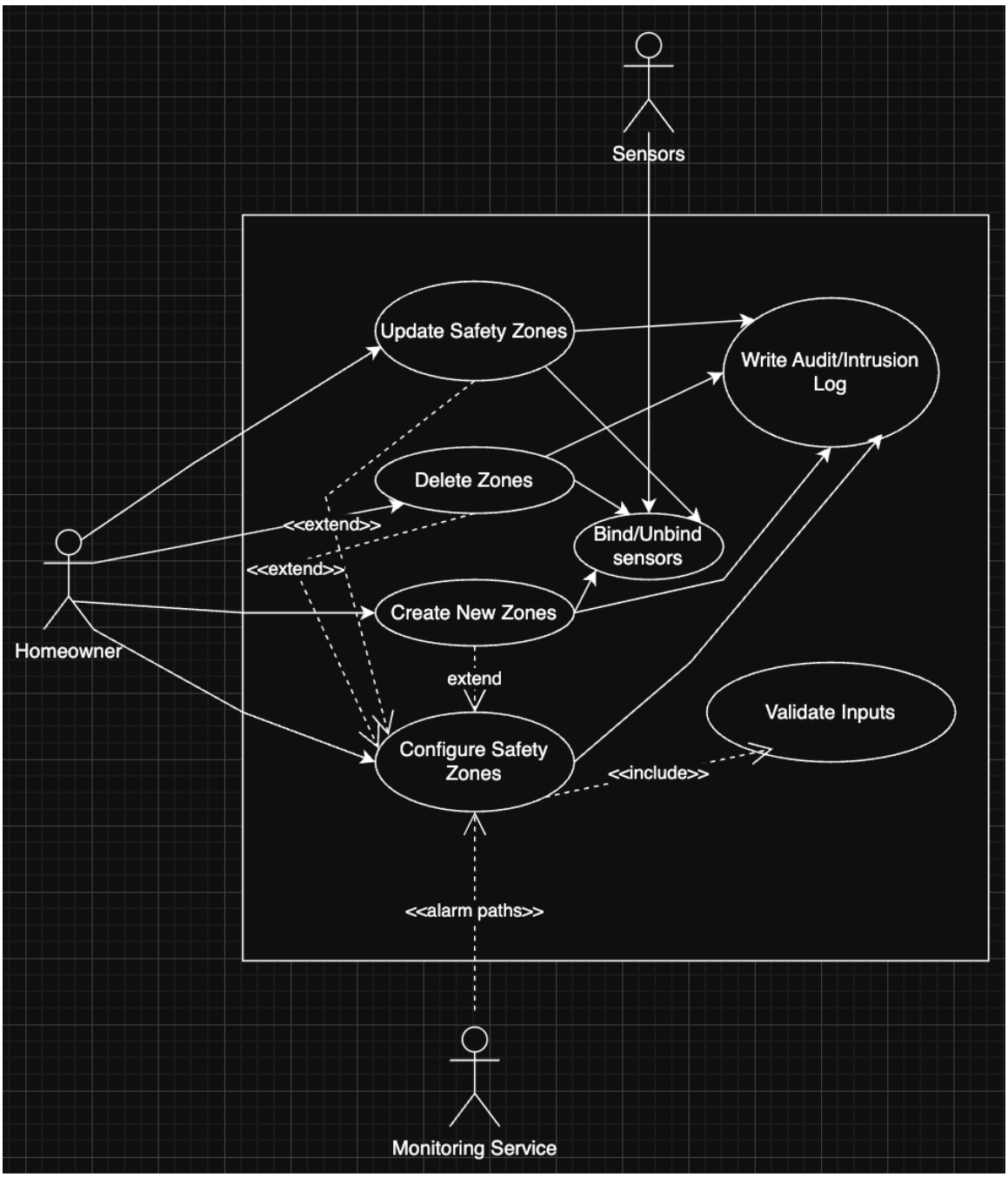
Reference:

- Panel, Web browser: Slide 20
- System related use cases: Slide 21
- Password change: Slide 20

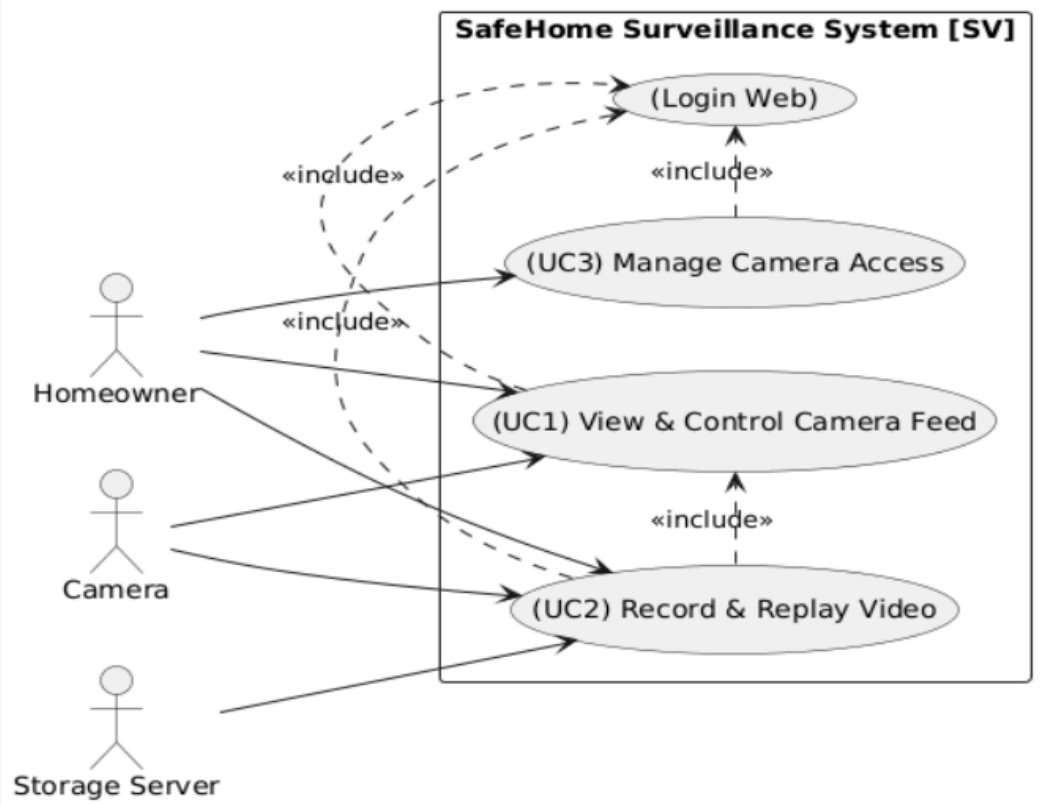
2. Security Functions



3. Configure Safety Zone Functions



4. Surveillance Functions



Surveillance functions

VI. Use Cases

1. Common Use Cases (Geunyeong)

a. Log onto the system through control panel

Use case:	Log onto the system through control panel
Primary actor:	Homeowner, Guest
Goal in context:	To log onto the Safehome system through control panel
Preconditions:	System has been configured. Appropriate password must be obtained.
Trigger:	The homeowner/guest decides to log onto the system.

Scenario:

1. The homeowner/guest uses the control panel.
2. The homeowner/guest enters master/guest password. (4 digits password)
3. The system validates password.
4. The system shows accessible functions on the control panel.

Exception:

3a. Password incorrect or not recognized.

.1: The system asks for password again.

.2: If the homeowner/guest enters incorrect or unrecognizable password three

times in a row the system locks itself for predefined time. Predefined time is 1, 2, 4, 8, 16 minutes and so on.

4a. An alarm condition is encountered – see use case: “alarm condition encountered”

Priority: High priority, basic functions.
When available: First increment.
Frequency of use: Frequent.
Channel to actor: control panel
Channel to secondary actors:

1. System administrator: PC-based system

Open issues:

1. What mechanisms protect unauthorized use of this capability by employees of the company?

b. Log onto the system through web browser

Use case: Log onto the system through web browser
Primary actor: Homeowner
Goal in context: To log onto the Safehome system through a web browser for remote monitoring and control.
Preconditions: System is fully configured and connected to the Internet. The Homeowner has a PC or device with a web browser and valid login credentials.
Trigger: The Homeowner decides to access the system remotely.

Scenario:

1. The Homeowner opens a web browser and navigates to the SafeHome Products Web site .
2. The system displays the Login Screen (Fig 2) .
3. The Homeowner enters his or her User ID.
4. The Homeowner enters two levels of passwords.
5. The system validates the credentials.
6. The system displays the main functions screen (Fig 3) .

Exception:

5a. User ID or passwords are incorrect or not recognized.
.1: The system asks for credentials again.
.2: If the Homeowner enters incorrect credentials three times in a row, the system locks the web account for a predefined time.

Priority: High priority, basic functions.
When available: First increment.
Frequency of use: Frequent.
Channel to actor: PC-based browser and Internet connection.
Secondary actors: System administrator
Channel to secondary actors:

1. PC-based system

Open issues:

1. What is the secure method for password recovery (e.g., "What if I forget my password?")

Reference in SafeHome dialog: Slide 17 (Internet accessibility requirement),

Slides 20-21 (Detailed web login scenario described by marketing).

c. Configure system setting

Use case: Configure system setting

Primary actor: Homeowner

Goal in context: To configure system parameters, such as security zones, modes, or sensor settings.

Preconditions: Homeowner is logged in through the web browser.

Trigger: The Homeowner decides to change or view system settings.

Scenario:

1. The Homeowner logs onto the system. «include» Log onto the system through web browser.
2. From the Main Functions screen (Fig 3), the Homeowner selects "CONFIGURE".
3. The system displays various configuration dashboards (e.g., Fig 4. Security Function - Safety zone, Fig 5. Security Function - Security Mode)..
4. The Homeowner selects a specific setting to modify (e.g., "Add Safety zone" , or selects a mode like "Overnight Travel").
5. The Homeowner follows the on-screen prompts to update the desired parameters.
6. The Homeowner saves the new configuration.
7. The system validates the new settings and provides a confirmation message.

Exception:

6a. The system detects an invalid setting (e.g., conflicting rules, invalid input).

.1: The system rejects the change and displays an error message explaining the conflict.

Priority: High priority.

When available: First increment.

Frequency of use: Occasional.

Channel to actor: PC-based browser and Internet connection.

Secondary actors: System administrator

Channel to secondary actors: PC-based system

Open issues:

1. Will all settings be available via the web, or are some only on the control panel?

Reference in SafeHome dialog: Slide 21 (Marketing requests ability to "reconfigure security zones"), Slides 73-74 (Detailed "administrator" use case for drawing floor plans and establishing settings).

d. Turn the system on

Use case: Turn the system on

Primary actor: Homeowner

Goal in context: To power on the main SafeHome system hardware.

Preconditions: The system is connected to a power source and is currently off.

Trigger: The Homeowner decides to activate the system.

Scenario:

1. The Homeowner presses the 'on' (1) button on the control panel.
2. The control panel display activates and shows "Starting system Please wait..." .
3. The 'power' indicator light turns green.
4. The system runs a self-diagnostic check.
5. Upon successful startup, the system enters a default state (e.g., "not ready") and is ready to accept commands.

Exception:

4a. The system fails the self-diagnostic check.

.1: The system displays an error code on the control panel and does not start.

Priority: High priority, basic functions.

When available: First increment.

Frequency of use: Infrequent.

Channel to actor: Control panel

Secondary actors: None

Channel to secondary actors: N/A

Open issues: None.

Reference in SafeHome dialog: Slide 2 (Prototype GUI, Fig 1) . The 'on' button is explicitly shown

e. Turn the system off

Use case: Turn the system off

Primary actor: Homeowner

Goal in context: To power off the main SafeHome system hardware.

Preconditions: The Homeowner is physically at the control panel.

Trigger: The Homeowner decides to completely deactivate the system (e.g., for maintenance, or when moving).

Scenario:

1. The Homeowner logs onto the system. «include» Log onto the system through control panel.
2. The Homeowner presses the 'off' (2) button on the control panel.
3. The system display prompts "Confirm system shutdown? Press 'off' again."
4. The Homeowner presses the 'off' (2) button again.
5. The system performs a safe shutdown procedure.
6. The control panel display and all indicator lights ('power', 'armed') turn off.

Exception:

1a. The system is currently in an alarm state.

.1: The system requires the alarm to be disarmed first before allowing shutdown.

4a. The Homeowner does not confirm within 10 seconds.

.1: The shutdown command is cancelled, and the system returns to its previous state.

Priority: High priority, basic functions.

When available: First increment.

Frequency of use: Infrequent.
Channel to actor: Control panel
Secondary actors: None
Channel to secondary actors: N/A
Open issues: None.
Reference in SafeHome dialog: Slide 2 (Prototype GUI, Fig 1) . The 'off' button is explicitly shown

f. Reset the system

Use case: Reset the system
Primary actor: Homeowner
Goal in context: To reboot the SafeHome system (e.g., if it becomes unresponsive).
Preconditions: The system is powered on.
Trigger: The Homeowner decides to restart the system.
Scenario:

1. The Homeowner logs onto the system. «include» Log onto the system through control panel.
2. The Homeowner presses the 'reset' (3) button on the control panel.
3. The system immediately performs a software reboot.
4. The system re-initializes (same as steps 2-5 in "Turn the system on" use case).

Exception:
(N/A - A reset is typically a forced action).
Priority: Medium priority.
When available: First increment.
Frequency of use: Infrequent.
Channel to actor: Control panel
Secondary actors: None
Channel to secondary actors: N/A
Open issues: None.
Reference in SafeHome dialog: Slide 2 (Prototype GUI, Fig 1) . The 'reset' button is explicitly shown

g. Change master password through control panel

Use case: Change master password through control panel
Primary actor: Homeowner
Goal in context: To change the 4-digit master password used for the control panel.
Preconditions: The Homeowner is physically at the control panel.
Trigger: The Homeowner decides to update their security password.
Scenario:

1. The Homeowner logs onto the system with the current password. «include» Log onto the system through control panel.
2. The Homeowner presses the 'code' (9) button.
3. The system display prompts: "Enter new 4-digit password".
4. The Homeowner enters the new 4-digit password.
5. The system display prompts: "Re-enter new password to confirm".

6. The Homeowner re-enters the new 4-digit password.
7. The system validates that the two new passwords match.
8. The system saves the new master password and confirms "Password Changed".

Exception:

7a. The new passwords do not match.

.1: The system displays "Error: Passwords do not match" and cancels the operation.

4a. The new password is not 4 digits.

.1: The system displays "Error: Invalid password format" and cancels.

Priority: Medium priority.

When available: First increment.

Frequency of use: Infrequent.

Channel to actor: Control panel

Secondary actors: System administrator

Channel to secondary actors: PC-based system

Open issues: None.

Reference in SafeHome dialog: Slide 2 (Prototype GUI, Fig 1) . The 'code' button and numeric keypad provide the interface for this function

2. Security Use Cases

a. Arm/disarm system through control panel

Use case:	Arm/disarm system through control panel
Primary Actor:	Homeowner
Goal in context:	To change house status to home or away
Precondition:	The system is running. Proper master password must be obtained
Trigger:	The homeowner decides to change the house safety status

Scenario:

1. The homeowner logs onto the system through control panel – see use case: “Log onto the system through control panel.”
2. The homeowner presses home/away button to change the safety status.
3. The system activates/deactivates sensors according to home/away condition.
4. The homeowner observes red light indicating armed or green light indicating disarmed on the control panel

Exception:

2a. The homeowner pressed away button and the doors or windows to be armed are not closed – control panel displays message “doors and windows not closed,” with a beep sound and does nothing.

1-4. An alarm condition is encountered – see use case: “alarm condition encountered.”

Priority:	Essential
Frequency of use:	frequent

Channel to actor: control panel
Secondary actor: System administrator, Sensors (door, window and motion detection)

Channels to secondary actors:

1. System administrator: PC-based system
2. Sensors: wireless connectivity

Open issues:

1. What mechanisms protect unauthorized use of this capability by employees of the company?

Reference in SEPA dialog slide: Slide 17, Slide 21

b. Arm/disarm system through web browser

Use case: Arm/disarm system through web browser

Primary Actor: Homeowner

Goal in context: To arm or disarm the entire security system remotely via the internet.

Precondition: The system is running. The homeowner has a valid User ID and two levels of passwords.

Trigger: The homeowner needs to arm or disarm the system while away from home.

Scenario:

1. The homeowner logs onto the SafeHome Products Web site.
2. The homeowner enters his or her user ID and two levels of passwords.
3. The system validates the credentials and may ask for secondary verification (e.g., address, phone number).
4. The system displays a screen representing all SafeHome functions.
5. The homeowner selects the "home security function".
6. The system displays a virtual representation of the security system control panel.
7. The homeowner selects the "arm the system" or "disarm the system" function.
8. The system executes the command, activating or deactivating the relevant sensors.
9. The system provides visual feedback on the web interface confirming the new status.

Exception:

- 2a. ID or passwords are incorrect – see use-case: "validate ID and passwords."
- 7a. The user selects "arm the system" and a sensor reports a door/window is open.
  .1: The system displays an error message on the web interface and does not arm.

Priority: High

Frequency of use: Frequent

Channel to actor: PC-based browser and Internet connection

Secondary actor: Sensors

Channels to secondary actors: Wireless connectivity

Open issues:

1. How to handle a forgotten password securely.
2. Ensuring the web connection is fully secure and encrypted to prevent hacking.

Reference: Slides 20-21

c. Arm/disarm safety zone selectively

Use case: Arm/disarm safety zone selectively

Primary Actor: Homeowner

Goal in context: To disarm one or more specific sensors or security zones while leaving the rest of the system armed.

Precondition: The homeowner is logged in via the web browser. The system is armed.

Trigger: The homeowner needs to grant temporary access to a specific area (e.g., for a repair person) without disarming the entire house.

Scenario:

1. The homeowner logs onto the system via the web browser (see use case: "Arm/disarm system through web browser").
2. The homeowner navigates to the home security function's control panel view.
3. The homeowner selects the function to "disarm one or more sensors".

4. The system displays the configured security zones or a list of sensors.
5. The homeowner selects the desired zone(s) or sensor(s) to disarm.
6. The system deactivates the selected sensors while keeping others active.
7. The system provides visual confirmation of the change.

Exception:

- 5a. The selected sensor is part of a critical, non-bypassable zone.
  .1: The system displays a warning and does not allow the action.

Priority: Medium

Frequency of use: Occasional

Channel to actor: PC-based browser and Internet connection

Secondary actor: Sensors

Channels to secondary actors: Wireless connectivity

Open issues:

1. How to automatically re-arm the disarmed zone after a certain period.

Reference: Slide 21

d. Alarm condition encountered

Use case: Alarm condition encountered

Primary Actor: Sensors

Goal in context: To alert the homeowner and/or monitoring service when a sensor is triggered while the system is armed.

Precondition: The system or a specific safety zone is armed. A sensor is active.

Trigger: A sensor (e.g., window, door, motion, doggie angst) detects an event that violates its set parameters.

Scenario:

1. A sensor detects an intrusion or specific event (e.g., dog barking for >1 minute).
2. The sensor sends a signal to the main system controller.
3. The system controller verifies the system is in an armed state where this sensor should trigger an alarm.

4. The system initiates the alarm sequence:
   a. Activates an audible alarm (if configured).
   b. Displays an alarm message on the control panel and web interface, identifying the sensor/zone.
   c. Initiates an automated call to the homeowner's phone or a monitoring service.
5. The system logs the event in the intrusion log.

Exception:

- 4c. The outgoing call fails to connect.
  .1: The system attempts to call a secondary number if configured.
  .2: The system logs the call failure.

Priority: High (Critical)

Frequency of use: Infrequent (only during alarm events)

Channel to actor: N/A (System-initiated)

Secondary actor: Homeowner, Monitoring Service

Channels to secondary actors: Phone call, Control Panel display, Web interface

Open issues:

1. Defining the protocol for communicating event details to the monitoring service.
2. How to handle false alarms and allow the homeowner to cancel the alarm sequence.

Reference: Slides 58-59 and 63-64

E. Reconfigure Safety Zone

Primary Actor: Homeowner

Goal in context: To manage security zones by creating, modifying, or deleting them.

Precondition: Homeowner is logged in with administrative privileges.

Trigger: Homeowner decides to change how sensors are grouped and behave.

Scenario:

1. The homeowner logs into the system (web or control panel).

2. The homeowner navigates to the security configuration section.

3. The homeowner selects "Manage Security Zones".

4. The system displays a list of existing zones.

5. The homeowner chooses an action:

Option A: Create a new zone

1. The homeowner selects "Create New Zone".

2. The system prompts for a zone name.

3. The system displays available sensors.

4. The homeowner selects sensors and saves.

Option B: Update an existing zone

1. The homeowner selects a zone and chooses "Edit".

2. The system displays current name and sensors.

3. The homeowner modifies name/sensors and saves.

Option C: Delete a zone

1. The homeowner selects a zone and chooses "Delete".

2. The system asks for confirmation.

3. The homeowner confirms deletion.

4. The system removes the zone.

6. The system confirms the changes.

Exception:

1. Zone name already exists → error message.

2. Zone is currently armed → cannot delete, error message.

Priority: Medium

Frequency of use: Infrequent

Channel to actor: Web browser or Control Panel

Secondary actor: Sensors

Reference: Slide 21

i. Configure Safehome modes

Use case: Configure Safehome modes

Primary Actor: Homeowner

Goal in context: To define the system's behavior for different situations (e.g., Home, Away, Travel).

Precondition: Homeowner is logged in with administrative privileges.

Trigger: Homeowner wants to customize how the security system behaves in predefined modes.

Scenario:

1. The homeowner navigates to the system configuration menu.
2. The homeowner selects "Configure Modes".
3. The system displays a list of modes: "Home", "Away", "Overnight Travel", "Extended Travel".
4. The homeowner selects a mode to configure (e.g., "Overnight Travel").
5. The system allows the homeowner to define which security zones are active in this mode.
6. For travel modes, the system allows configuring settings for making the house look occupied (e.g., random light activation - though this overlaps with home management, the security aspect is relevant).
7. The homeowner saves the configuration for the mode.

Exception:

- 5a. The user attempts to create a configuration with conflicting rules.
  .1: The system flags the conflict and requests correction.

Priority: Medium

Frequency of use: Infrequent (typically during initial setup)

Channel to actor: Web browser or Control Panel

Channels to secondary actors: Internal data bus

Open issues:

1. How to allow homeowners to create their own custom modes.

Reference: Slide 39

k. Call monitoring service through control panel

Use case: Call monitoring service through control panel (Panic Button)

Primary Actor: Homeowner

Goal in context: To manually trigger an emergency call to the monitoring service.

Precondition: The system is powered on.

Trigger: The homeowner perceives an emergency and presses the panic button on the control panel.

Scenario:

1. The homeowner presses and holds the dedicated "Panic" button on the control panel.
2. The system immediately initiates an automated call to the pre-configured monitoring service.
3. The system may also activate an audible alarm, depending on configuration.
4. The system logs the manual panic event.

Exception:

- 1a. The panic button is pressed accidentally and released quickly.
  .1: The system may have a short delay (e.g., 3 seconds hold) to prevent accidental triggers. The call is not made.

Priority: High (Critical)

Frequency of use: Very Infrequent (Emergency only)

Channel to actor: Control Panel

Secondary actor: Monitoring Service

Channels to secondary actors: Phone line / VoIP

Open issues: None identified from dialogue.

Reference: Slides 63-64, and is also present within the GUI provided in the template.

3. Surveillance Use Cases

a. View and Control Camera Feed (UC1)

Use Case: View and Control Camera Feed
Primary Actor: Homeowner

Goal in Context: To allow the homeowner to view live video from any camera and control it (pan, zoom, enable/disable, or view all cameras at once).

Preconditions:
System should be configured, the Internet connection must be available, and the homeowner must have valid login credentials and, if applicable, a camera password.

Trigger: The homeowner decides to monitor one or more areas of the house.

Scenario:

1. The homeowner logs onto the system – see use case: "Log onto the system through web browser."
2. The system authenticates the user and displays main function buttons.
3. The homeowner selects "Surveillance."
4. The system displays the floor plan of the house with all camera icons.
5. The homeowner selects a camera icon or "View All Cameras."
6. If the selected camera is password-protected, the system requests a password.
7. The homeowner enters the password.
8. The system validates the password.
9. The system displays the selected camera's state (active, disabled, etc.).
10. The homeowner selects "View."
11. The system displays the live video feed in a viewing window at approximately one frame per second.
12. The homeowner may choose to **Pan** or **Zoom** the camera; the system updates the live view accordingly.
13. If "View All Cameras" is chosen, the system displays thumbnail feeds of all available cameras; the homeowner can click one to enlarge.

Exceptions:

2a. Surveillance function not configured → system displays an error message; see use case: "Configure Surveillance Function."
5a. Floor plan not configured → display error message and refer to "Configure Floor Plan."
6a. If the camera does not have a password, skip step 7.
8a. Incorrect password → prompt for reentry (up to 3 tries), then lock temporarily.
9a. If the camera is disabled → show message "Camera Disabled" and suggest "Enable Camera."
13a. Connection loss or bandwidth too low → display "Connection Unstable" warning.

When Available: First increment
Frequency of Use: Many times per day
Channel to Actor: PC-based system with web browser

Secondary Actors: Camera
Channels to Secondary Actors:

- Camera: wireless connectivity

Open Issues:

- Will system performance remain acceptable with multiple simultaneous video streams?
- Should the frame rate automatically adjust to available bandwidth?
- What happens if a camera is offline or broken?
- Will camera pan/zoom controls be standardized across all models?

Reference in SEPA Dialogue Slides: Slides 29-34 (Meredith describes camera selection, password protection, pan/zoom, and thumbnail viewing.)

---

b. Record and Replay Video (UC2)

Use Case: Record and Replay Video
Primary Actor: Homeowner

Goal in Context: To record video from a selected camera and replay it later for review.

Preconditions:
The system and selected camera must be active and connected. The homeowner must be logged in.

Trigger: The homeowner decides to record footage or replay previously recorded footage.

Scenario:

1. The homeowner logs into the system.
2. The homeowner selects “Surveillance” and chooses a camera.
3. The homeowner clicks “Start Recording.”
4. The system stores the live video stream in the local or cloud storage.
5. The homeowner clicks “Stop Recording” to end recording.
6. To view a recorded clip, the homeowner selects “Replay.”
7. The system retrieves the recorded file and plays it in the viewing window.
8. The homeowner may pause, fast-forward, or stop playback at any time.

Exceptions:
3a. Recording fails due to insufficient storage space → system displays an error message.
4a. Network connection lost → system pauses recording and logs an alert.
7a. Requested file not found or corrupted → system displays “Replay Unavailable.”

When Available: Second increment
Frequency of Use: Occasionally (on-demand for security events)
Channel to Actor: PC-based system with web browser

Secondary Actors: Storage Server, Camera
Channels to Secondary Actors:

- Storage Server: internal data transfer
- Camera: wireless connectivity

Open Issues:

- How long will recorded data be retained?
- Should the homeowner be able to download video files?
- Will recording affect the performance of live viewing?

Reference in SEPA Dialogue Slides: Slide 31 (“To allow the homeowner to check the house while away, to record and play back video that is captured.”)

---

c. Manage Camera Access (UC3)

Use Case: Manage Camera Access
Primary Actor: Homeowner

Goal in Context: To secure cameras by setting or removing individual passwords that control who can view specific feeds.

Preconditions:
System must be configured, and the homeowner must be logged in.

Trigger: The homeowner decides to protect or unprotect specific camera views.

Scenario:

1. The homeowner logs into the system.
2. The homeowner selects “Surveillance” → “Manage Access.”
3. The system displays all installed cameras.
4. The homeowner selects a camera.
5. The homeowner chooses one of the following options:
    a. “Set Password” → enters and confirms new password.
    b. “Delete Password” → removes existing password.
6. The system validates and saves the new setting.
7. The system confirms completion and updates the camera’s status.

Exceptions:
5a. Passwords do not match → prompt for re-entry.
6a. Invalid password format (too short/weak) → show warning and reject.
7a. System unable to update camera → display “Operation Failed.”

When Available: Second increment
Frequency of Use: Occasional (on setup or change of access)
Channel to Actor: PC-based system with web browser

Open Issues:

- Should there be a recovery mechanism for forgotten camera passwords?
- Should password rules (length/complexity) be enforced?
- Can different users have unique passwords for the same camera?

Reference in SEPA Dialogue Slides: Slide 31 ("I also want to be able to block access to one or more cameras with a specific password.")

4. Configure Safety Zone Use Cases

a. Configure Safety Zones (UC-SZ1)

Use Case: Configure Safety Zone
Primary Actor: Homeowner

Goal in Context: To modify the configuration and operational parameters of an existing safety zone.

Preconditions: The system must be operational, and the user must be authenticated with master-level credentials.

Trigger: The homeowner selects Configure → Safety Zone → Edit from the control panel or web interface.

Scenario:

1. The homeowner logs onto the system (see UC: Log onto the system through control panel or web browser).
2. The homeowner selects Configure → Safety Zone.
3. The system displays the list of available zones with their current status (Activated/Deactivated).
4. The homeowner selects a specific zone to configure.
5. The system displays all editable zone parameters, including:
    - Zone name and description
    - Bound sensors (door/window/motion)
    - Entry/Exit delay times
    - Alarm type (audible/silent) and duration
    - Active modes (Home/Away/Overnight/Travel)
    - Schedule for auto-arming/disarming
    - Bypass permissions and sensitivity levels

6. The homeowner updates one or more parameters.

7. The system validates inputs and confirms the update.

8. The system saves the changes, updates the configuration database, and logs the event.

Exceptions:
5a. No zones available → system prompts to Create New Zone (see UC–SZ2).

6a. Invalid inputs (e.g., duplicate name, missing sensor) → system displays an error.

8a. System fails to save changes due to a technical issue → user notified and prompted to retry.

When Available: First increment
Frequency of Use: Occasionally
Channel to Actor: Control panel and web interface

Secondary Actors: Sensors, System Administrator (system itself)
Channels to Secondary Actors:

- Wireless connection to sensors

Open Issues:

- Should the system apply updated rules immediately or after disarming?

- How should overlapping schedules be handled?

Reference in SEPA Dialogue Slides: Slide 25 (“It'll also be polling the PC to determine if there is any input from it, for example Internet based access or configuration information.”)

b. Create New Safety Zone (UC-SZ2)

Use Case: Create New Safety Zone
Primary Actor: Homeowner

Goal in Context: To add a new safety zone with selected sensors and parameters.

Preconditions: The homeowner is authenticated; sensors are available and unassigned.

Trigger: The homeowner selects *Add Safety Zone* from the configuration menu.

Scenario:

1. The homeowner logs into the system.
2. The homeowner selects the *Add Safety Zone*.
3. The system opens the *New Zone* setup window.
4. The homeowner enters zone name and description.
5. The homeowner selects sensors (door, window, motion) to include.
6. The homeowner sets parameters such as alarm type, delay, and active modes.
7. The homeowner clicks *Create Zone*.
8. The system validates data, saves the configuration, and displays confirmation.
9. The system logs the creation in the system event log.

Exceptions:
4a. Zone name already exists → system prompts for a new name.

5a. No sensors available → system notifies user and allows setup continuation.

8a. Save failure → user prompted to retry or cancel.

When Available: First increment
Frequency of Use: Occasionally
Channel to Actor: Web browser or control panel

Secondary Actors: Sensors
Channels to Secondary Actors:

- Wireless connection to sensors

Open Issues:

- Should the system automatically arm a newly created zone if the house is already armed?
- How will duplicate sensor assignments be handled if a sensor is already linked to another zone?
- Will the system allow creating an empty zone (without sensors) as a placeholder?
- Should there be default configuration templates (e.g., “Bedroom zone,” “Garage zone”) for quicker setup?

- How should the system handle invalid or missing hardware connections during setup?

Reference in SEPA Dialogue Slides: Slide 30 (“the first configures the system including laying out a floor plan--we need tools to help the homeowner do this”)

c. Delete Safety Zone (UC-SZ3)

Use Case: Delete Safety Zone
Primary Actor: Homeowner

Goal in Context: To delete an existing safety zone safely.

Preconditions: Zone exists and is disarmed.

Trigger: The homeowner selects *Add Safety Zone* from the configuration menu.

Scenario:

1. The homeowner logs into the system.
2. The homeowner selects *Configure* → *Safety Zone*.
3. The homeowner chooses a zone and clicks *Delete*.
4. The system displays a confirmation dialog warning about unbinding sensors.
5. The homeowner confirms deletion.
6. The system checks the zone status (armed/disarmed).
7. The system deletes the zone configuration and unbinds related sensors.
8. The system logs the deletion.

Exceptions:
6a. Zone armed → system prompts the user to disarm first.

7a. Delete operation fails → system displays error and retains current state.

When Available: First increment
Frequency of Use: Infrequently
Channel to Actor: Web browser or control panel

Open Issues:

- Should the system permanently remove deleted zones, or archive them for recovery/audit purposes?

- How will logs linked to deleted zones (e.g., intrusion history) be retained or reassigned?
- Should the system automatically unassign all sensors upon deletion, or require user confirmation for each?
- Will deleting a zone trigger any automatic notifications to the monitoring service or administrator?
- Should deletion be restricted when the system is armed or in certain security modes (e.g., "Away" mode)?

Reference in SEPA Dialogue Slides: Slide 37 ("we ought to role play through them, just make sure nothing has been omitted.")

d. Update Existing Safety Zone (UC-SZ4)

Use Case: Update Existing Safety Zone
Primary Actor: Homeowner

Goal in Context: To modify the configuration of an existing zone.

Preconditions: The zone exists and user is authenticated.

Trigger: The homeowner selects *Update Safety Zone*.

Scenario:

1. The homeowner logs into the system.
2. The homeowner selects *Configure → Safety Zone*.
3. The homeowner selects the *Update Safety Zone*.
4. The system loads the zone details.
5. The homeowner modifies parameters (sensors, delays, modes, alarms, etc.).
6. The homeowner clicks *Save Changes*.
7. The system validates the updates.
8. The system applies the changes and confirms completion.
9. The system updates the status display and logs the event.

Exceptions:

4a. Removing all sensors → system prevents save and prompts warning.

6a. Invalid data or connection issue → display error and retry option.

When Available: First increment
Frequency of Use: Occasionally
Channel to Actor: Web browser or control panel

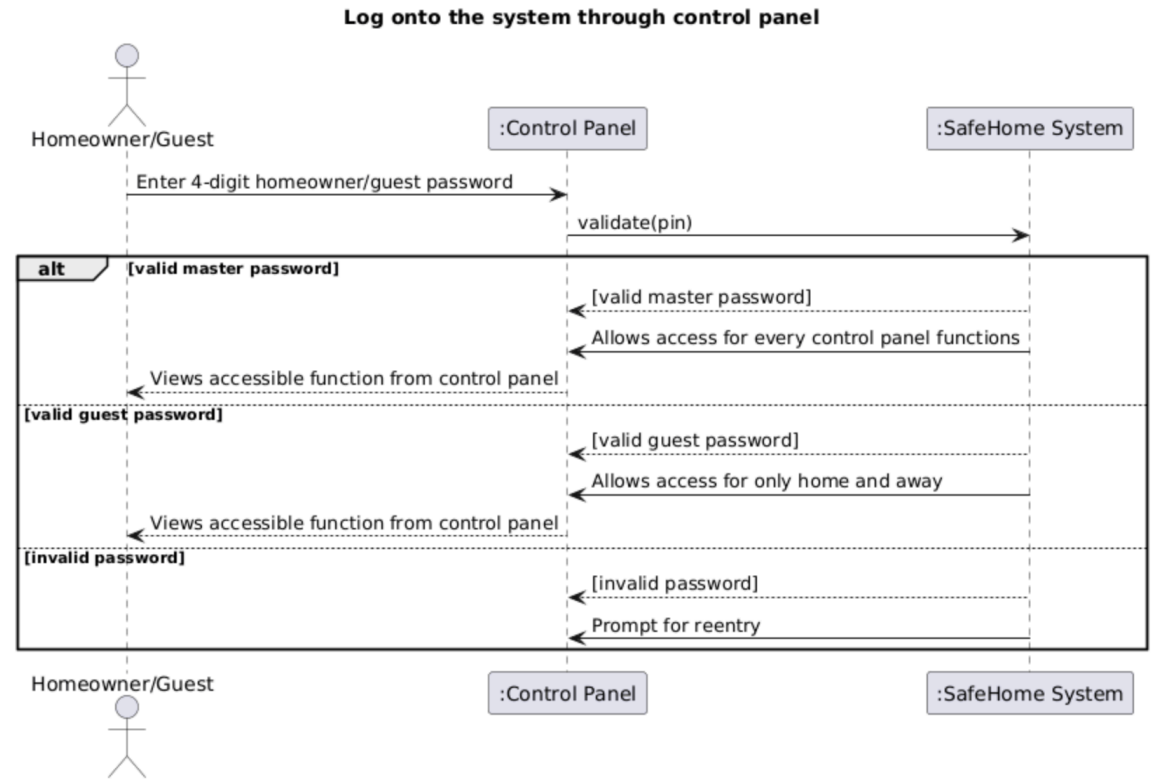
Open Issues:

- Should updated configurations take effect immediately, or only after the system is disarmed?
- How will the system handle concurrent updates (e.g., two users editing zones at the same time)?
- Should sensor reassignments automatically propagate to other zones if overlap occurs?
- Will changes in alarm type or duration require reconfirmation by the user for safety compliance?
- Should the system notify users or log a timestamped record when a zone's rules are modified?

VII. Sequence Diagram

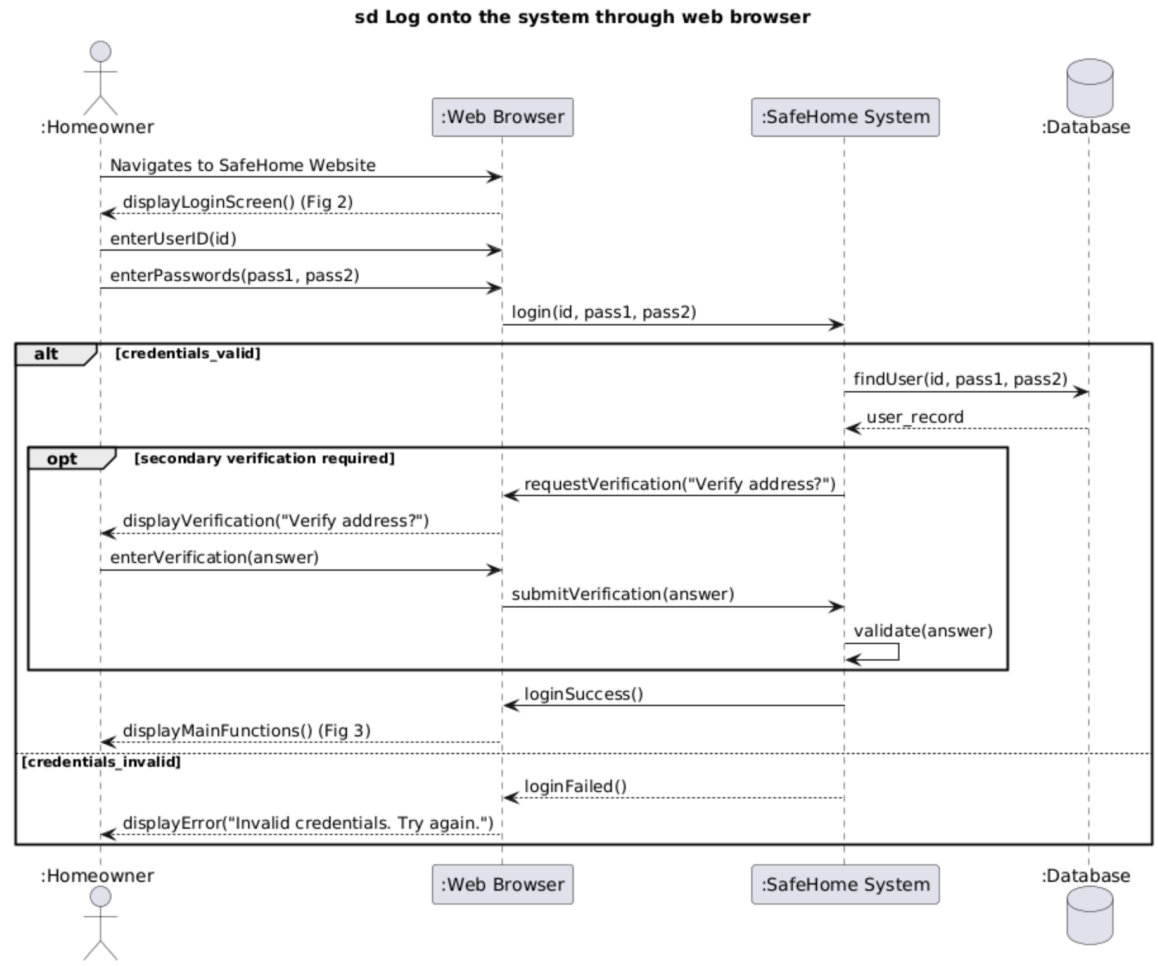
1. Common Sequence Diagram

a. Log onto the system through control panel



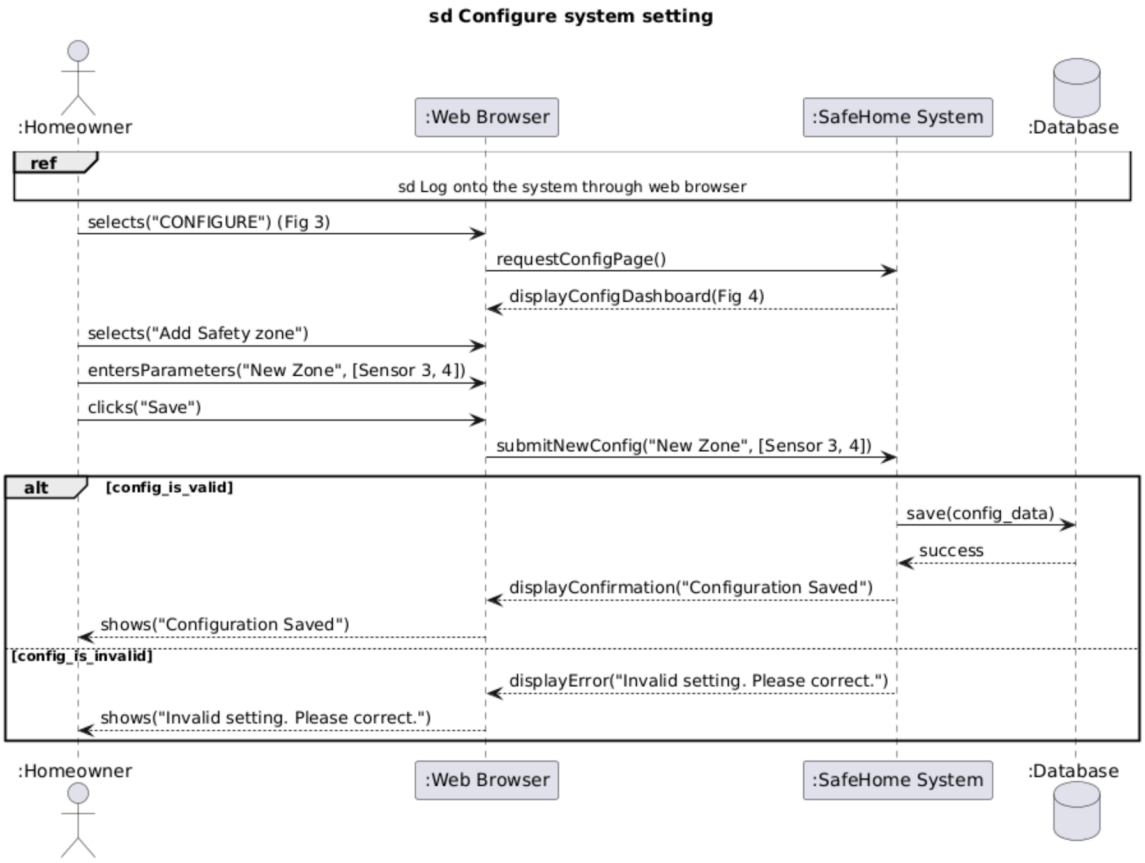
Reference: slide 20, slide 21

b. Log onto the system through web browser



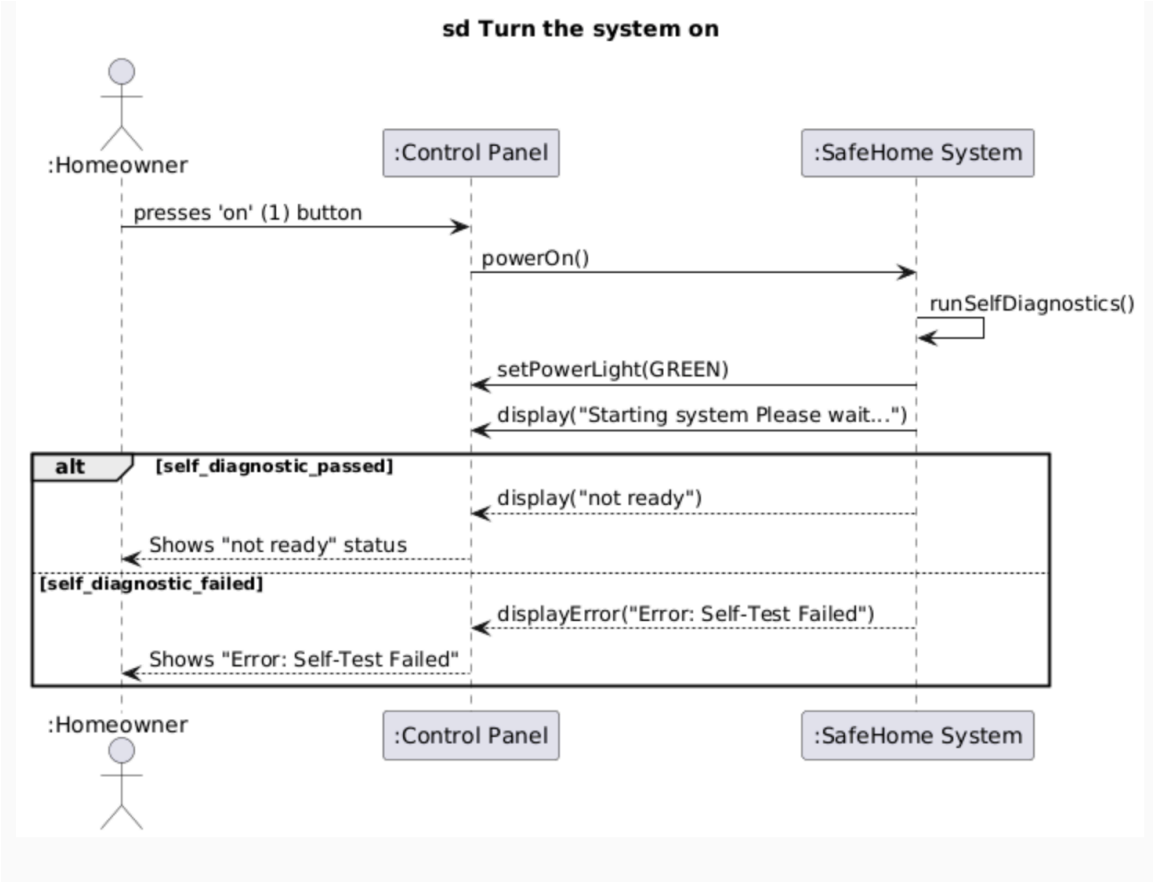
Reference: slide 17, 20, 21

c. Configure system setting



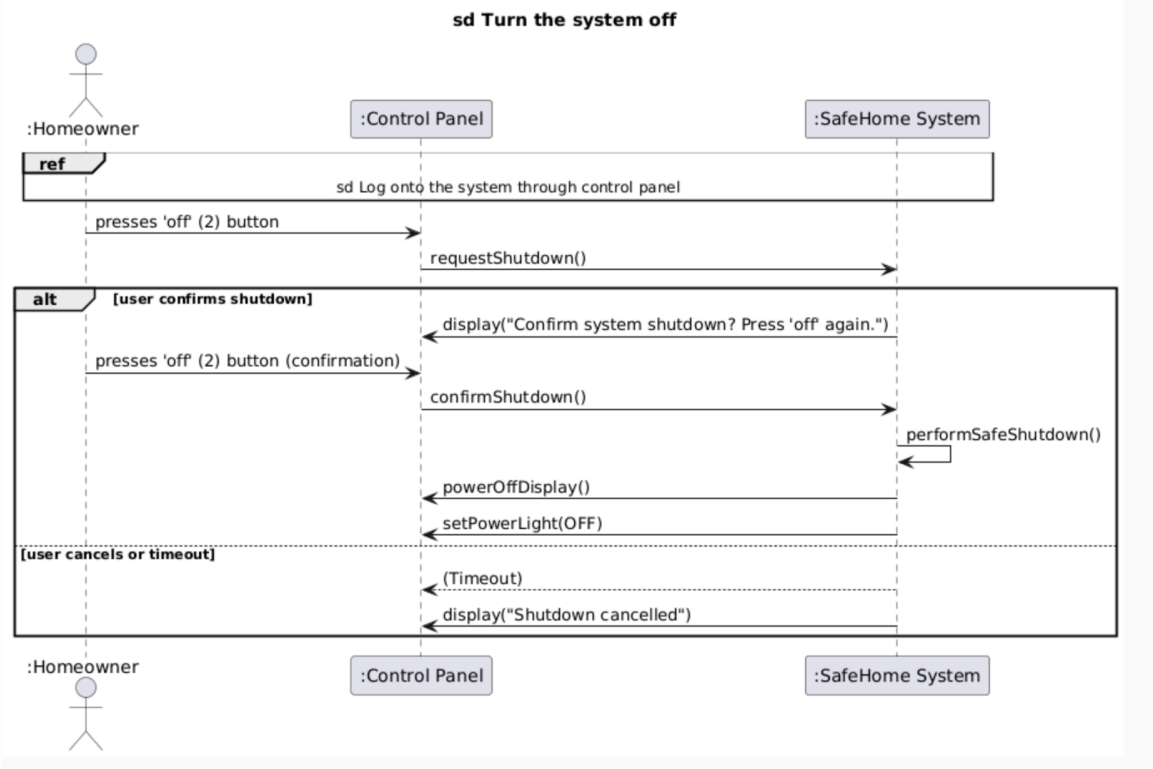
Reference: slide 21, slide 73, 74

d. Turn the system on



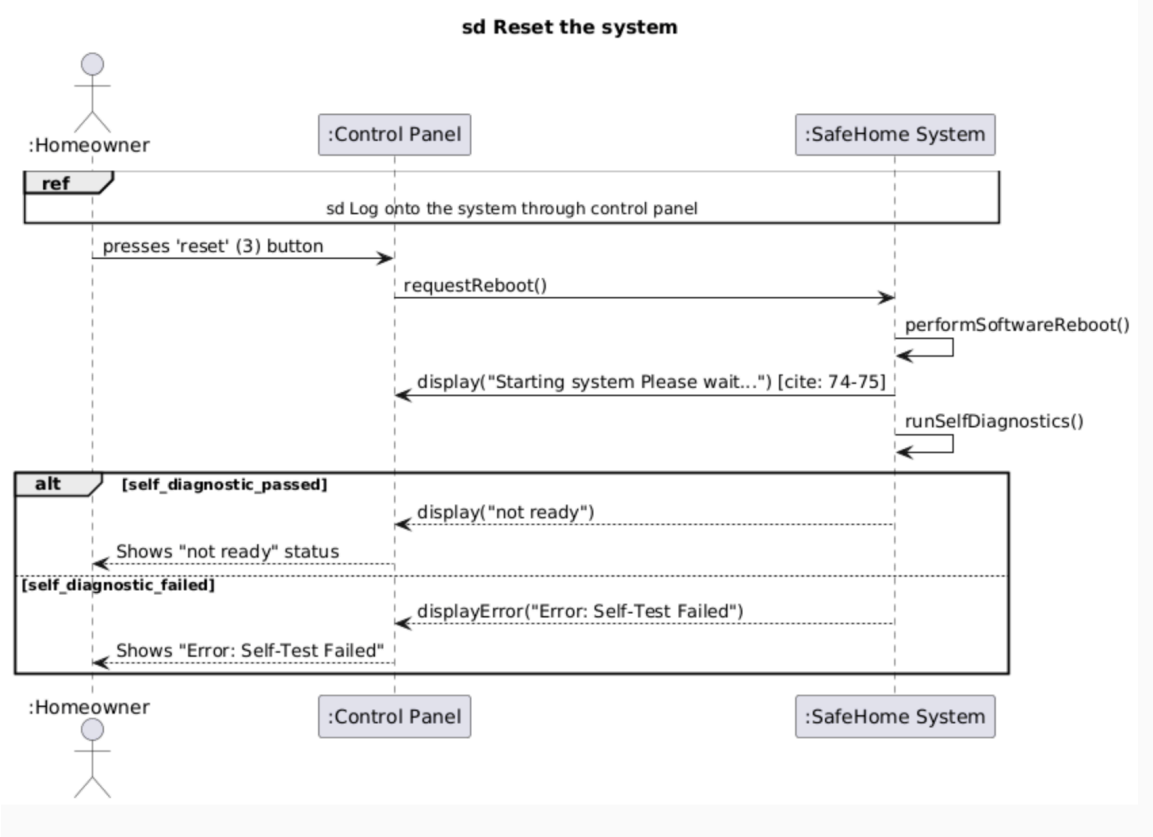
Reference: Fig 1 Prototype GUI

e. Turn the system off



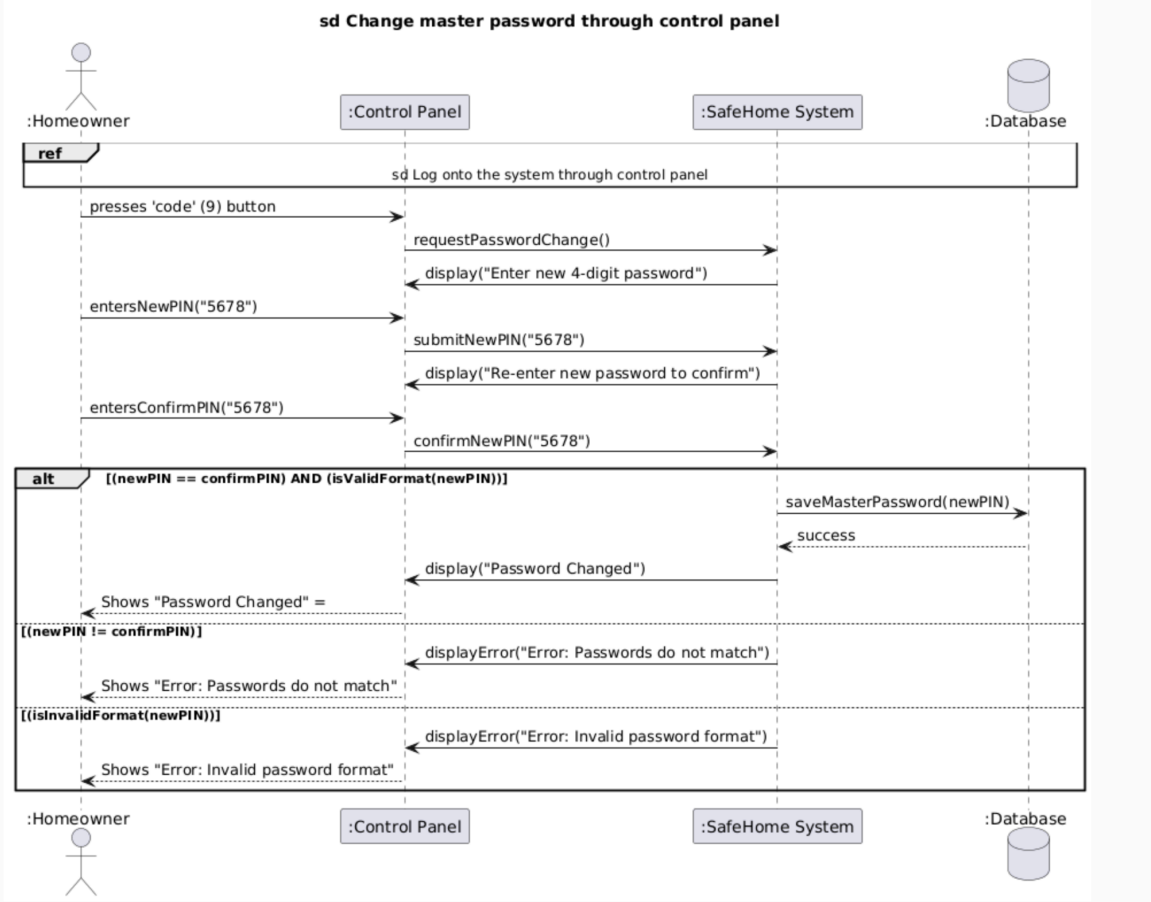
Reference: Fig 1 Prototype GUI

f. Reset the system



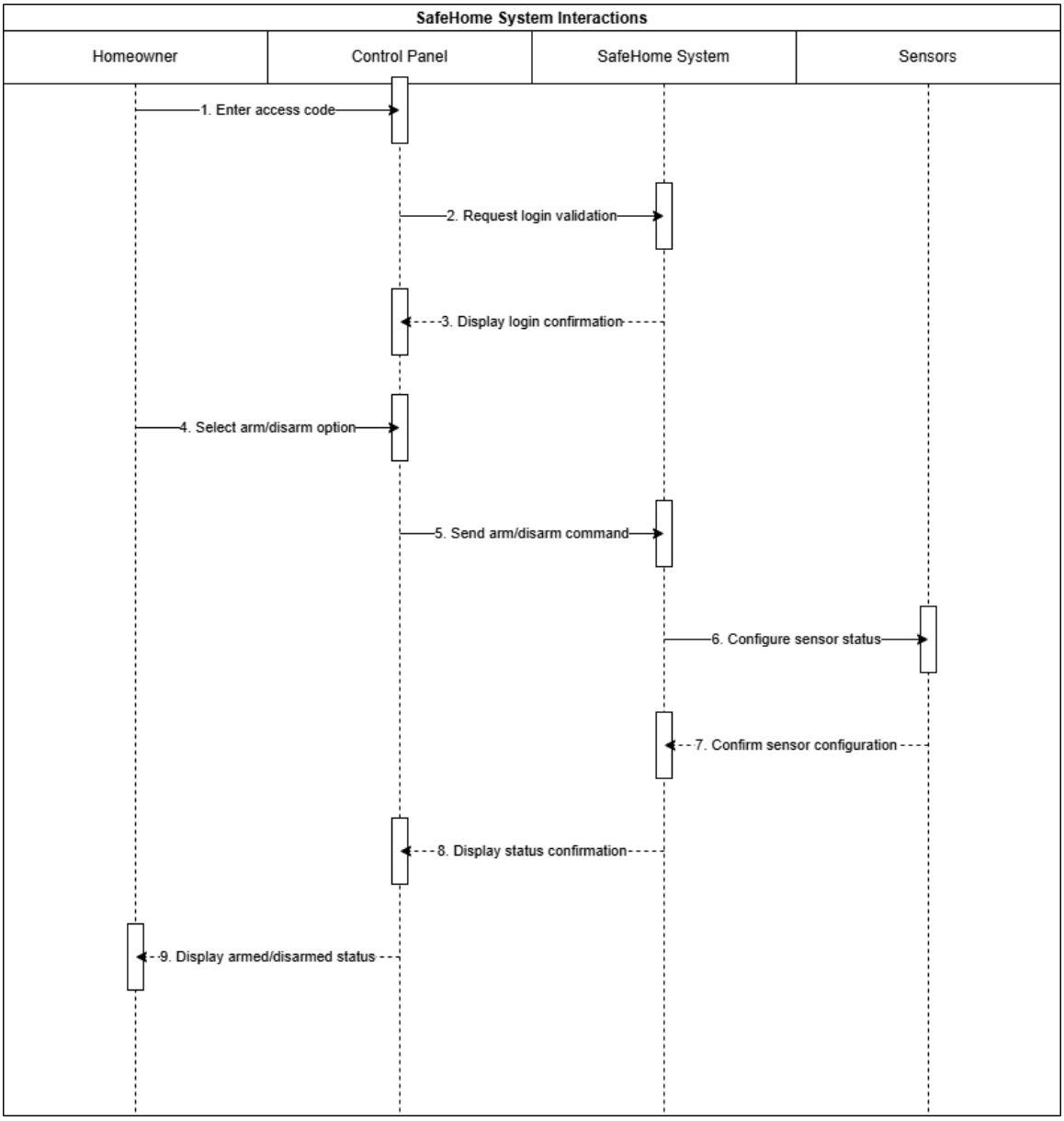
Reference: Fig 1 Prototype GUI

g. Change master password through control panel

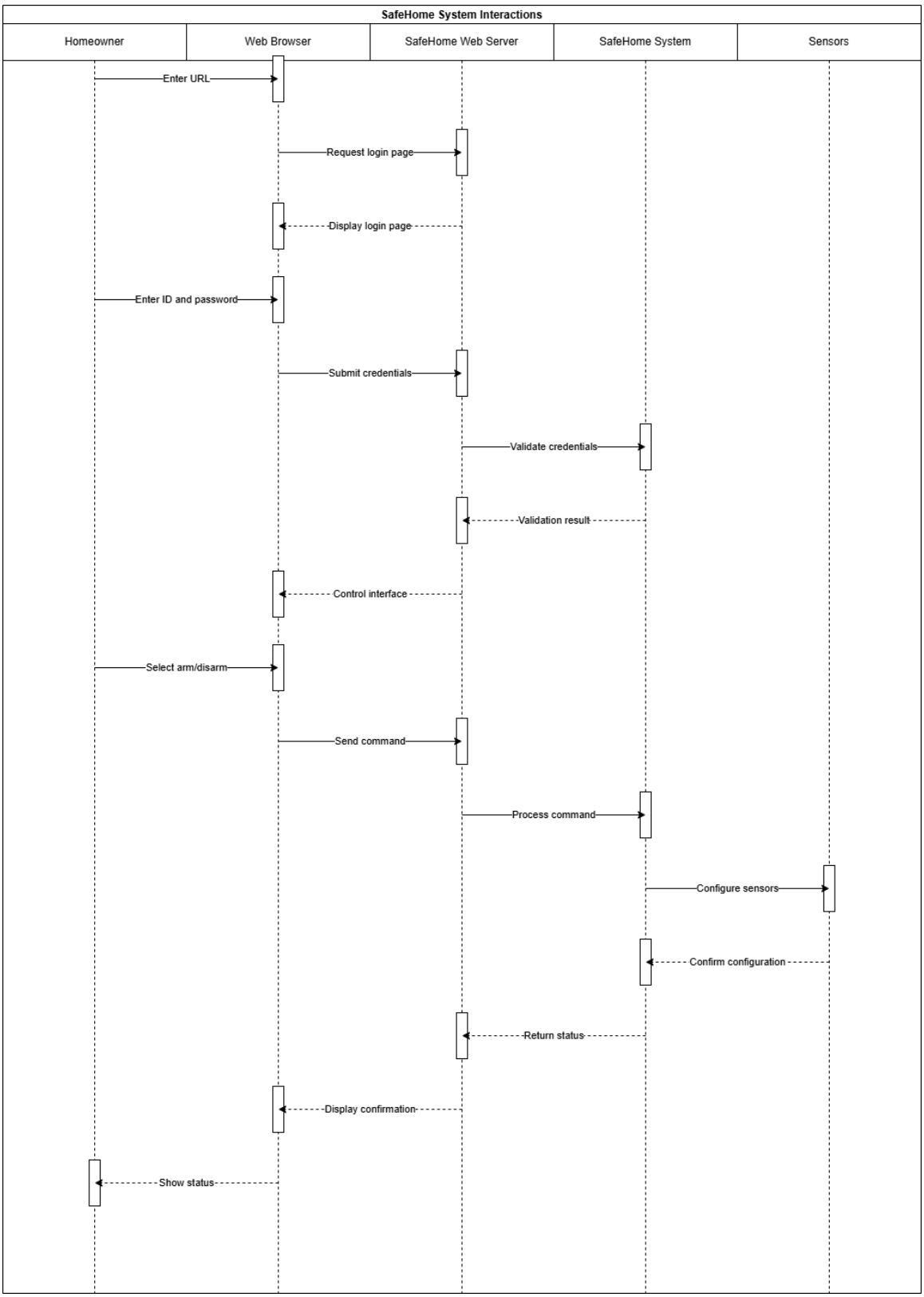


2. Safety Functions Sequence Diagram

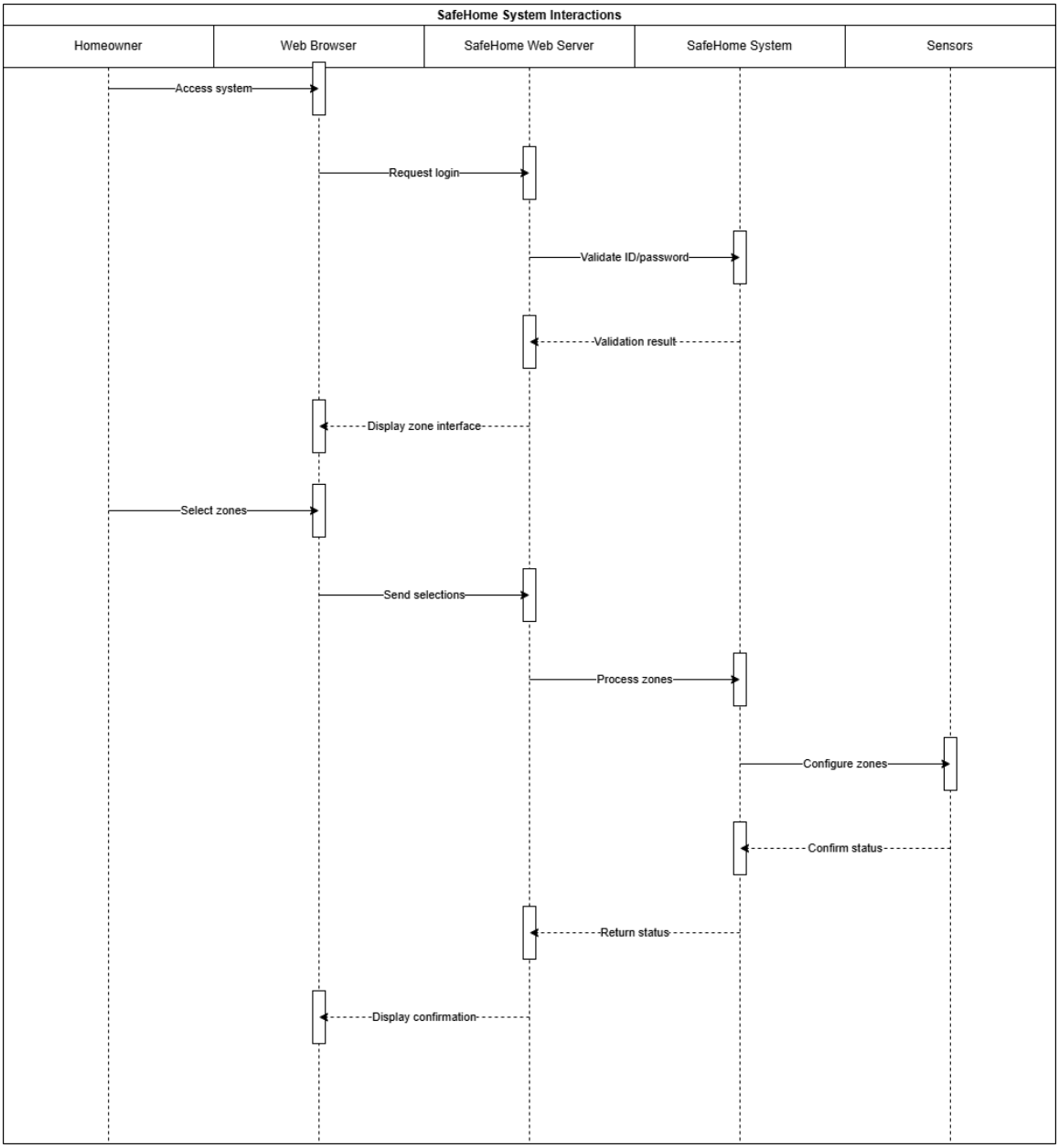
a. Control Panel Arm/Disarm



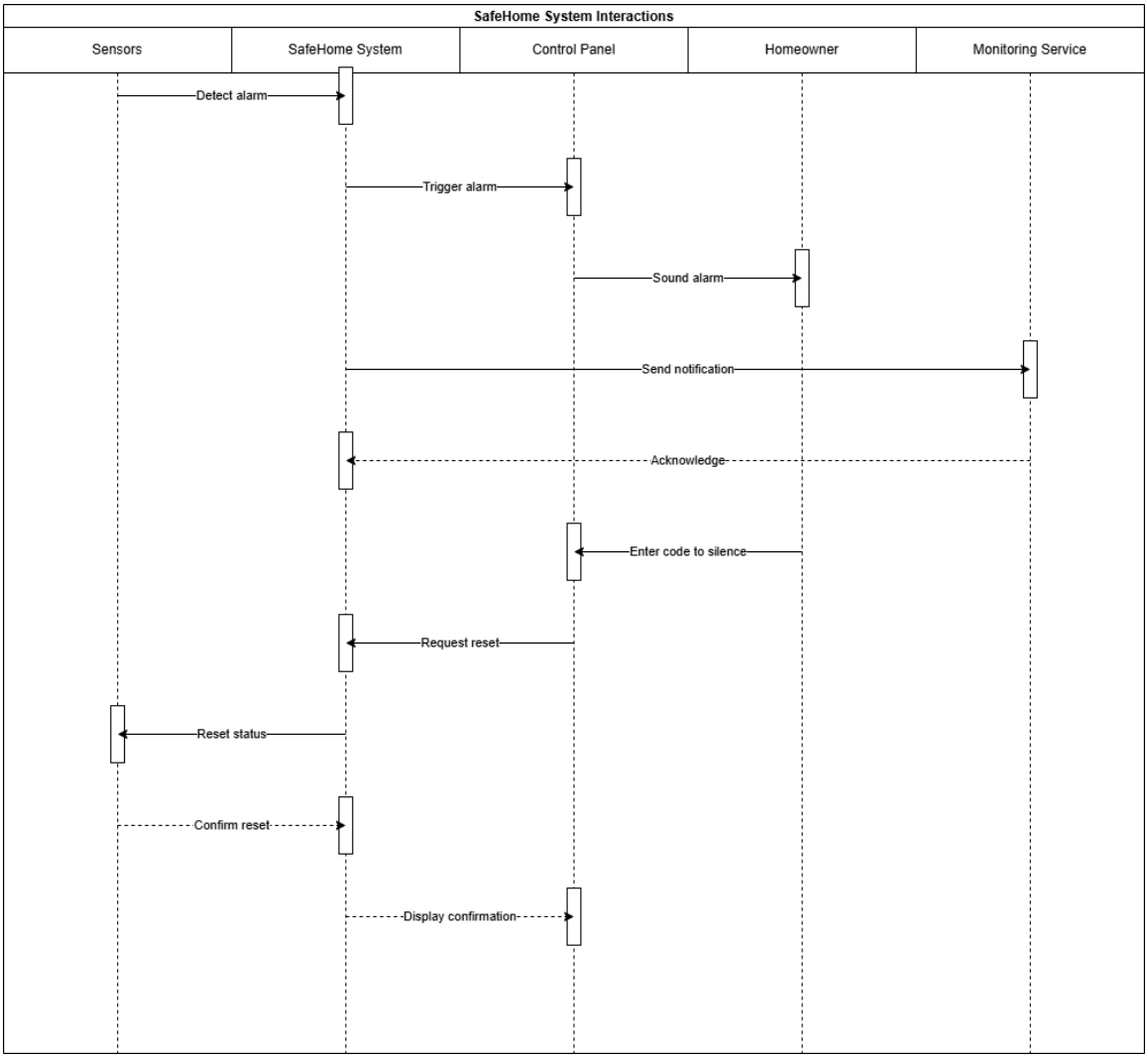
b. Web Browser Arm/Disarm



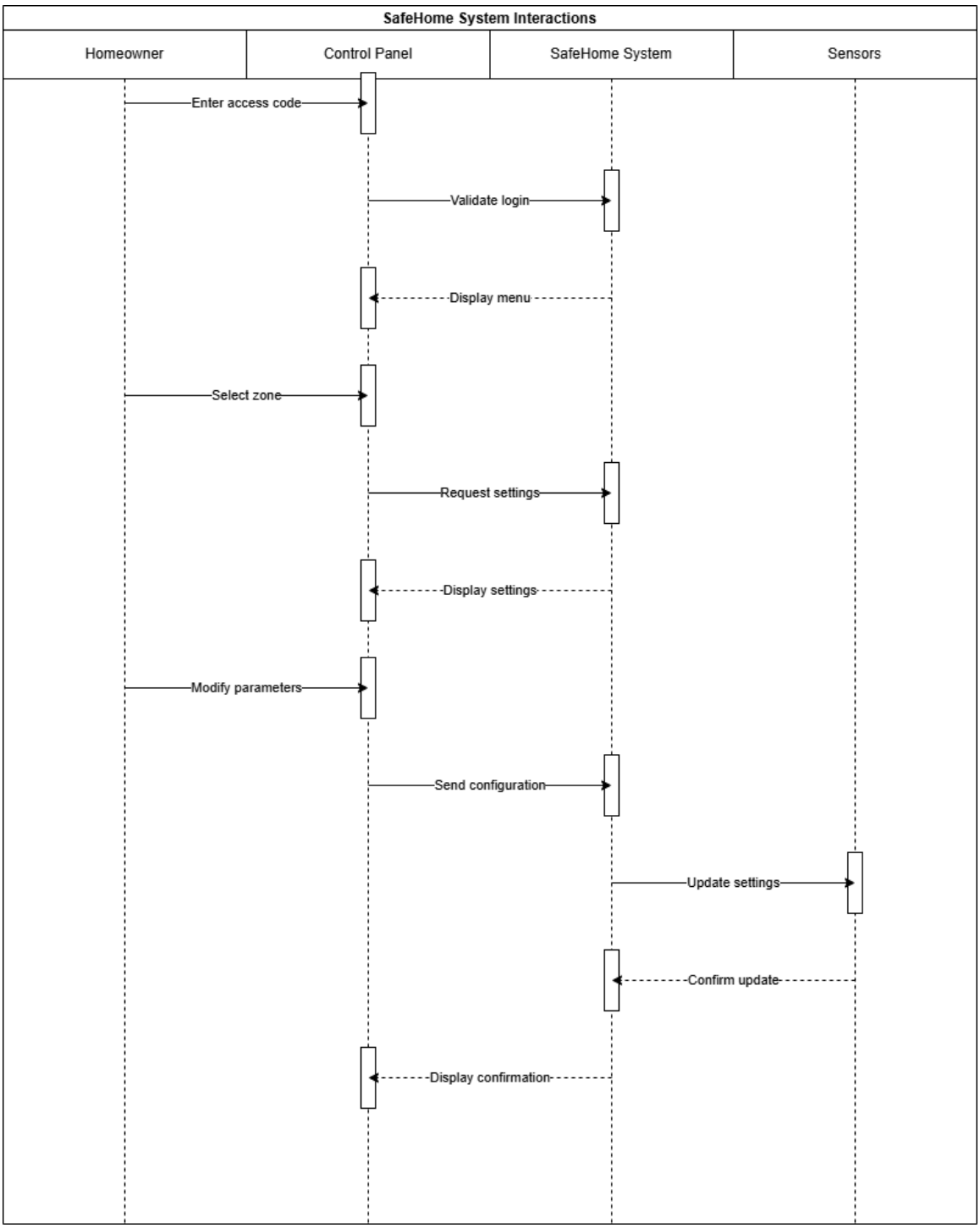
c. Selective Zone Arming



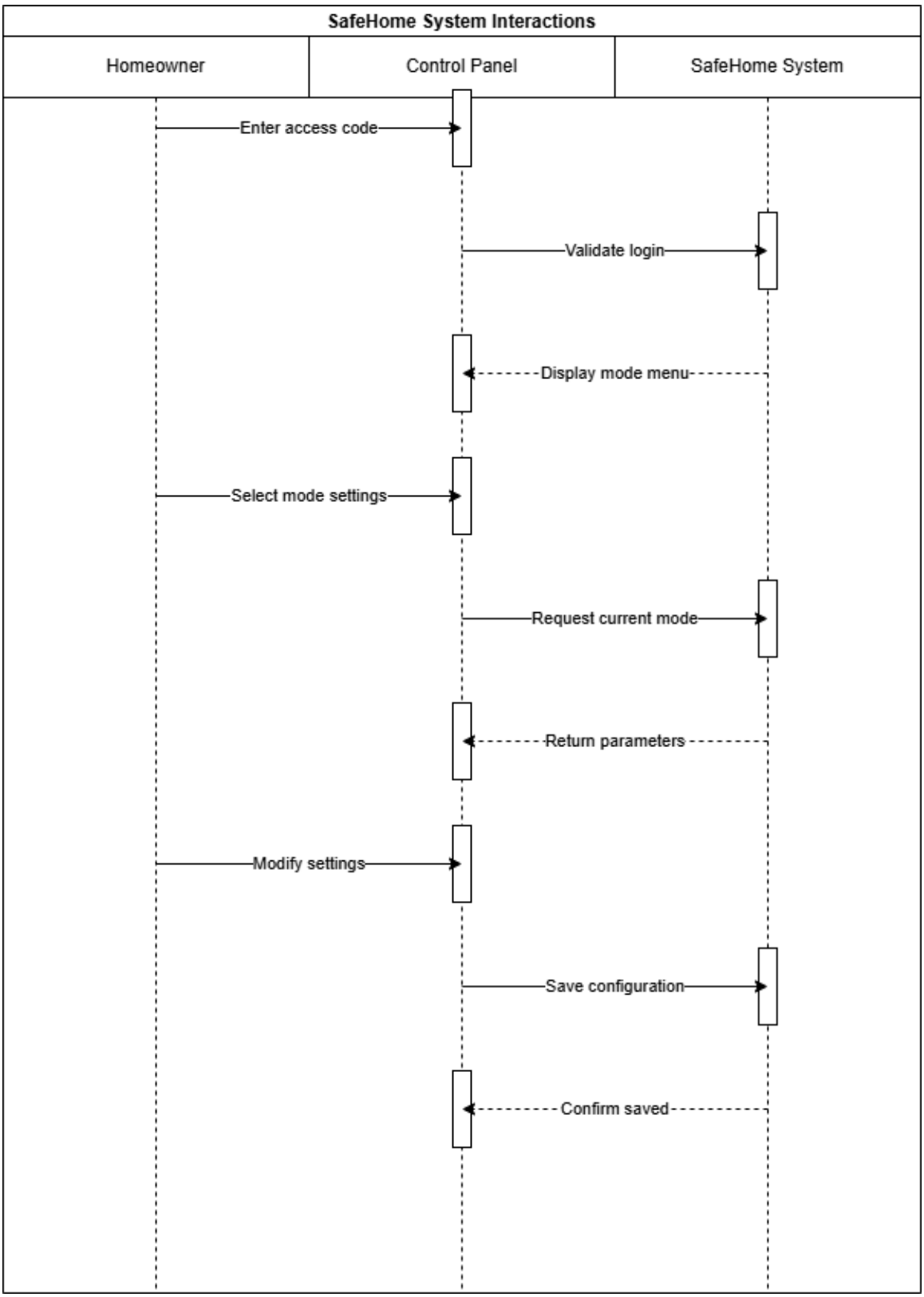
d. Alarm Condition



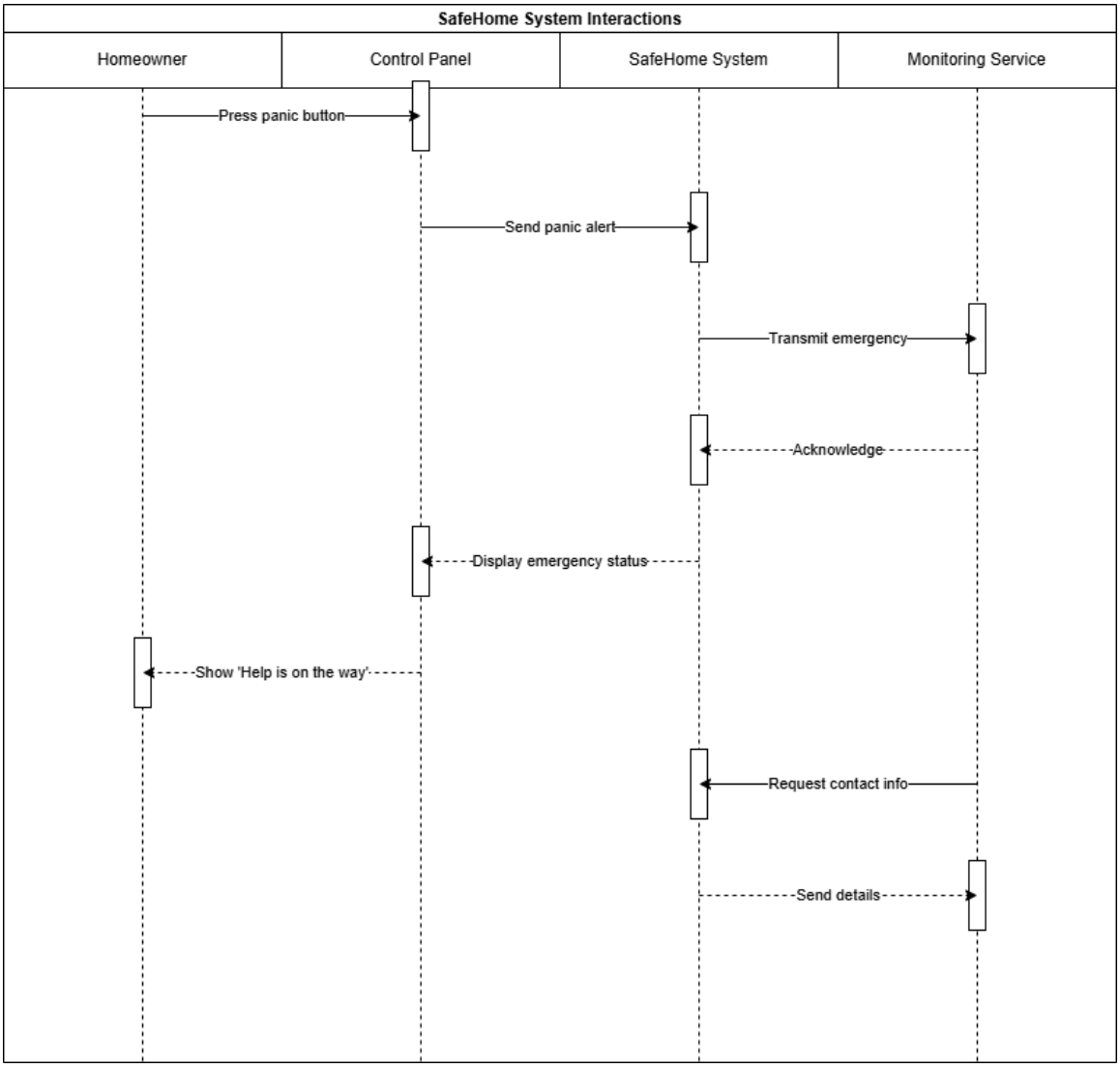
e. Reconfigure Zone



f. Configure Modes

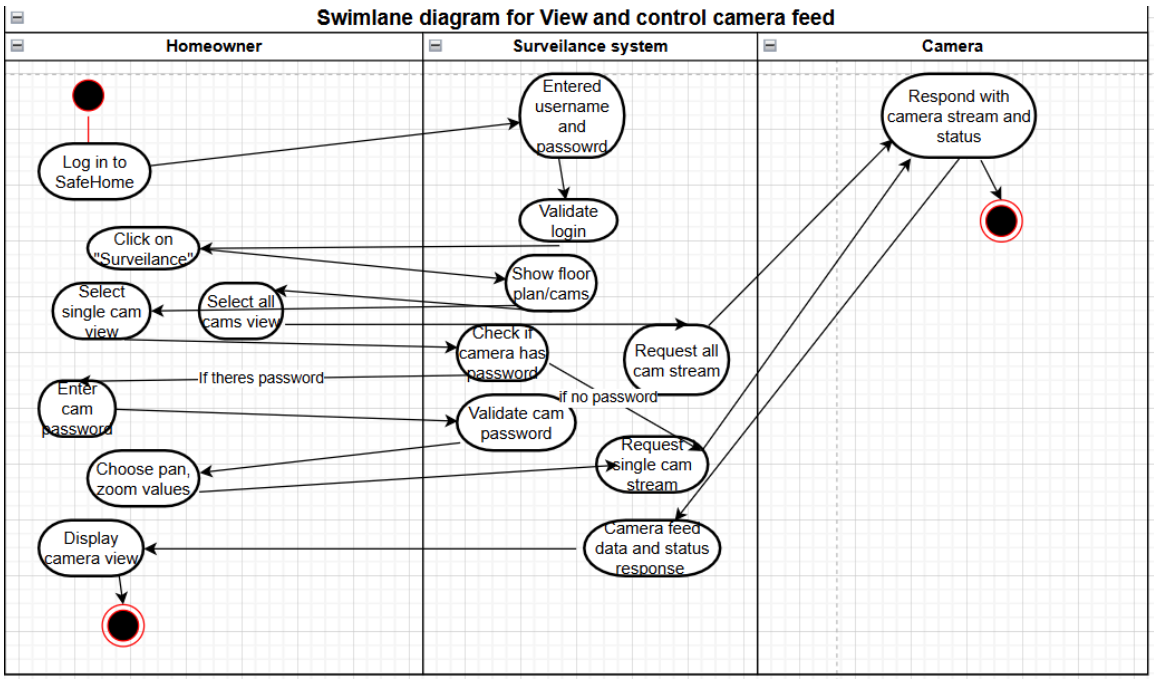


g. Panic Button

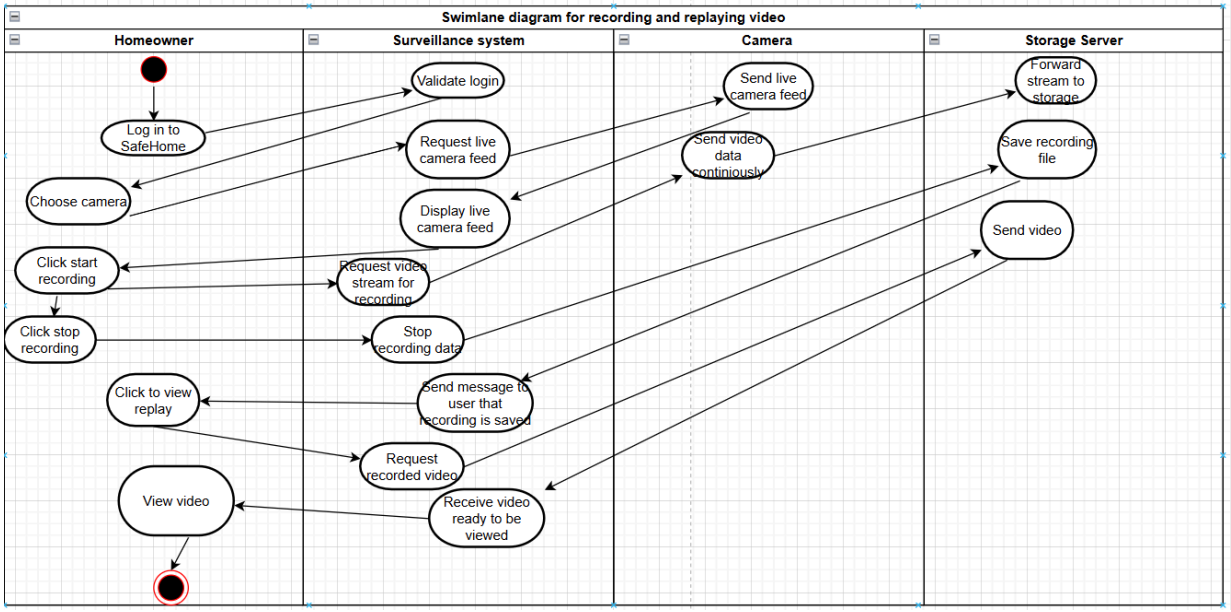


3. Surveillance Sequence Diagram

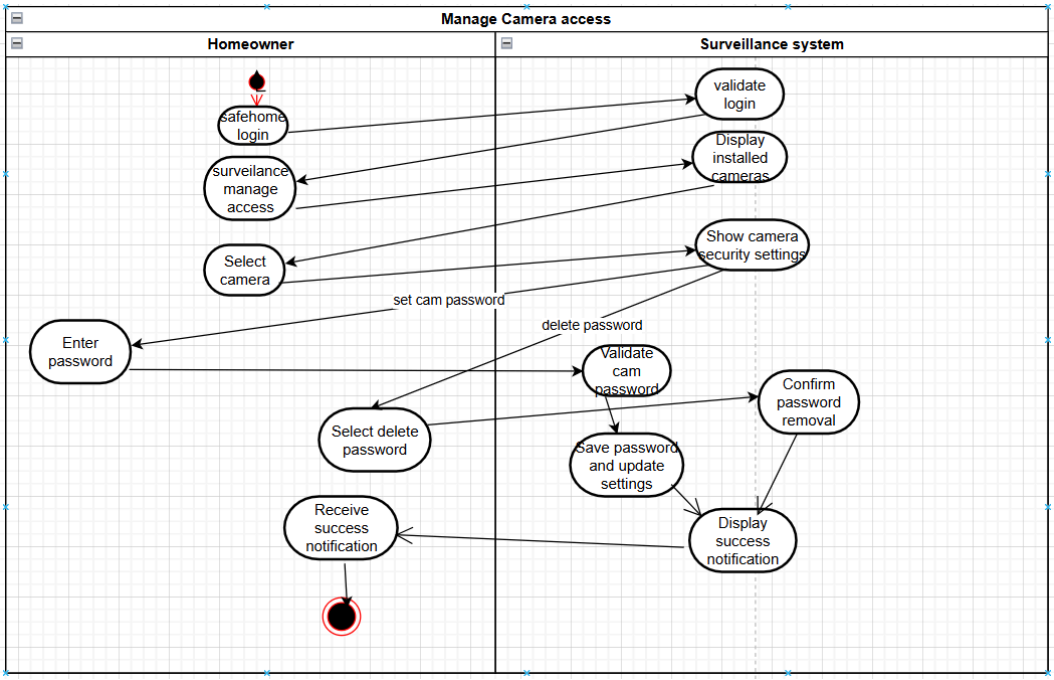
a. View and control camera feed



b. Record and replay video



c. Manage camera access



VIII. Who did what

Team member Geunyeong
1. Use case diagram (UML use case diagram) 2. Use case scenario for common functions 3. Sequence diagram for common functions 4. Refinement of sequence diagram 5. Finding reference from SEPA 6. Writing Meeting logs 7. Writing project schedule 8. Added glossary
Team member Alan
1. Use cases for Surveillance 2. Use case diagram for Surveillance 3. Sequence diagram for Surveillance 4. Added references from dialogue for some of the assumptions 5. Added additional assumption
Team member Yernaz
1. Use cases for Configure Safety Zone 2. Use case diagram for Configure Safety Zone 3. Added references from dialogue for some of the assumptions 4. Fixed mistakes in Meeting logs
Team member Arda
1. Added additional assumptions for the security functions

2. Added references from the dialogue for some of the assumptions
3. Added Use cases for security functions
4. Added case diagram for security functions
5. Created the sequence diagram for Security functions
6.

IX. Meeting logs

Meeting logs should clearly describe 5W1H (who will do what by when with why, where and how)

Project (Why): CS350 Safehome Project - SRS
Date (When): 2025.10.28
Location (Where): Library meeting room 3A
Attendees (Who): Arda, Geunyeong, Alan, Yernaz

Meeting Summary (What)
1. Key Topics Discussed
Defining "Assumptions":

- Geunyeong asked if minor technical details (e.g., "the box is wireless") should be assumptions.
- Arda clarified that the 'Assumptions' section should focus on stakeholder expectations and opinions extracted from the safehome_dialog.pdf, not on nitpicking technical details.

Decision: The team will extract assumptions based on stakeholder expectations (e.g., "Lisa expects...") rather than basic technical facts.

Confirming SRS Template Scope:

- The team, led by Arda, defined which sections of the provided Safehome-SRS-template-v1.docx.pdf to modify and which to keep.
- Keep as-is: Overview, Introduction, Goal, Major Functionalities, Prototype GUI (for simplicity).
- Modify/Replace: Project Schedule (to match homework deadlines), Assumptions (to be fully edited), Use Case Diagrams, Use Cases (text descriptions), Sequence Diagrams.

2. Work Distribution (Action Items)
The team divided the four main functional areas for the Use Case Diagrams and Use Case text descriptions among the four members.

Who (Owner)	**What (Assigned Task)**
Arda	Security Functions

Geunyeong	Common Functions
Alan	Surveillance Functions
Yernaz	Configure Safety Zone

Decisions & Action Items (How & By When)

Who	What (Action Item)	When (Deadline)
Arda	Complete the Use Case Diagram and Use Case descriptions for Security Functions.	Before next meeting
Geunyeong	Complete the Use Case Diagram and Use Case descriptions for Common Functions.	Before next meeting
Alan	Complete the Use Case Diagram and Use Case descriptions for Surveillance Functions.	Before next meeting
Yernaz	**Create** a new section for the Use Case Diagram and Use Case descriptions for Configure Safety Zone (which was missing from the template).	Before next meeting

Arda	**Ask the TA:** Clarify if the Assumptions section only needs references for existing items, or if the team should add new assumptions.	Before next meeting
All	Read the entire safehome_dialog.pdf individually to analyze their assigned sections.	Before next meeting
All	The Sequence Diagrams will be developed collaboratively after the use cases are complete.	TBD

Appendix A. Glossary

Control panel: a small gadget to display basic information and receive your commands See Fig. 1 in page 6, use case “Log onto the system through control panel” in page 11, and …

Guest: A non-homeowner, such as a housekeeper or repair person, who needs temporary access to the home. This actor has limited system privileges via a Guest password.

Arm / Disarm: The action of activating (Arm) or deactivating (Disarm) the system's sensors. When armed, a triggered sensor will cause an alarm.

Control Panel: A small gadget (physical hardware keypad) to display basic information and receive user commands. (See Fig. 1) .

Homeowner: The primary actor of the system. This user has full administrative privileges, including configuring settings, changing master passwords, and accessing all functions.

Monitoring Service: An external security company or agency that is automatically called by the system when an alarm condition is encountered or the panic button is pressed.

Panic Button: A dedicated button on the Control Panel (Fig 1.) designed for the user to manually trigger an emergency alarm and call the Monitoring Service .

Safety Zone: A logical grouping of sensors (e.g., "First Floor," "Bedrooms") defined by the Homeowner. A zone can be armed or disarmed independently of other zones .

Sensors: Hardware devices that detect changes in the physical environment, such as door/window sensors or motion detectors .

System Administrator: Refers to a role played by the Homeowner when performing configuration tasks, or the system itself acting as a facilitator. It is not a dedicated IT person .

Thumbnail Shots: A feature of the surveillance function that displays small, simultaneous video feeds from all cameras on a single screen.

Web Browser: The software interface (e.g., on a PC) used by the Homeowner to remotely access, monitor, and control the SafeHome system via the Internet .