# CS350 Safehome Project

## Software Requirement Specification (SRS)


**Project Team #9 Members:**

| | |
|---|---|
| **20220541** | Jien Lee |
| **20240410** | Jonghwa An |
| **20240685** | Minseok Jo |

# Table of Contents

# I. Overview

## 1. Introduction

SafeHome is a new-generation home automation and security product designed for private homeowners. In an age of increasing mobility, SafeHome addresses the fundamental need for a flexible, accessible, and reliable system to manage and protect one's property. By integrating security, surveillance, and remote environmental controls into a single, cohesive web-based platform, SafeHome makes comprehensive home management feasible for everyone.

The system is built on the principle of providing absolute safety and peace of mind. It provides a convenient and secure way for homeowners to manage their property, granting access not only to themselves but also to trusted individuals with specific, time-limited permissions.

This document provides the Software Requirement Specification (SRS) for the SafeHome system. It details the functional and non-functional requirements, use cases, and operational scenarios that define the system's behavior and capabilities, focusing on its web-based interface and core functionalities.

## 2. Goal

Providing a safe, secure, and remotely managed home environment is the primary goal of this project. The customer who uses this product will be assured that their home is safe and controllable from anywhere with an internet connection.

1. Functional Goals are to provide the following:

    a. Security Functions: To remotely arm/disarm the system, manage distinct security zones, and provide immediate alerts upon sensor detection.
    b. Surveillance Functions: To provide real-time visual monitoring and access to recorded footage, complete with motion event indicators.
    c. Remote Control Functions: To offer remote management of integrated smart home devices, specifically home lighting and air conditioning systems.
    d. Access Management Functions: To provide secure, role-based access control and allow Homeowners to easily create and manage temporary or restricted access for Authorized Guests.
2. Non-Functional Goals & Principles are as follows:
    a. Reliability: The system must provide reliable service 24/7, especially in handling critical alarm conditions and sensor triggersensor detecus.
    b. Security: The system must be secure against unauthorized access. All web-based interactions must be protected, and user authentication must be robust.

c. User-friendliness: The web interface must be intuitive and simple to navigate for all user roles, ensuring that complex tasks like zone configuration or guest management are straightforward.
d. Customization: The system must be configurable to a specific homeowner's environment, allowing for the creation of custom safety zones, sensor assignments, and granular guest permissions.
e. Completeness: The SafeHome system developed will implement all functions specified in the functional requirements detailed in this document.

## 3. Major Functionalities

Based on the detailed Use Cases, the system's major functionalities are categorized as follows:

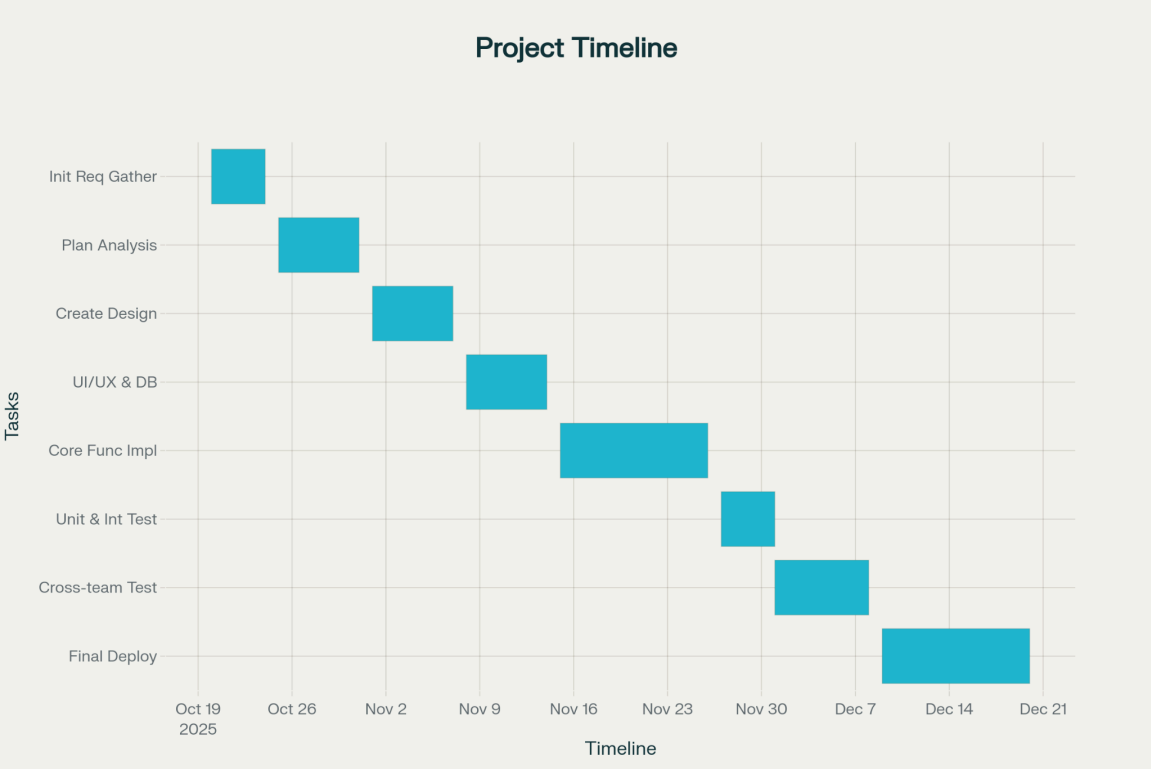
1) Common Use Cases: Defines the system's foundational interactions. This includes secure, role-based login via the web portal using a User ID and 4-digit password, and a comprehensive system configuration module for high-level settings.
2) Security Use Cases: Comprises the core defense mechanisms. This allows Homeowners and Authorized Guests to remotely arm/disarm the entire system or selectively manage individual safety zones. It defines the system's response to an alarm condition and includes controls to enable or disable cameras for privacy or monitoring.
3) System Configuration & Access Management: Covers the administrative setup of the system. This allows Admins to manage safety zones and manage hardware. It also empowers Homeowners to manage guest access, creating unique guest accounts with specific, time-limited permissions and 4-digit passwords.
4) Remote Control Use Cases: Details the smart home integration. This allows authorized users to remotely control home lighting and fully manage the air conditioning system, including viewing zone status, changing modes, setting temperatures, and scheduling ON/OFF timers.
5) Surveillance Use Cases: Describes the complete visual monitoring suite. This includes a thumbnail overview of all accessible cameras, a specific camera live view, Pan/Tilt/Zoom controls, the ability to replay recorded video from a timeline, and a camera event display that highlights cameras on the overview map when motion is detected.

# 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 24, 2025 |
| Planning and creating analysis model | Oct 25 - Oct 31, 2025 |
| Creating design model | Nov 1 - Nov 7, 2025 |
| UI/UX design, database schema | Nov 8 - Nov 14, 2025 |
| Core functionality implementation | Nov 15 - Nov 26, 2025 |
| Unit testing and integration testing | Nov 27 - Dec 1, 2025 |
| Cross-team integration testing&bug fixing | Dec 1 - Dec 8, 2025 |
| Final deployments, documentation updates | Dec 9 - Dec 20, 2025 |



# III. Prototype GUI


**Fig 1. Login Screen**

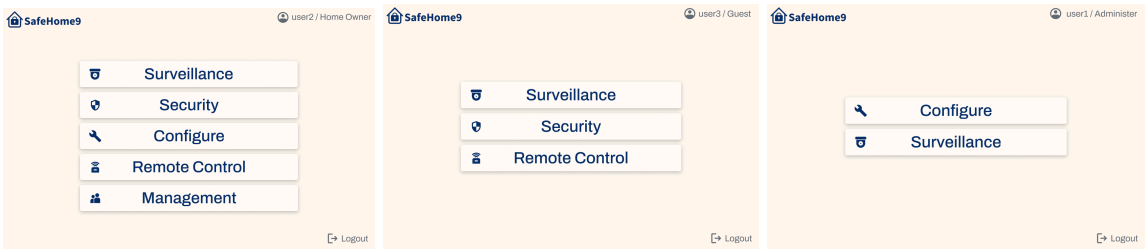



**Fig 2. MainFunctions(Administer/Home Owner/Guest)**

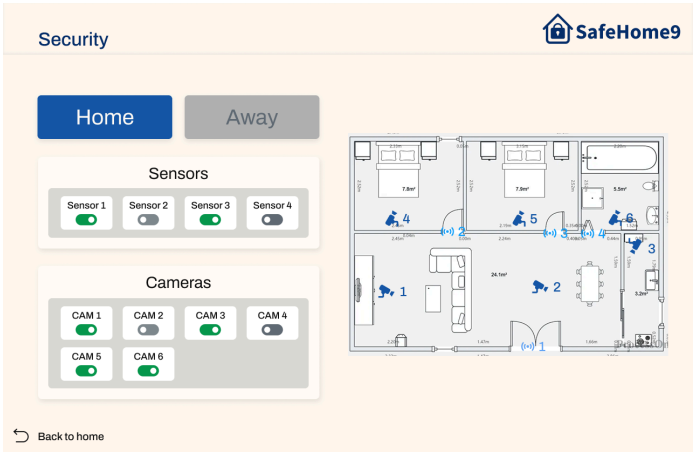



**Fig. 3 Security Function**


**Fig. 4 Configuration Function(Administer/Home Owner)**


**Fig. 5.1 Surveillance Function(Administer)**


**Fig. 5.2 Surveillance Function(Home owner, Guest) – Grid View**

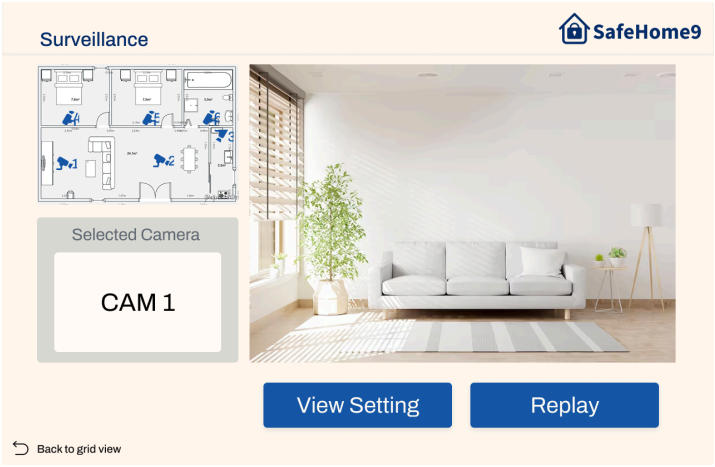



**Fig. 5.3 Surveillance Function – Full Screen View**

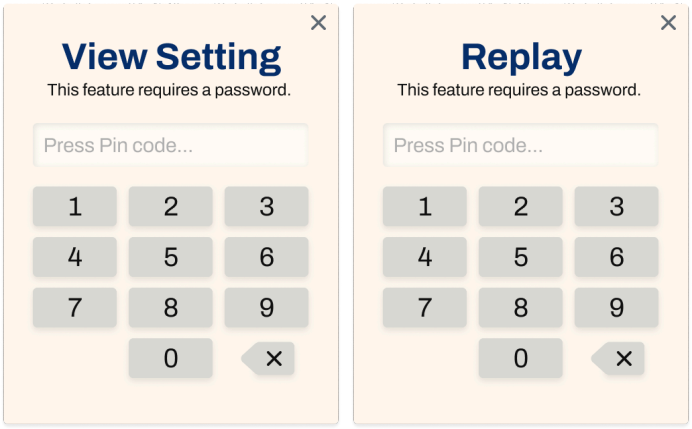



**Fig. 5.4 Surveillance Function – Pin-code Input Window(View Setting/Replay)**

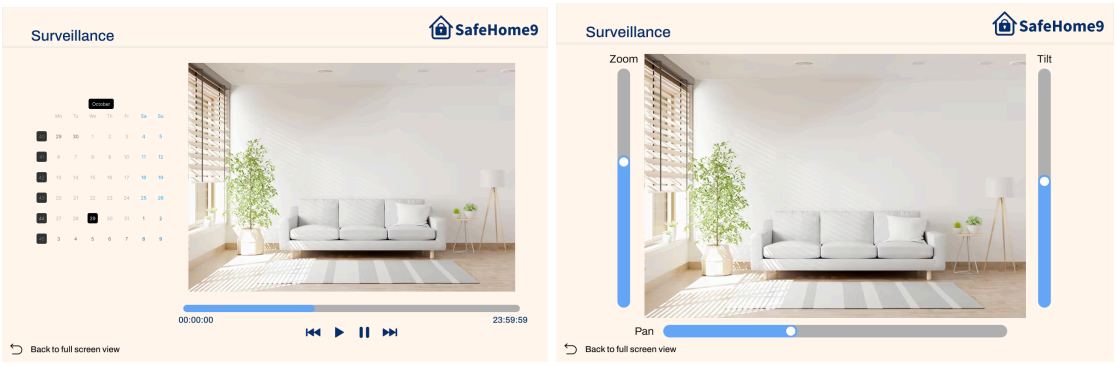



**Fig. 5.5 Surveillance Function – View Setting/Replay**

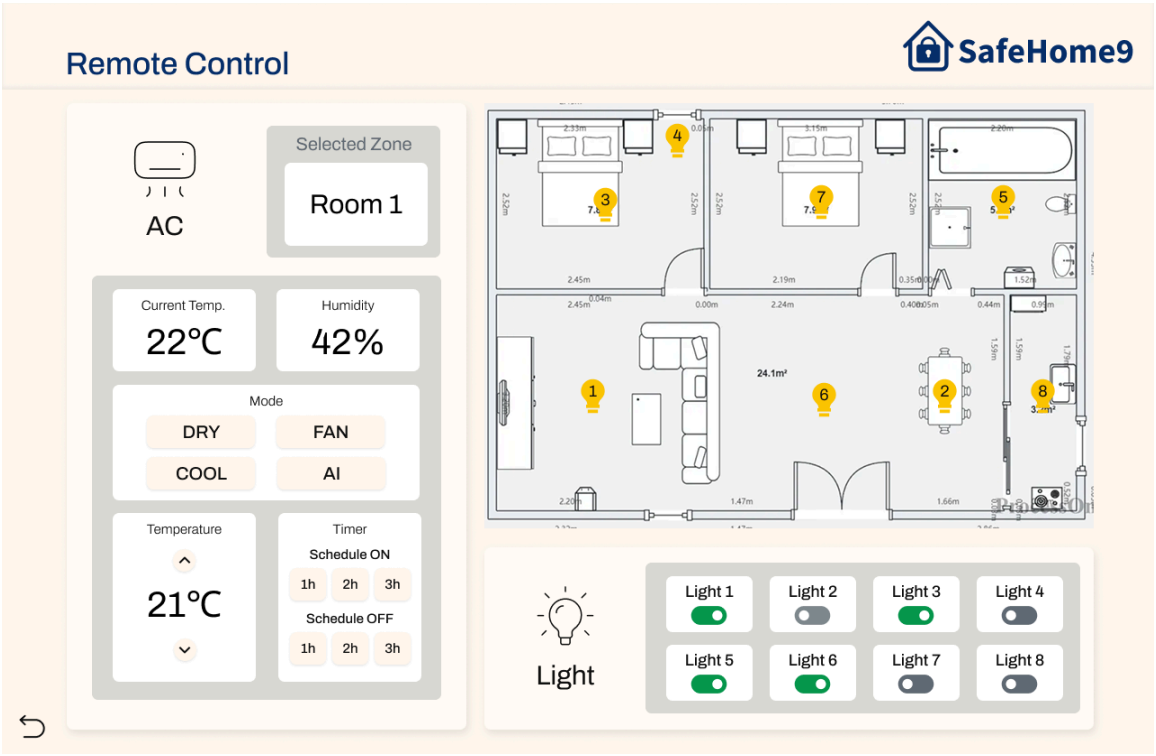



**Fig. 6 Remote Control Function**

# IV. Assumptions

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

2. Reconfiguring floor plan or relocating the sensors or cameras are not in the scope of our project. The rearrangement of sensors or cameras can be replaced by the add/delete sensors/cameras function on page 26~29.

3. In reference to Use Case 2.c, the "notification" received by the Homeowner/Guest is assumed to be SMS message, or push notification sent to their registered mobile device(s). This is triggered by the System concurrently with the notification to the Monitoring Service and the local audible alarm.

4. “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.

5. Intrusion logs (e.g., login attempts, arm/disarm events, alarms) are maintained centrally on the system server as backend log files. These logs are intended primarily for system diagnostics, debugging, and advanced auditing by system administrators/developers, and are not directly accessible to Homeowner or Administer roles via the SafeHome Web user interface.

6. We added enabling and disabling all the cameras

7. When the user enters an incorrect PIN 3 consecutive times in page 41, the system locks further PIN entry for 30 seconds. After the 30-second lock period, the system automatically unlocks and resets the PIN input attempt counter to 3. This cycle repeats for each 3 consecutive incorrect PIN attempts, with the system prompting the user appropriately about their lock status and remaining wait time.

8. The 4-digit password for Log onto the system and the PIN for high-sensitivity functions are separate credentials. The 4-digit password authenticates the user's web session. The PIN is a secondary authorization required within an authenticated session to access specific sensitive functions. The "3 consecutive incorrect attempts" lockout policy for 30 seconds will apply independently to both the 4-digit password and the PIN.

9. All recorded video from enabled cameras is automatically uploaded to a pre-configured server in 1-hour intervals.

10. Video stored on the server is automatically deleted 30 days after upload.

11. In the event of an internet connection failure during video upload, recordings will be buffered locally within the SafeHome Control Panel. Upon internet reconnection, the system will automatically resume uploading any unsent buffered video data, ensuring continuity. If the local buffer capacity is exceeded, the oldest recorded video footage will be automatically deleted (FIFO) to accommodate new recordings.

12. The SafeHome Control Panel is connected to the Internet (cloud) to support external access and settings. However, the final equipment control, such as the lighting inside the house and the air conditioner (A.C), is done directly through the internal bus or the local area network, not through the Remote Protocol method.

13. The system will adopt a "Last Command Wins" policy for concurrent commands. The most recent valid command from any authenticated session will override the previous state. Concurrent login sessions will be permitted.

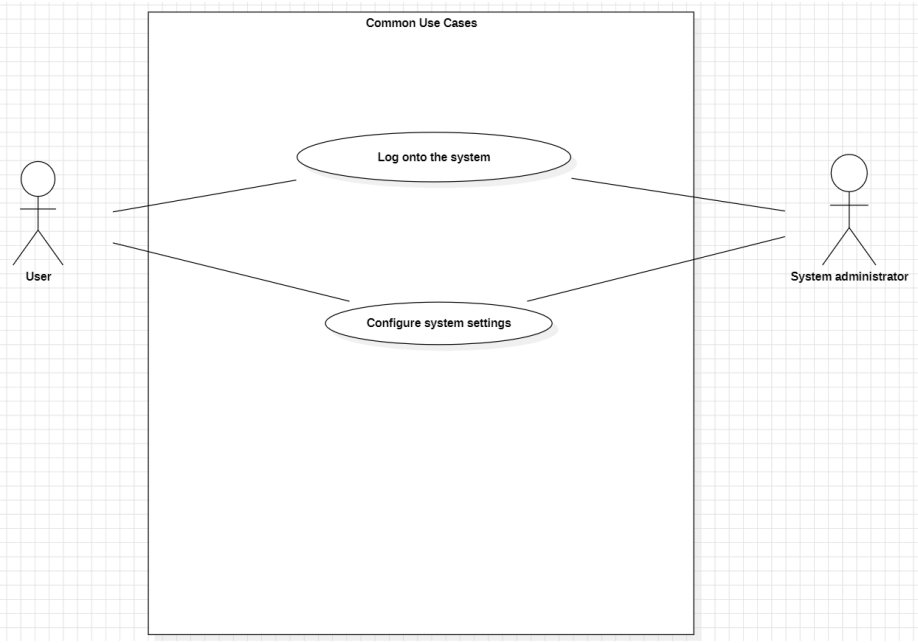
14. Guest privileges will be managed by the Homeowner via a checklist upon creation.

15. The system will periodically check the 'heartbeat' of all connected hardware. If a device fails to respond, its status will be updated to 'Offline' on the web interface. The system will prevent arming a zone if a critical sensor within that zone is 'Offline'. Commands sent to 'Offline' devices will be rejected with an error message.

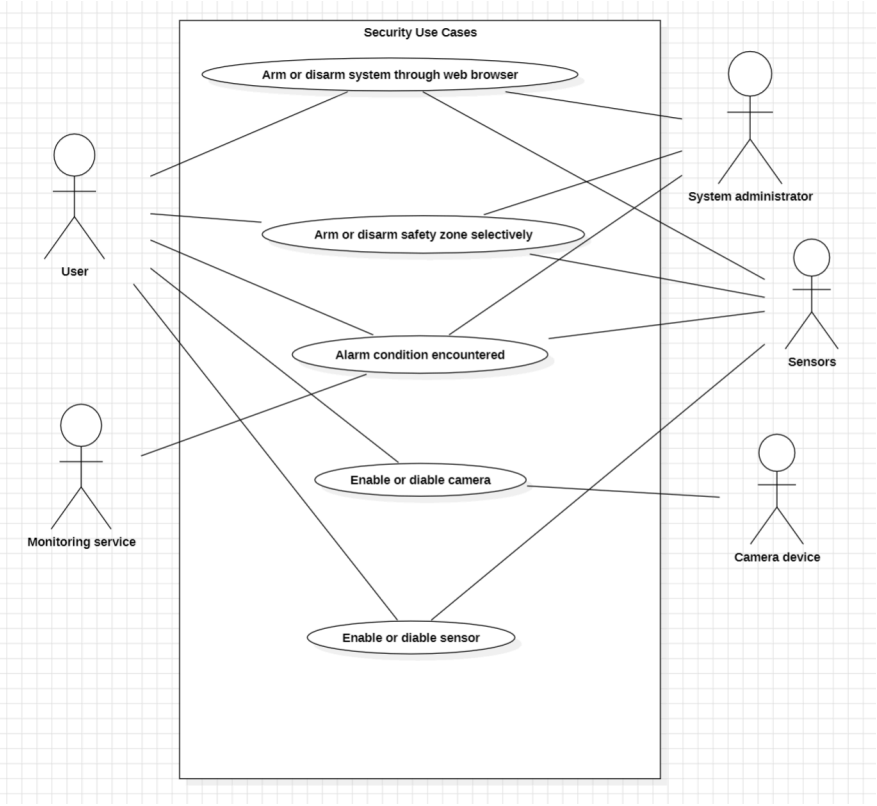
16. All web traffic must be encrypted using SSL/TLS (HTTPS).

# V. Use Case Diagrams

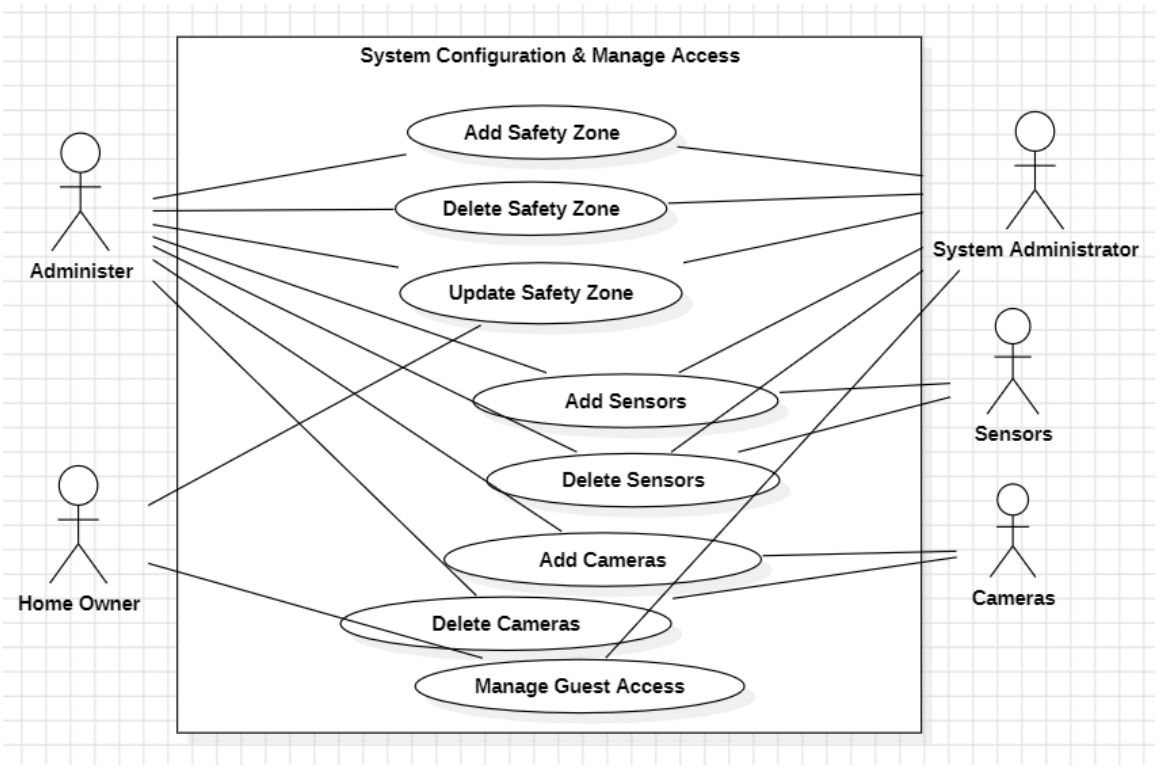
## 1. Common Functions



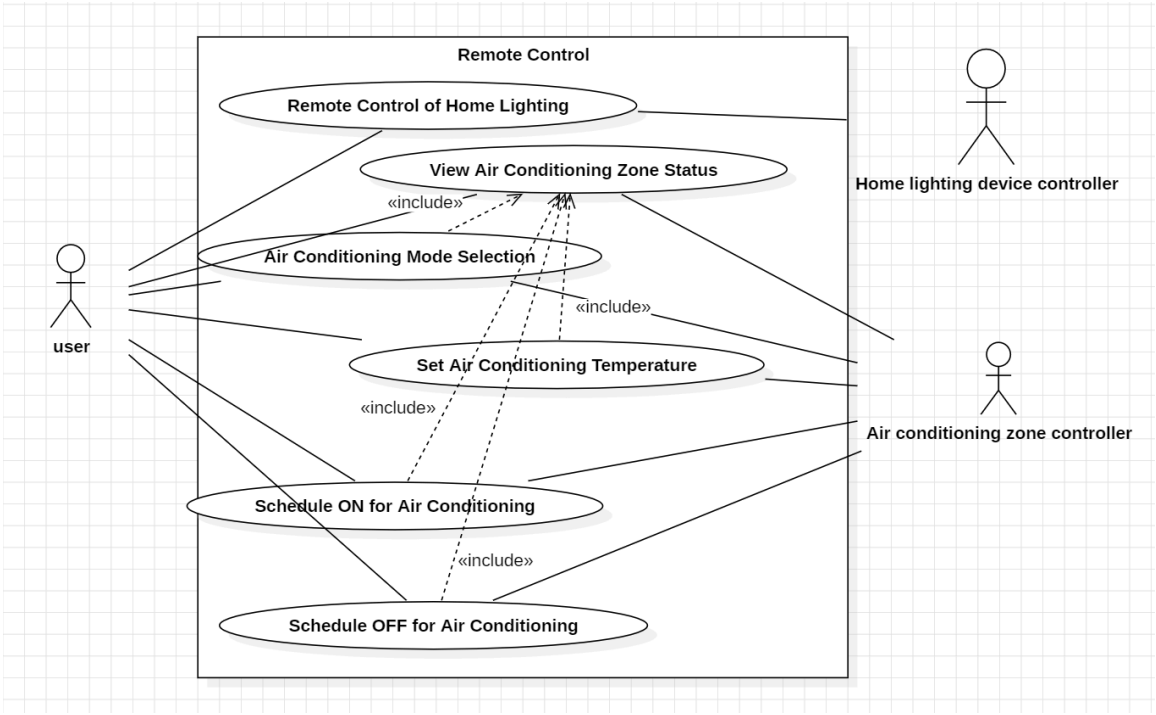

## 2. Security Functions



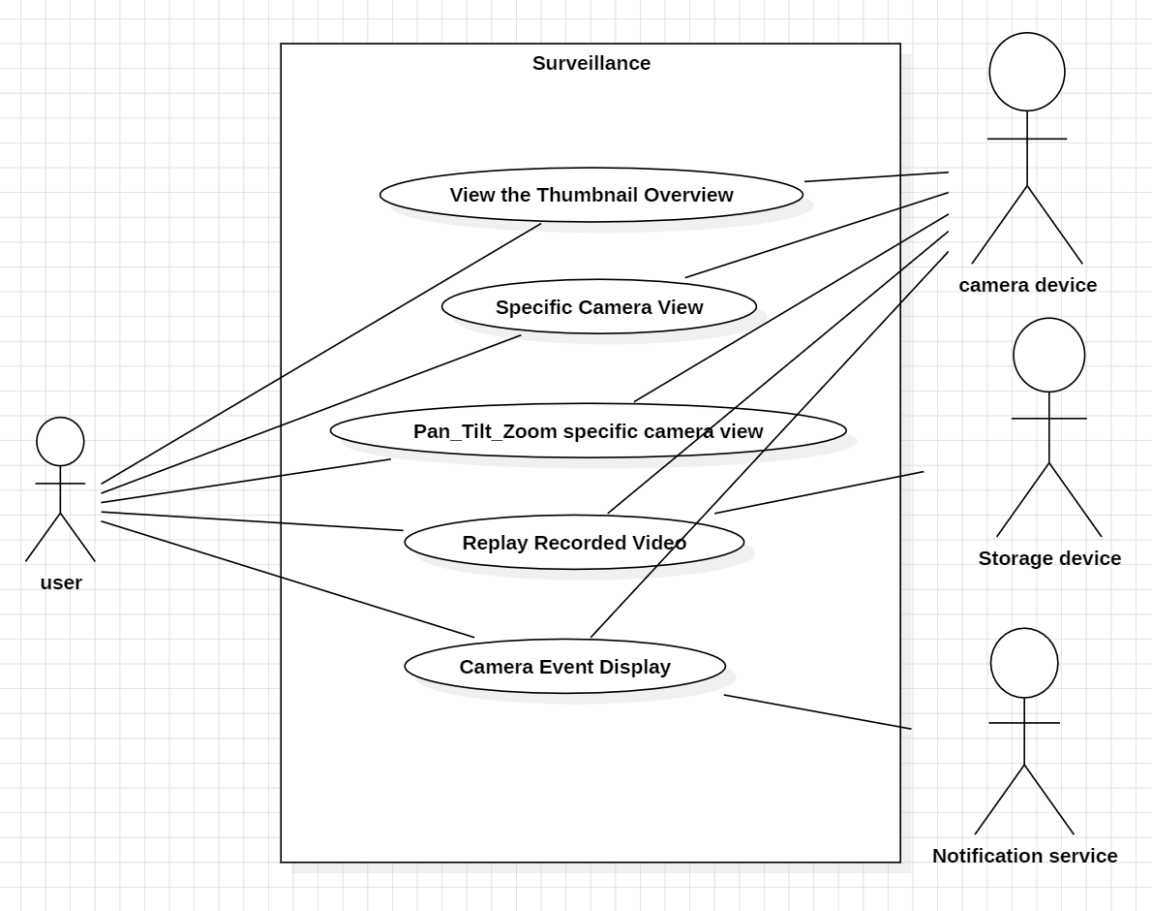
## 3. System Configuration & Manage Access Functions




## 4. Remote Control Functions



## 5. Surveillance Functions



# VI. Use Cases

## 1. Common Use Cases

### a. Log onto the system through web

Use case: Log onto the system

Primary actor: Homeowner, Guest, Administer

Goal in context: To gain authenticated access to the SafeHome system's features and data via a web browser.

Preconditions: The system is powered on and operational. The user has valid login credentials (username/ID and a 4-digit password). An internet connection is established.

Trigger: The user wishes to interact with the system (e.g., check status, change settings, arm/disarm).

Scenario:

1. The user navigates to the SafeHome web portal.
2. The system presents the login screen requesting a User ID and a 4-digit Password.
3. The user enters their credentials.
4. The system validates the credentials against its user database.
5. Upon successful validation, the system grants access and displays the user's dashboard or main interface, appropriate to their access level.

Exception:

4a. Invalid credentials: The system denies access and displays an "Invalid User ID or Password" message.

4b. Account locked due to too many failed attempts: The system denies access and displays an "Account Locked" message, providing instructions for recovery.

4c. Network connection lost: The system cannot communicate with the server, displaying a connection error.

Priority: High

When available: First increment

Frequency of use: Very Frequent

Channel to actor: Web browser

Secondary actors: System Administrator

Channels to secondary actors: safehome system for admin tools.

Open issues:

1. What is the password recovery process for a forgotten 4-digit password?
2. How are concurrent logins from different web browsers/devices handled?
3. Potential point of discussion: Given the 4-digit password limitation, is a secondary authentication factor (e.g., 2FA) considered for enhanced security, especially for Admin or Homeowner accounts?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg18, 20]**

**b. Configure system setting**

Use case: Configure system setting

Primary actor: Homeowner, Authorized Guest, Administer

Goal in context: To modify system parameters such as safety zone setting, or changing information of safety zones

Preconditions: The system is operational. The user is logged in via web browser with appropriate privileges.

Trigger: The user decides to change system settings.

Scenario:

1. The user logs into the system via web browser.
2. The user navigates to the 'Configuration' section via the web interface.
3. The system displays configuration options. The available options depend on the user's login privileges.
4. The user selects the category to modify.
5. The user modifies the settings, then saves the changes.
6. The system validates the changes and applies the new settings.
7. The system confirms successful application of settings via the web interface.

Exception:

4a. Unauthorized user attempts to access settings beyond their defined scope: The system denies access and displays an "Unauthorized Access" message.

5a. Invalid value input: The system rejects the change and prompts for valid input.

6a. Failure to apply settings: The system displays an error message on the web interface.

Priority: High

When available: First increment

Frequency of use: Frequent during initial setup; intermittent thereafter.

Channel to actor: Web browser

Secondary actors: System Administrator

Channels to secondary actors: safehome system for admin tools.

Open issues:

1. Potential point of discussion: What specific settings can a Homeowner define for an Authorized Guest?
2. How are configuration changes logged for security auditing purposes?
3. Is there a rollback mechanism for configuration changes?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 21, 73, 74]**

## 2. Security Use Cases

**a. Arm/disarm system through web browser.**

Use case: Arm/disarm system through web browser

Primary actor: Homeowner, Authorized Guest

Goal in context: To remotely change the entire security system's status via a web interface.

Preconditions: The system is powered on and operational. The user is logged into the system via web browser with appropriate permissions. An internet connection is established.

Trigger: The Homeowner or Authorized Guest decides to remotely change the home's security status.

Scenario:

1. The user logs into the SafeHome web portal.
2. The user navigates to the 'Security' section on the web interface.
3. The system displays the current security status and available options.
4. The user selects the desired security state.
5. If arming, the system may prompt the user to confirm that all monitored doors/windows are closed.
6. The system processes the command, arming or disarming all relevant sensors based on the selected state.
7. The web interface displays a confirmation message with the new system status.

Exception:

5a. User attempts to arm but a monitored sensor is open: The system displays a warning message ("Door/window open") and may prevent arming until the condition is resolved or manually bypassed.

1-7a. Loss of internet connection during command: The operation fails, and the system status remains unchanged.

1-7b. Alarm condition encountered during this process: (Refer to Use case "Alarm condition encountered")

5b. Unauthorized Guest attempts to arm/disarm beyond their delegated authority: The system denies the action and displays an "Unauthorized" message.

Priority: High

When available: First increment

Frequency of use: Frequent

Channel to actor: Web browser

Secondary actors: System Administrator, Sensors

Channels to secondary actors: System administrator: safehome system. Sensors: wireless connectivity

Open issues:

1. What is the expected response time (latency) for remote arming/disarming via

web browser?

2. How are conflicts handled if a user attempts to change system status via two different web browser sessions simultaneously?
3. How are bypass codes or temporary overrides handled for specific sensors when arming?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 21]**

**b. Arm/disarm safety zone selectively**

Use case: Arm/disarm safety zone selectively
Primary actor: Homeowner, Authorized Guest
Goal in context: To activate or deactivate specific safety zones via a web interface without changing the overall system's global armed/disarmed status.
Preconditions: The system is running. The user is logged in via web browser. Safety zones are pre-configured by the Homeowner. An internet connection is established.
Trigger: The user wishes to keep one part of the house armed/disarmed while another part remains disarmed/armed.
Scenario:

1. The user logs into the system via web browser.
2. The user navigates to the ‘Configure’ section on the web interface.
3. The system displays a list of defined safety zones and their current status.
4. The user selects a specific zone to change.
5. The user toggles its status.
6. The system validates the request and the user's authority for that zone.
7. The system arms/disarms only the sensors associated with the selected zone.
8. The system updates the status display for the affected zone on the web interface.

Exception:

5a. Attempting to arm a zone with an open sensor: The system displays a warning and prevents arming that specific zone until the condition is resolved or bypassed.

1-8a. Alarm condition encountered: (Refer to "Alarm condition encountered" use case)

1-8b. Loss of internet connection during command: The command fails, and the zone status remains unchanged.

5b. Unauthorized Guest attempts to arm/disarm a zone for which they lack delegated authority: The system denies the action and displays an "Unauthorized" message.

Priority: High
When available: First increment
Frequency of use: Frequent

Channel to actor: Web browser
Secondary actors: System Administrator, Sensors
Channels to secondary actors: System administrator: PC-based system. Sensors: wireless connectivity
Open issues:

1. How does selective zone arming interact with the overall system's 'Away' or 'Home' status? (e.g., does arming a zone override a global 'Disarmed' state for that zone?)
2. Can Homeowners set specific schedules for zone arming/disarming via the web interface?
3. How are the permissions for Authorized Guests to arm/disarm specific zones managed by the Homeowner via the web interface?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 21]**

**c. Alarm condition encountered**

Use case: Alarm condition encountered
Primary actor: Homeowner, Authorized Guest, Monitoring Service
Goal in context: To alert the Homeowner, Guest, and/or a monitoring service when an armed sensor detects an intrusion or a specific event and initiate a response.
Preconditions: The system is in an "Armed" state. Sensors are active and configured. An internet connection is established.
Trigger: An armed sensor detects an event that meets alarm criteria.
Scenario:

1. An armed sensor detects an intrusion/event.
2. The sensor sends a signal wirelessly to the main system.
3. The system validates the signal and confirms the armed status of the affected zone/system.
4. The system activates an audible alarm locally.
5. The system displays an alarm message on the web interface.
6. The system automatically sends notifications to the monitoring service.
7. The Homeowner/Guest receives the notification.
8. The Homeowner/Guest logs in via web browser to verify the system status or investigate the alarm via surveillance cameras on the web interface.
9. The Homeowner/Guest can disarm the system by entering their 4-digit password on the web interface.

Exception:

1a. False alarm: Sensor invokes the wrong alarm for some reason.
6a. Internet connection failure: The system cannot send remote notifications to the monitoring service.

6b. Power outage: The sensor's battery is low and cannot function.

9a. User attempts to disarm with an incorrect password: The system denies the disarm command and may log the failed attempt.

Priority: High
When available: First increment
Frequency of use: Infrequent
Channel to actor: Web browser
Secondary actors: System Administrator, Sensors, Monitoring Service
Channels to secondary actors: Sensors: wireless connectivity. Monitoring Service.
Open issues:

1. What is the procedure for canceling a false alarm after it has been reported to the monitoring service?
2. How are different alarm types handled or prioritized?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 63-64, 68]**

**d. Enable/disable camera**

Use case: Enable/disable camera
Primary actor: Homeowner, Authorized Guest
Goal in context: To control the operational state of specific cameras via the web interface.
Preconditions: The camera is physically installed and connected to the SafeHome system. The user is logged into the system via web browser with appropriate authorization. An internet connection is established.
Trigger: The user wishes to control camera operation for surveillance, privacy, bandwidth/storage management, or to prepare for motion detection.
Scenario:

1. The user logs into the SafeHome web portal.
2. The user navigates to the 'Security' section on the web interface.
3. The system displays a list of installed cameras and their current status.
4. The user selects the specific camera they wish to manage.
5. The user clicks the toggle to change the state.
6. The system sends the corresponding command to the selected camera.
7. The system updates the status of the camera on the web interface to reflect the new state.
8. The web interface behavior updates.

Exception:

4a. User attempts to manage a camera for which they lack authority: The system displays an "Unauthorized Access" message.

6a. Camera not responding or disconnected: The system displays an error message and the camera status remains or reverts to 'Disabled'.

6b. Network connection lost during command: The command fails, and the camera state may remain unchanged.

Priority: High
When available: First increment
Frequency of use: Moderate
Channel to actor: Web browser
Secondary actors: Camera device
Channels to secondary actors: Camera device
Open issues:

1. How are recording preferences configured (e.g., continuous, on motion detection, scheduled) when a camera is enabled?
2. What is the expected latency for live streaming after a camera is enabled or disabled?
3. How is data storage managed for recorded footage?
4. What is the default state of cameras when the system is armed/disarmed?
5. Can a disabled camera still be triggered to record by an alarm event, or must it be actively enabled?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 34]**

**e. Enable/disable sensor**

Use case: Enable/disable sensor
Primary actor: Homeowner, Authorized Guest
Goal in context: To control the operational state of specific security sensors via the web interface, influencing their role in the armed system.
Preconditions: The sensor is physically installed and connected to the SafeHome system. The user is logged into the system via web browser with appropriate authorization. An internet connection is established.
Trigger: The user wishes to temporarily bypass a sensor or to reactivate a bypassed sensor.
Scenario:

1. The user logs into the SafeHome web portal.
2. The user navigates to the 'Security' section on the web interface.
3. The system displays a list of installed sensors and their current status.
4. The user selects the specific sensor they wish to manage.
5. The user clicks the toggle to change the state.
6. The system sends the corresponding command to update the sensor's status.

7. The system updates the status of the sensor on the web interface to reflect the new state.

Exception:

4a. User attempts to manage a sensor for which they lack authority: The system displays an "Unauthorized Access" message.

6a. Sensor not responding or disconnected: The system displays an error message and the sensor status may remain unchanged or revert.

6b. Network connection lost during command: The command fails, and the sensor state may remain unchanged.

Priority: High
When available: First increment
Frequency of use: Infrequent
Channel to actor: Web browser
Secondary actors: Sensors
Channels to secondary actors: Sensor device: wireless connectivity.
Open issues:

1. How does a bypassed sensor behave if the system enters an alarm state?
2. Are bypassed sensors automatically re-enabled when the system is disarmed and re-armed, or do they remain bypassed until manually re-enabled?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 21]**

## 3. System Configuration & Access Management

### a. Add Safety Zones

Use case: Add Safety Zones
Primary Actor: Administer
Goal in Context: To create a safety zone by filling in information such as area and location.
Precondition: The SafeHome system is operational.
Trigger: Initial system setup, property renovation, or a major change in security policy requires restructuring zones.
Scenario:

1. The Administer logs into the system – see use case: "Log onto the system through control panel".
2. The Administer clicks the 'Configure' button on the home screen.
3. The System displays the Configuration screen, showing buttons for 'Add Safety Zone', 'Delete Safety Zone', and 'Update Safety Zone'.
4. The Administer selects the 'Add Safety Zone'.

5. The System displays the creation interface. The Administer enters the Zone Name and defines core security parameters (Entry/Exit Delay, Sensitivity).
6. The System validates the changes and applies the updated zone configuration.

Exception:

5a.Administer enters a Zone Name that is already in use: The System displays a warning and requires a unique Zone Name.

5b. Administer attempts to proceed without entering a Zone Name or required security parameter (e.g., Entry/Exit Delay): The System highlights the missing fields and displays an error requiring completion.

6a. Administer enters an invalid value or format for a security parameter (e.g., Delay value out of range): The System rejects the input, displays a format error, and prevents advancing to validation.

6b. The System successfully validates parameters but fails to apply the new zone configuration due to an internal error (e.g., bus communication issue): The System displays a system error message to the Administer and logs the failure internally.

Priority: Essential
When available: First increment
Frequency of use: Infrequent
Channel to actor: Web browser
Secondary actor: System administrator (configuration validation), New Sensor Hardware
Channels to secondary actors: New Sensor Hardware: Wireless connectivity (802.11n). System administrator: PC-based configuration network / Internal System Bus.
Open issues:

1. How does the system handle concurrent updates to a single zone made by multiple administrators?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 21,73-74]**

**b. Delete Safety Zones**

Use case: Delete Safety Zones
Primary Actor: Administer
Goal in Context: To permanently remove an unwanted or obsolete safety zone from the system's configuration.
Precondition: The SafeHome system is operational. The zone to be deleted must not be currently armed or in an alarm state.
Trigger: The Administer determines a specific safety zone is no longer required.
Scenario:

1. The Administer logs into the system – see use case: "Log onto the system through control panel".

2. The Administer clicks the 'Configure' button on the home screen.
3. The System displays the Configuration screen, showing buttons for 'Add Safety Zone', 'Delete Safety Zone', and 'Update Safety Zone'.
4. The Administer selects the 'Delete Safety Zone' and chooses the target zone from the list.
5. The System removes the zone configuration from the database and updates the floor plan.

Exception:

4a. The selected zone is currently in an armed state: The System rejects the request and prompts the Administer to disarm the zone first.

Priority: Essential
When available: First Increment
Frequency of use: Infrequent
Channel to actor: Web browser
Secondary actor: System administrator, Selected Sensor Hardware
Channels to secondary actors: Selected Sensor Hardware: Wireless connectivity (802.11n). System administrator: PC-based configuration network / Internal System Bus.
Open issues:

1. Should the system retain a record (audit trail) of deleted zones for liability purposes?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 21,73-74]**

**c. Update Safety Zones**

Use case: Update Safety Zone
Primary Actor: Administer, Homeowner
Goal in Context: To modify the properties of an existing safety zone, allowing Administer to change core structural elements and Homeowner to change non-structural descriptive elements.
Precondition: The SafeHome system is operational. The user is logged into the system.
Trigger: A change in property layout, security policy, or a need to update descriptive information requires zone modification.
Scenario:

1. The user logs into the system – see use case: "Log onto the system". The user clicks the 'Configure' button on the home screen.
2. The System displays the Configuration screen. The user selects the 'Update Safety Zone' button and chooses the target zone from the list.
3. The System displays the zone's properties (Area, Position/Boundary, Name, Description, Core Security Parameters). If the user is the Administer, they are able

to modify all displayed properties. If the user is the Homeowner, they are restricted to modifying only the Name and Description.

4. The user saves the changes.
5. The System validates the input based on the user's role and applies the updated configuration. The System displays a confirmation message ("Zone information updated successfully").

Exception:

4a. Unauthorized Parameter Change: The Homeowner attempts to modify the zone's area, position/boundary, or core security parameters: The System rejects the save action and displays a message: "Administrative privileges required for structural changes."

4b. Boundary Overlap (Administer Only): The Administer attempts to set a new boundary that overlaps with an existing zone: The System displays an overlap error and blocks the save action.

5a. Invalid Input: Any user enters invalid data (e.g., prohibited characters in name): The System displays an error and prompts for correction.

Priority: Essential
When available: First Increment
Frequency of use: Frequent
Channel to actor: Web browser
Secondary actor: System administrator, Selected Sensor Hardware
Channels to secondary actors: Selected Sensor Hardware: Wireless connectivity (802.11n). System administrator: PC-based configuration network / Internal System Bus.
Open issues:

1. How should the system prevent and resolve concurrent updates to the same zone made by multiple Administer users?
2. Should the Homeowner be allowed to change the name if the zone is currently armed?
3. What level of audit logging is required for Administer changes versus Homeowner changes?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 21,73-74]**

**d. Add Sensors**

Use case: Add Sensors(Registration)
Primary Actor: Administer
Goal in Context: To successfully integrate new physical security sensors into the system database for eventual use by the SafeHome system.
Precondition: The SafeHome system is operational. The new sensor hardware is physically installed and ready for network pairing. The Administer is logged into the configuration system.

Trigger: New sensor hardware is installed and needs to be recognized by the software system.
Scenario:

1. The Administer logs into the system (see: "Log onto the system").
2. The Administer clicks ‘Surveillance’ button on the home screen.
3. The Administer selects the 'Add Sensors' button in the Sensor Management section.
4. The System displays the registration interface. The Administer enters the sensor's hardware ID and type (e.g., Door Sensor, Motion Detector).
5. The System initiates a wireless pairing process with the sensor and attempts to verify connectivity.
6. The System prompts the Administer to give the sensor a user-friendly reference name (e.g., "Front Door Left").
7. The System saves the sensor's details to the device registry, marks its status as 'Unassigned' to any safety zone, and logs the event.

Exception:

5a. The sensor fails to connect or the hardware ID is already registered: The System displays an error and prompts the Administer to troubleshoot or re-enter the ID.

7a. The System registry is full (storage limit reached): The System prevents registration and prompts the Administer to delete obsolete devices.

Priority: Essential
When available: First Increment
Frequency of use: Infrequent
Channel to actor: Web browser
Secondary actor: New Sensor Hardware, System administrator
Channels to secondary actors: New Sensor Hardware: Wireless connectivity (802.11n). System administrator: PC-based configuration network / Internal System Bus.
Open issues:

1. How does the system automatically determine the sensor's type and capabilities (e.g., battery level, signal strength) during the pairing process?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 63-64, 68]**

**e. Delete Sensors**

Use case: Delete Sensors
Primary Actor: Administer
Goal in Context: To permanently remove an obsolete, broken, or physically removed security sensor from the system's hardware registry.

Precondition: The SafeHome system is operational. The sensor to be deleted is disarmed (not actively being monitored). The Administer is logged into the configuration system.
Trigger: A sensor is permanently removed from the property or is irreparably broken.
Scenario:

1. The Administer logs into the system (see: "Log onto the system").
2. The Administer clicks the 'Surveillance' button on the home screen.
3. The Administer selects the 'Delete Sensors' button in the Sensor Management section.
4. The System displays a list of all currently registered sensors. The Administer selects the sensor to be deleted.
5. The System displays a final confirmation prompt, warning that the deletion is irreversible.
6. The System checks if the sensor is currently logically linked to any Safety Zone.
7. The Administer confirms the deletion.
8. The System removes the sensor's details from the registry and logs the permanent removal event.

Exception:

8a. Device Still Assigned: The selected sensor is currently logically linked to a Safety Zone: The System blocks deletion and displays an error message: "Device must be unassigned before deletion. Please update Safety Zone configuration first."

8b. Deletion Failure: Communication with the sensor fails during the deletion process: The System removes the device from the registry but flags the event as 'Deletion (Offline)' for manual inspection.

Priority: Essential
When available: First Increment
Frequency of use: Infrequent
Channel to actor: Web browser
Secondary actor: System administrator
Channels to secondary actors: System administrator
Open issues:

1. Should the system force a system reboot or security check after a sensor is deleted to ensure network integrity?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 63-64, 68]**

**f. Add Cameras**

Use case: Add Cameras(Registration)
Primary Actor: Administer

Goal in Context: To integrate a new HomeCam into the system's registry, enabling its video stream and management functions to be controlled by SafeHome.
Precondition: The SafeHome system is operational. The new camera hardware is physically installed and network-ready. The Administer is logged into the configuration system.
Trigger: New HomeCam hardware is added to the property.
Scenario:

1. The Administer logs into the system (see: "Log onto the system").
2. The Administer clicks the 'SURVEILLANCE' button on the home screen.
3. The Administer selects the 'Add Cameras' button in the Camera Management section.
4. The System prompts for the camera's network details (e.g., IP Address, Manufacturer Model, or pairing code).
5. The Administer enters the required details.
6. The System initiates communication with the camera and verifies connectivity.
7. The System prompts the Administer to give the camera a user-friendly reference name (e.g., "Living Room Cam").
8. The System saves the camera's details and capability profile to the registry and logs the event.

Exception:

6a. Communication with the camera fails (e.g., wrong IP/network error): The System displays an error and prompts the Administer to verify network settings.
8a. The camera is not supported by the SafeHome integration library: The System displays an incompatibility error and blocks registration.

Priority: Essential
When available: First Increment
Frequency of use: Infrequent
Channel to actor: Web browser
Secondary actor: New Camera Hardware, System administrator
Channels to secondary actors: New Camera Hardware: Wireless connectivity (802.11n) / Network interface. System administrator
Open issues:

1. How does the system handle different camera resolutions and frame rates from various manufacturers during registration?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 73-74]**

**g. Delete Cameras**

Use case: Delete Cameras
Primary Actor: Administer

Goal in Context: To permanently remove an obsolete, broken, or removed HomeCam from the system's registry and clear all associated configuration data.
Precondition: The SafeHome system is operational. The Administer is logged into the configuration system.
Trigger: A HomeCam is permanently removed from the property.
Scenario:

1. The Administer logs into the system (see: "Log onto the system").
2. The Administer clicks the 'Surveillance' button on the home screen.
3. The Administer selects the 'Delete Cameras' button in the Camera Management section.
4. The System displays a list of all registered cameras. The Administer selects the camera to be deleted.
5. The System displays a final confirmation prompt, warning that the camera and its associated data (e.g., viewing passwords, logical monitoring links) will be removed.
6. The System checks if the camera is currently linked to any logical monitoring task (e.g., a surveillance recording schedule).
7. The Administer confirms the deletion.
8. The System removes the camera from the registry, sends a command to the Storage Subsystem to clear associated footage, and logs the permanent removal event.

Exception:

8a. Deletion Failure: The camera fails to be cleared from the registry: The System logs the status as 'Deletion Failed' and requires the Administer to resolve the issue manually.

Priority: Essential
When available: First Increment
Frequency of use: Infrequent
Channel to actor: Web browser
Secondary actor: System administrator, Storage Subsystem
Channels to secondary actors: System administrator
Open issues:

1. How will the system verify that cloud-stored footage associated with the camera is also securely marked for deletion after the camera is removed from the local registry?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 73-74]**

**h. Manage Guest Access**

Use case: Manage Guest Access (Grant Temporary/Regular Access)
Primary Actor: Homeowner

Goal in Context: To provide flexible, controlled access to a guest by issuing a unique access code with specific permissions, optional time limits (temporary or regular access), and designated Safety Zones for arming/disarming.
Precondition: The SafeHome system is operational. The Homeowner is logged onto the system through the web application or mobile app.
Trigger: The Homeowner needs to grant access to a third party (guest, service provider, or family member).
Scenario:

1. The Homeowner logs into the system (see: "Log onto the system").
2. The Homeowner clicks the 'MANAGEMENT' button on the home screen.
3. The System displays the Management screen. The Homeowner clicks the 'Create New Guest' section and begins entering Guest details.
4. The Homeowner enters Guest details, specifies valid duration (selects either a fixed start/end date/time for temporary access, or selects 'Regular Access (No Expiration Date)').
5. The Homeowner selects the permitted Safety Zones the Guest is authorized to arm/disarm (see use case: "Arm/disarm safety zone selectively").
6. The Homeowner clicks the 'Create' button.
7. The System generates a unique access code based on the inputs, validates the permissions, saves the Guest's profile, and logs the new access permission.
8. The System displays the generated code to the Homeowner for sharing.

Exception:

1. The Homeowner attempts to select a duration that conflicts with an existing schedule or system rule: The System displays an error and prompts for adjustment.
2. The Homeowner attempts to select a Safety Zone that is permanently restricted from guest access: The System prevents selection.
3. Guest Attempts Unauthorized Access: A Guest attempts to access a zone or function for which they were not granted permission: The System denies access and logs the unauthorized attempt.

Priority: High priority
When available: First Increment
Frequency of use: Infrequent (Creation)
Channel to actor: Web browser
Secondary actor: System administrator
Channels to secondary actors: System administrator
Open issues:

1. How will the Homeowner be notified if a Guest access code is used to arm/disarm a zone?
2. Should the system allow the Homeowner to pause or temporarily revoke a Regular Access code without deleting the profile?

3. How does the system ensure the generated access code is cryptographically strong and unique?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 20]**

## 4. Remote Control use cases

### a. Remote Control of Home Lighting

Primary actor: Homeowner, Authorized Guest

Goal in context: To monitor and control the on/off status of lights in the home remotely.

Preconditions: The user must have valid credentials (user ID and passwords).
The home lighting control system is fully operational and connected via the network.
Internet connectivity is established.

Trigger: The homeowner or guest decides to access the remote control function to view or modify light status.

Scenario:

1. The user logs onto the system – see use case: “Log onto the system through web” in page 16.
2. The user selects “remote control” from the major function buttons.
3. The system displays a floor plan of the home alongside the current on/off status of each light (Figure 6 in page 10).
    a. The homeowner can control all lights shown on the floor plan.
    b. The guest can control only the lights for which explicit access permission has been granted. Lights without permission are hidden.
4. The user selects the on/off control button for a specific light on the floor plan.
5. The system changes the status of the selected light accordingly and updates the display.
6. The user can continue adjusting other lights or exit the remote control function.

Exceptions:

3a. Remote control function not configured or offline: display an error message and prompt the user to retry or seek assistance.

4a. Attempt to control a non-existent or offline light: system displays an error indicating the light cannot be controlled.

5a. Network failure during command execution: system alerts the user and rolls back to previous light status.

When available: Second increment

Frequency of use: Frequently

Channel to actor: Web browser or mobile application interface
Secondary actors: Support technician, Home lighting device controller
Channels to secondary actors:
Support technician: phone line, email
Home lighting device controller: wireless or wired network communication
Open issues:

1. How to ensure reliable command execution in varying network conditions?
2. What security measures protect against unauthorized lighting control?
3. How to gracefully handle device failures or offline statuses?
4. User experience considerations for efficient multi-light management?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 41-42]**

### b. View Air Conditioning Zone Status

Primary actor: Homeowner, Authorized Guest
Goal in context: To check the current air conditioning status including temperature, humidity, mode, timer, and set temperature for a selected zone in the home.
Preconditions: The user is logged in to the system with valid credentials (user ID and password).
The remote control system and network are fully operational.
Internet connectivity is established.
Trigger: The homeowner or guest decides to view the air conditioning status for a specific zone.
Scenario:

1. The user logs onto the system – see use case: “Log onto the system through web in page 16”.
2. The user selects “remote control” from the major function buttons.
3. The system displays the floor plan of the home, accompanied by a panel on the left showing current air conditioning status variables: temperature, humidity, mode (DRY, FAN, COOL, AI), set temperature, and timer (Schedule ON, Schedule OFF), all displayed as “-” initially (Figure 6 in page 10).
    a. The homeowner can view this status information for all zones in the house.
    b. The guest can view status information only for the zones to which they have been granted explicit access permission. Zones without permission remain hidden.
4. The user clicks on a zone on the floor plan.
5. The system updates the status panel to show real-time data for the selected zone’s air conditioning conditions.

Exceptions:

3a. Remote control system or network not configured or offline: display an error message and prompt user to retry or contact support.

4a. Selected zone does not have air conditioning control available: display an informative message indicating the unavailability.

5a. Network failure during status retrieval: notify the user and retain previous readings or default values.

When available: Second increment

Frequency of use: As needed to monitor air conditioning zones

Channel to actor: Web browser or mobile app interface

Secondary actors: Support technician, Air conditioning zone controller device

Channels to secondary actors:

Support technician: phone line, email

Zone controller device: wireless or wired network communication

Open issues:

1. How to ensure real-time and reliable data updates under variable network conditions?
2. How to secure communication between the user interface and zone controllers?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 4, 41-42]**

**c. Air Conditioning Mode Selection**

Primary actor: Homeowner, Authorized Guest

Goal in context: To select and activate a single air conditioning mode (DRY, FAN, COOL, AI) for a chosen zone. Only one mode can be activated at a time.

Preconditions:

User is logged in with valid credentials

Remote control system and air conditioning system are operational

Internet connectivity exists

Trigger: The homeowner or guest decides to change the air conditioning mode for a specific zone.

Scenario:

1. The user views the current air conditioning status for a zone – see use case: “View Air Conditioning Zone Status” in page 33.
2. The user selects one of the mode buttons: DRY, FAN, COOL, or AI.
3. The system deactivates any previously active mode.
4. The system activates the newly selected mode for the zone.
5. The system updates the UI to reflect the current active mode.

Exceptions:

2a. If multiple modes are attempted to be activated simultaneously (e.g., due to rapid user input), the system rejects additional inputs until the current mode change is processed.

3a. If the system fails to deactivate the previous mode, an error message is displayed and the operation is canceled.

4a. If the new mode activation fails due to system error or connectivity issues, display an error and revert to previous stable state.

When available: Second increment

Frequency of use: Regularly as needed for climate control

Channel to actor: Web browser or mobile app interface

Secondary actors: Support technician, Air conditioning zone controller device

Channels to secondary actors:

Support technician: phone, email

Zone controller device: wireless/wired network

Open issues:

1. How to handle concurrent mode change requests gracefully?
2. What diagnostics or feedback help users understand mode activation status?
3. How to ensure secure command transmission preventing unauthorized mode changes?
4. What is the recovery process if the air conditioner fails to respond to mode change?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 4, 41-42]**

### d. Set Air Conditioning Temperature

Primary actor: Homeowner, Authorized Guest

Goal in context: To adjust the air conditioning set temperature for a selected zone using increment (up) and decrement (down) buttons.

Preconditions:

The user is logged in with valid credentials.

Remote control and air conditioning devices are operational.

Network connectivity is active.

Trigger: The user decides to change the set temperature for a specific zone.

Scenario:

1. The user accesses the air conditioning control panel – see use case: “View Air Conditioning Zone Status” in page 33.
2. The user selects the temperature adjustment interface for the target zone.
3. The user presses the up (increase) or down (decrease) arrow button to change the temperature setting incrementally.
4. The system updates the set temperature accordingly and reflects the new value on the display.
5. The user may repeat adjustments or exit once satisfied.

Exceptions:

3a. If the temperature attempts exceed device supported limits, system restricts input and notifies the user.

4a. Network or device communication failure during adjustment: system alerts the user and retains the previous valid setting.

When available: Second increment

Frequency of use: Regularly during air conditioning operation

Channel to actor: Web browser or mobile interface

Secondary actors: Support technician, Air conditioning zone controller device

Channels to secondary actors:

Support technician: phone line, email

Zone controller device: wireless or wired communication

Open issues:

1. How to ensure synchronization between UI and zone controller for temperature consistency?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 4, 41-42]**

### e. Schedule ON for Air Conditioning

Primary actor: Homeowner, Authorized Guest

Goal in context: To schedule the air conditioning to turn on automatically after a selected delay (1 hour, 2 hours, or 3 hours). Only one schedule can be active at any time; setting a new timer overrides the previous one. Pressing the active timer button again cancels the scheduled operation.

Preconditions:

The user is logged in with valid credentials.

Remote control and air conditioning devices are operational.

Network connectivity is active.

Trigger: The user decides to set or cancel a timer to turn on the air conditioning after a delay.

Scenario:

1. The user accesses the air conditioning control panel – see use case: “View Air Conditioning Zone Status” in page 33.
2. The user selects the timer setting interface.
3. The user presses one of the timer buttons under schedule ON: 1h, 2h, or 3h.
4. If no schedule is active, the system registers the selected delay and sets the air conditioning to turn on after the delay.
5. If a schedule is already active and the user presses a different timer button, the system cancels the previous schedule and registers the new delay.
6. If the user presses the currently active timer button again, the system cancels the scheduled turn-on.

7. The system confirms the scheduled operation, update, or cancellation to the user, displaying the timer countdown or status.

Exceptions:

3a. Timer setting fails due to network or device error: display an error message and allow retry.

5a. Conflicting or overlapping timer requests: system prioritizes the latest valid request and cancels previous.

6a. Scheduled activation fails due to system issues, notify the user.

When available: Second increment

Frequency of use: Used occasionally to automate air conditioning operation

Channel to actor: Web browser or mobile app interface

Secondary actors: Support technician, Air conditioning zone controller device

Channels to secondary actors:

Support technician: phone, email

Zone controller device: wireless or wired communication

Open issues:

1. How to manage conflicting timer settings from multiple users?
2. What security measures prevent unauthorized schedule settings?
3. How to handle system recovery if timing service is interrupted or device fails?
4. How user can easily see and cancel active schedules?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 4, 41-42]**

### f. Schedule OFF for Air Conditioning

Primary actor: Homeowner, Authorized Guest

Goal in context: To schedule air conditioning to automatically turn off after a selected delay (1h, 2h, or 3h). Only one schedule can be active; setting a new timer overrides prior. Pressing the active timer button again cancels the schedule.

Preconditions:

User is logged in with valid credentials.

Remote control and air conditioning systems operate normally.

Network connection is stable.

Trigger: User selects or cancels a schedule to turn off the air conditioning after a delay.

Scenario:

1. User accesses air conditioning control panel – see use case: “View Air Conditioning Zone Status” in page 33.
2. The user selects the timer setting interface.
3. The user presses one of the timer buttons under schedule OFF: 1h, 2h, or 3h.
4. If no previous schedule exists, system sets timer starting from the current moment to turn off after selected delay.

5. If a previous schedule exists and a different button is pressed, the previous timer cancels and new timer begins from current time.
6. If user presses the currently active timer button again, the schedule cancels immediately.
7. System confirms current timer status or cancellation, showing countdown or idle indicator.

Exceptions:

3a. Timer setup fails due to system or network issues; error message shown and retry allowed.

5a. Overlapping timer requests handled by canceling older timers and prioritizing the latest user action.

6a. Failure to turn off air conditioning at scheduled time due to system faults; notify user.

When available: Second increment or later
Frequency of use: Used occasionally
Channel to actor: Web or mobile app interface
Secondary actors: Support technician, Air conditioning zone controller
Channels to secondary actors:

Support technician: phone, email
Zone controller: wireless or wired

Open issues:

1. Handling concurrent timer commands from multiple users
2. Securing timer control against unauthorized access
3. Ensuring reliable operation despite network or system failures
4. Providing clear user feedback on active or canceled schedules

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 4, 41-42]**

## 5. Surveillance Use Cases

### a. View the Thumbnail Overview

Primary actor: Homeowner, Authorized Guest
Goal in context: To view an overview of all available cameras through thumbnail images.
Preconditions: The surveillance system must be fully operational;
Internet connectivity must be established;
The user must have valid credentials (user ID and passwords).

Trigger: The homeowner (or guest) decides to view the thumbnail overview of camera grids to quickly check the status of accessible cameras.
Scenario:

1. The user logs onto the system – see use case: “Log onto the system through web” in page 16.
2. The user selects “surveillance” from the major function buttons.
3. The system displays an overview screen showing the floor plan alongside a grid of available camera thumbnail images. The floor plan indicates camera locations by their IDs (Figure 5.2 in page 9).
    a. The homeowner can view thumbnail images for all cameras installed in the system.
    b. The guest can view thumbnail images only for the cameras to which they have been granted explicit access permission. Cameras without permission are hidden or indicated as inaccessible.

Exceptions:

2a. Surveillance function or floor plan not configured: display an error message and possibly direct to configuration use cases (outside current project scope).

3a. If homeowner selects “back to home”, redirect to a main screen(Figure 2 in page 7) displaying the major function buttons.

When available: First increment
Frequency of use: Multiple times daily
Channel to actor: Web browser on PC or mobile device
Secondary actor: Support technician, Webmaster, Camera device
Channels to secondary actors:
Support technician: phone line.
Webmaster: E-mail.
Camera: wireless connectivity

Open Issues:

1. Will system response via the Internet be acceptable given the bandwidth required for camera views?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 34-36]**

### b. Specific Camera View

Primary actor: Homeowner, Authorized Guest
Goal in context: To view a specific camera for live video streaming.
Preconditions: The surveillance system must be fully operational;
Internet connectivity must be established;
The user must have valid credentials (user ID and passwords).

Trigger: The homeowner decides to monitor the house using the surveillance function.
Scenario:

1. The user view of all available cameras through thumbnail - see use case : “view the thumbnail overview” in page 38.
2. The user clicks on a thumbnail or camera icon to select a specific camera.
3. displays the live video feed of the selected camera at one frame per second(Figure 5.3 page 9).

Exceptions:

2a. If user selects “back to home”, redirect to a main screen(Figure 2 in page 7) displaying the major function buttons.

2b. If a guest selects a camera they are not authorized to access, the system displays an error message: "You do not have permission to view this camera."

3a. Camera is disabled or not functioning: display an error message; see use case “Enable/disable camera” in page 21.

When available: First increment
Frequency of use: Multiple times daily
Channel to actor: Web browser on PC or mobile device
Secondary actor: Support technician, Webmaster, Camera device
Channels to secondary actors:

Support technician: phone line.
Webmaster: E-mail.
Camera: wireless connectivity

Open Issues:

1. Will we develop a capability to provide video at a higher frames-per-second rate when high bandwidth connections are available?
2. What if a specific camera is broken?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 34-36]**

**c. Pan/Tilt/Zoom/ specific camera view**

Primary actor: Homeowner, Authorized Guest
Goal in context: To control camera functions (zoom, tilt, pan);
Preconditions: The surveillance system must be fully operational;
Internet connectivity must be established;
The user must have valid credentials (user ID and passwords).
Trigger: The homeowner wants to manipulate camera angles
Scenario:

1. The homeowner view specific camera live video - see use case : “Specific Camera View” in page 39.
2. The homeowner selects View Setting buttons on the live video viewing interface(Figure 5.3 page 9).
3. The system asks for a PIN for control authorization(Figure 5.4 page 9).
4. The homeowner enters the PIN.

5. The system validates the PIN and activates control features(Figure 5.5 page 10).
6. The homeowner uses pan, tilt, and zoom controls to adjust the camera's perspective.

Exceptions:

3a. Invalid PIN input: The system prompts the user to reenter the PIN, allowing up to three attempts; upon exceeding the limit, it locks the control access temporarily.

3b. PIN attempts exhausted: The system prevents further control access until timeout.

6a. Camera does not support control functions: Control buttons (pan, tilt, zoom) are disabled; user is informed accordingly.

When available: Second increment

Frequency of use: Used as needed during monitoring sessions

Channel to actor: Web browser or mobile application interface

Secondary actor: Support technician, Camera device

Channels to secondary actors:

Support technician: phone line

Camera device: wireless connectivity

Open issues:

1. How to ensure secure PIN transmission and authentication during control?
2. What fallback mechanisms exist for network/hardware failures?
3. How to handle cases where users forget their PIN and need to regain control access securely?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 34, 78]**

### d. Replay Recorded Video

Primary actor: Homeowner, Authorized Guest

Goal in context: To control camera functions (zoom, tilt, pan);
To view recorded video clips.

Preconditions: User is logged in and viewing a specific live camera feed.
Camera control features are enabled and configured.

Trigger: The homeowner wants to manipulate camera angles or review past video footage.

Scenario:

1. The user view specific camera live video - see use case : "Specific Camera View" in page 39.
2. The user selects "Replay" buttons on the live video viewing interface(Figure 5.3 page 9).
3. The system asks for a PIN for control authorization(Figure 5.4 page 9).
4. The user enters the PIN.
5. The system validates the PIN and activates timeline bar of recorded video(Figure 5.5 page 10).

6. The user selects a time segment on the timeline to play back recorded footage.

Exceptions:

3a. Invalid PIN input: The system prompts the user to reenter the PIN, allowing up to three attempts; upon exceeding the limit, it locks the control access temporarily.

3b. PIN attempts exhausted: The system prevents further control access until reset or timeout.

5a. Recorded video playback not supported by the camera or system: Timeline bar or playback controls are disabled; corresponding notification is shown to the user.

6a. Network or hardware failure during control or playback: System interrupts the session and displays an error message with possible recovery instructions.

When available: Second increment
Frequency of use: Used as needed during monitoring sessions
Channel to actor: Web browser or mobile application interface
Secondary actor: Support technician, Camera device, Storage device
Channels to secondary actors:

Support technician: phone line
Camera device: wireless connectivity
Storage device: wired or wireless network connection to the video management system

Open issues:

1. How to ensure secure PIN transmission and authentication during control?
2. What fallback mechanisms exist for network/hardware failures?
3. User experience improvements for smoother video playback under constrained bandwidth?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 33-34]**

### e. Camera Event Display

Primary actor: Homeowner, Authorized Guest
Goal in context: To detect motion events from cameras and alert the homeowner visually through the user interface.
Preconditions: The surveillance system must be fully operational;
Internet connectivity must be established;
The user must have valid credentials (user ID and passwords).
Trigger: Motion is detected by one or more cameras.
Scenario:

1. The homeowner or guest view of all available cameras through thumbnail - see use case : “view the thumbnail overview” in page 38.
2. A camera detects motion and sends a signal to the surveillance system in real-time.

3. The system processes the signal and determines the triggering camera(s).
4. On the thumbnail overview screen, the grid cell corresponding to the detected camera is highlighted with a red indicator at the top of the cell.
5. The homeowner or guest notices the visual alarm and can quickly identify which camera detected motion.

Exceptions:
2a. Motion detection hardware or algorithm failure causes false negative or lack of alarm; system logs error.
3a. False positive (false alarm) due to environmental factors; system filters or suppresses redundant alerts.
4a. Network or communication disruption prevents alarm signal transmission; system notifies user of connectivity issues.
5a. Failure to record or log detected events; system alerts user of potential data loss.
Secondary actor: Support technician, Camera device; Notification service
Channels to secondary actors:
Support technician: via phone or email
Camera device: wireless or wired network communication
Notification service: Internet messaging, push notifications
Open issues:

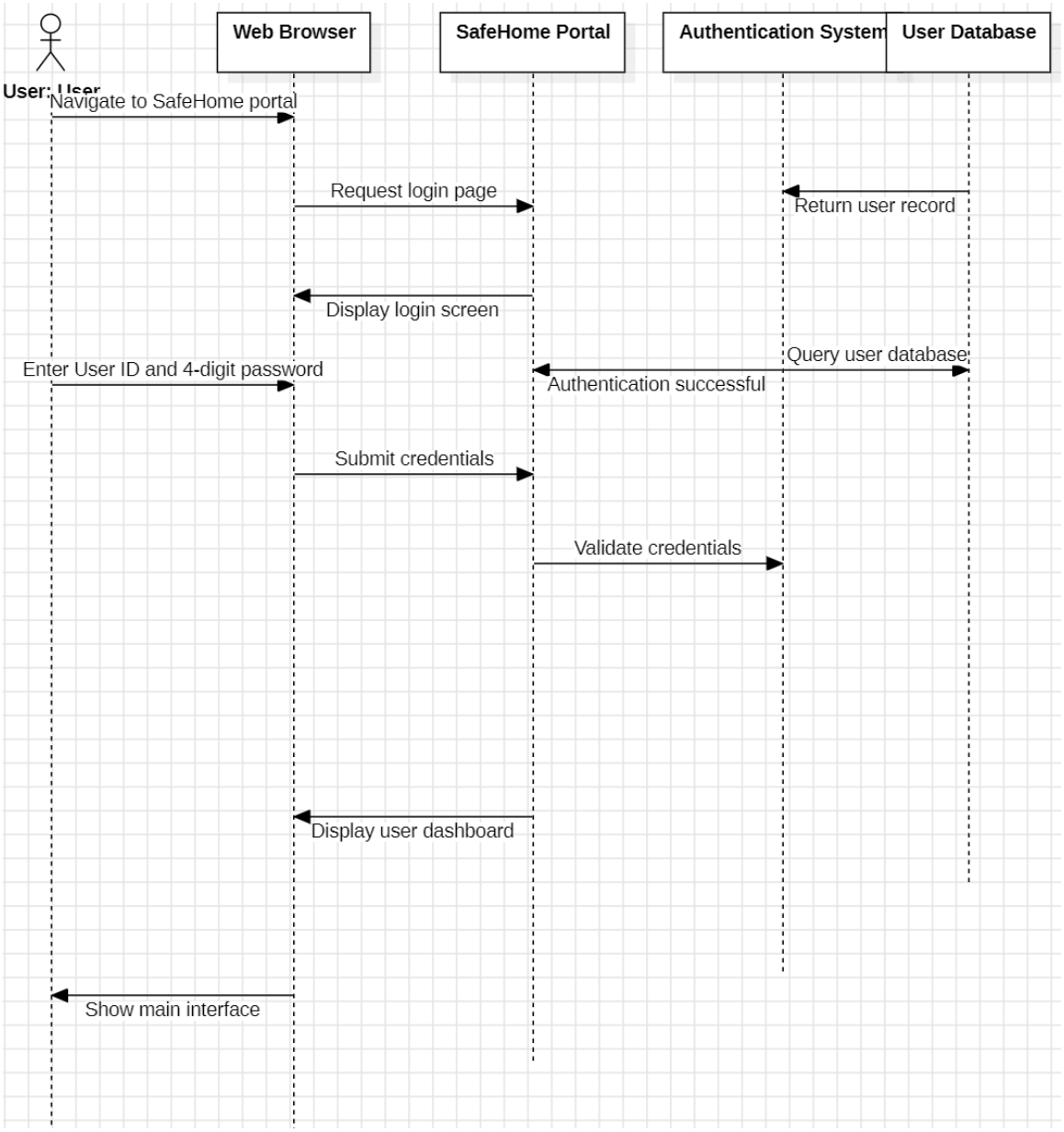
1. How to minimize false alarms while maintaining sensitivity?
2. How to ensure timely delivery of alarm notifications under varying network conditions?
3. What privacy safeguards are in place for motion-triggered alerts?
4. How to handle multiple simultaneous alarms from several cameras?

**Reference in SEPA dialog slide: [safehome_dialog.pdf pg 36]**

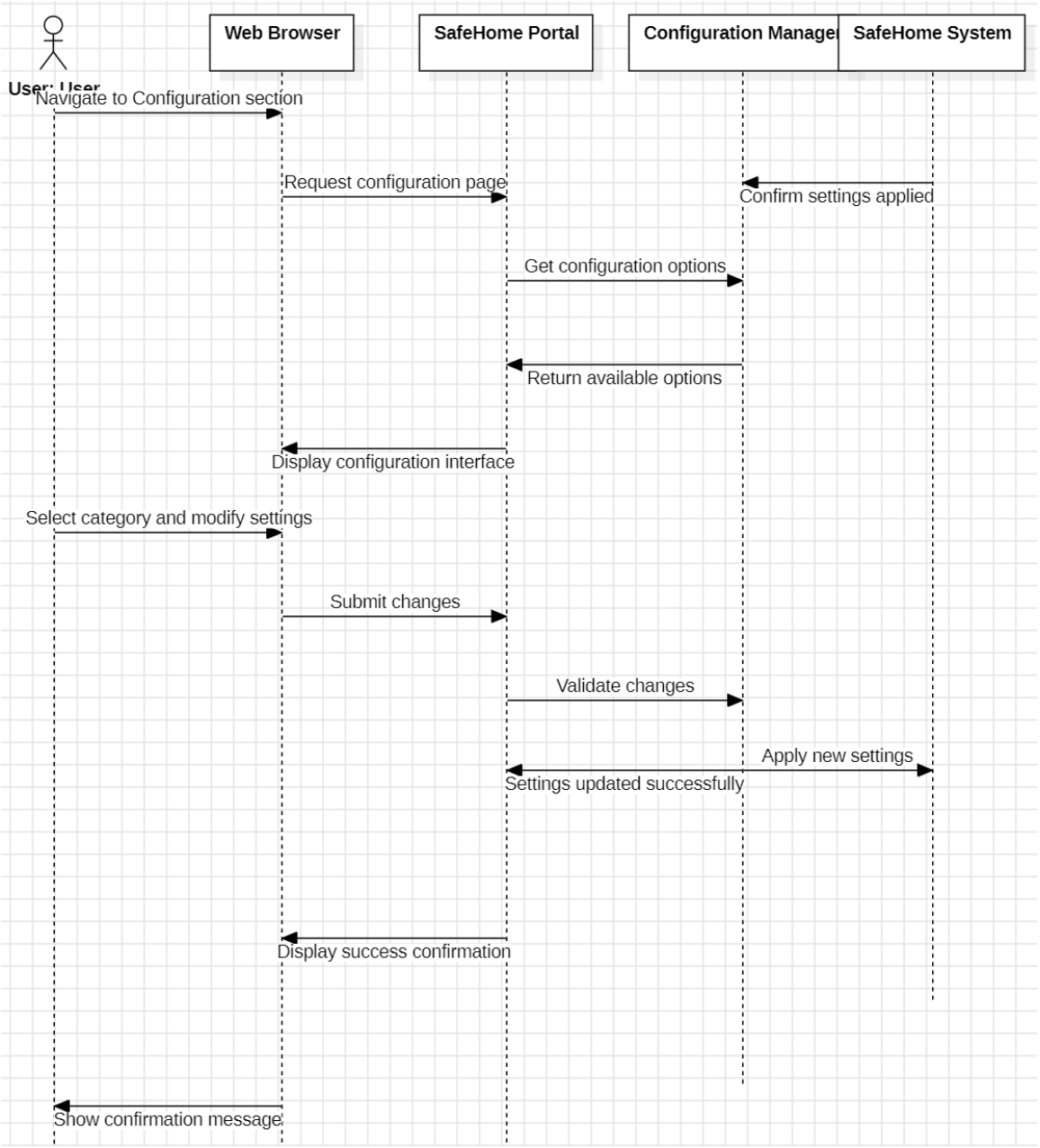
# VII. Sequence Diagram

## 1. Common Sequence Diagram

### a. Log onto the system through web

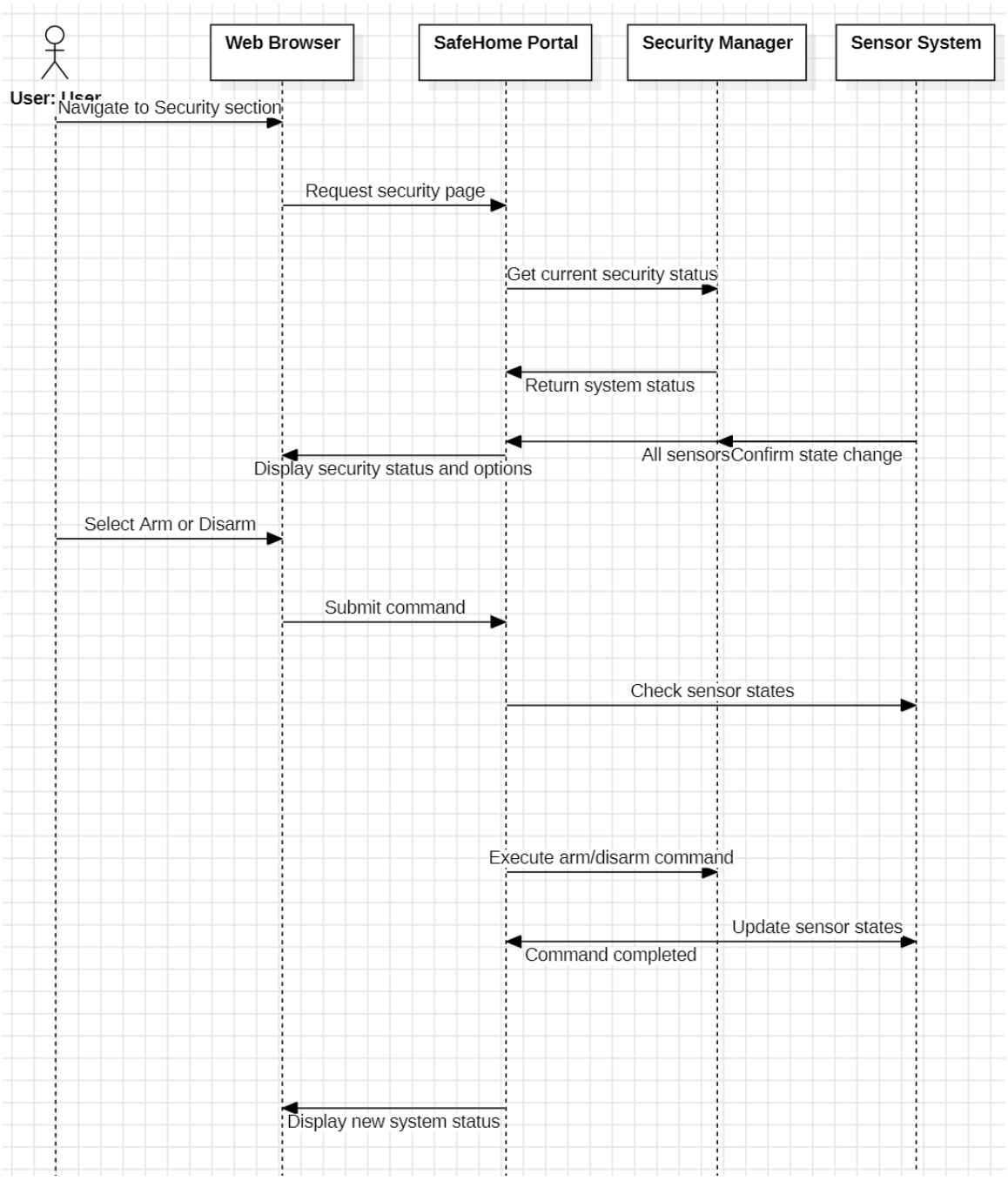


## b. Configure System Settings

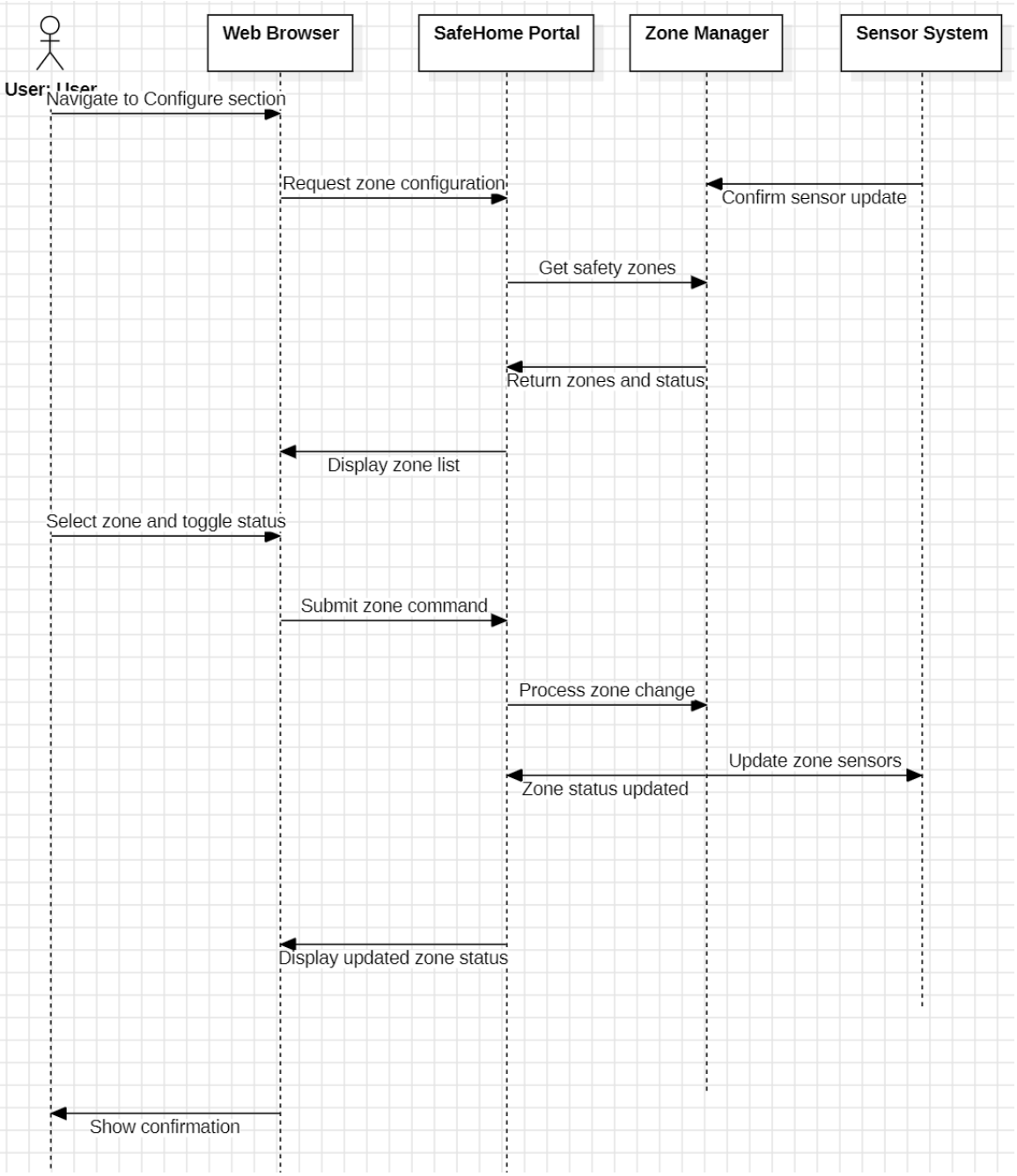


## 2. Security Use Cases

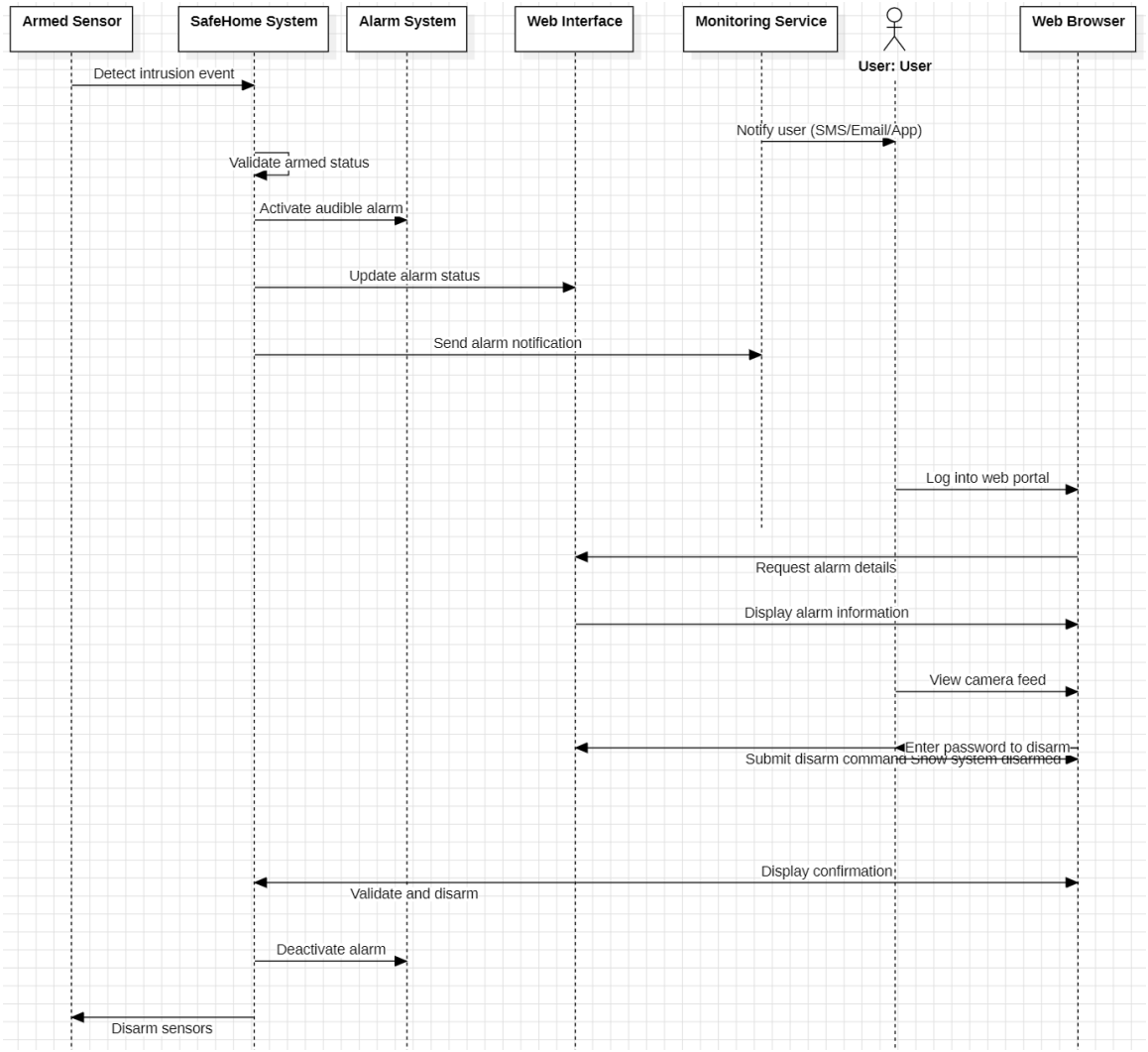
### a. Arm/disarm system through web browser



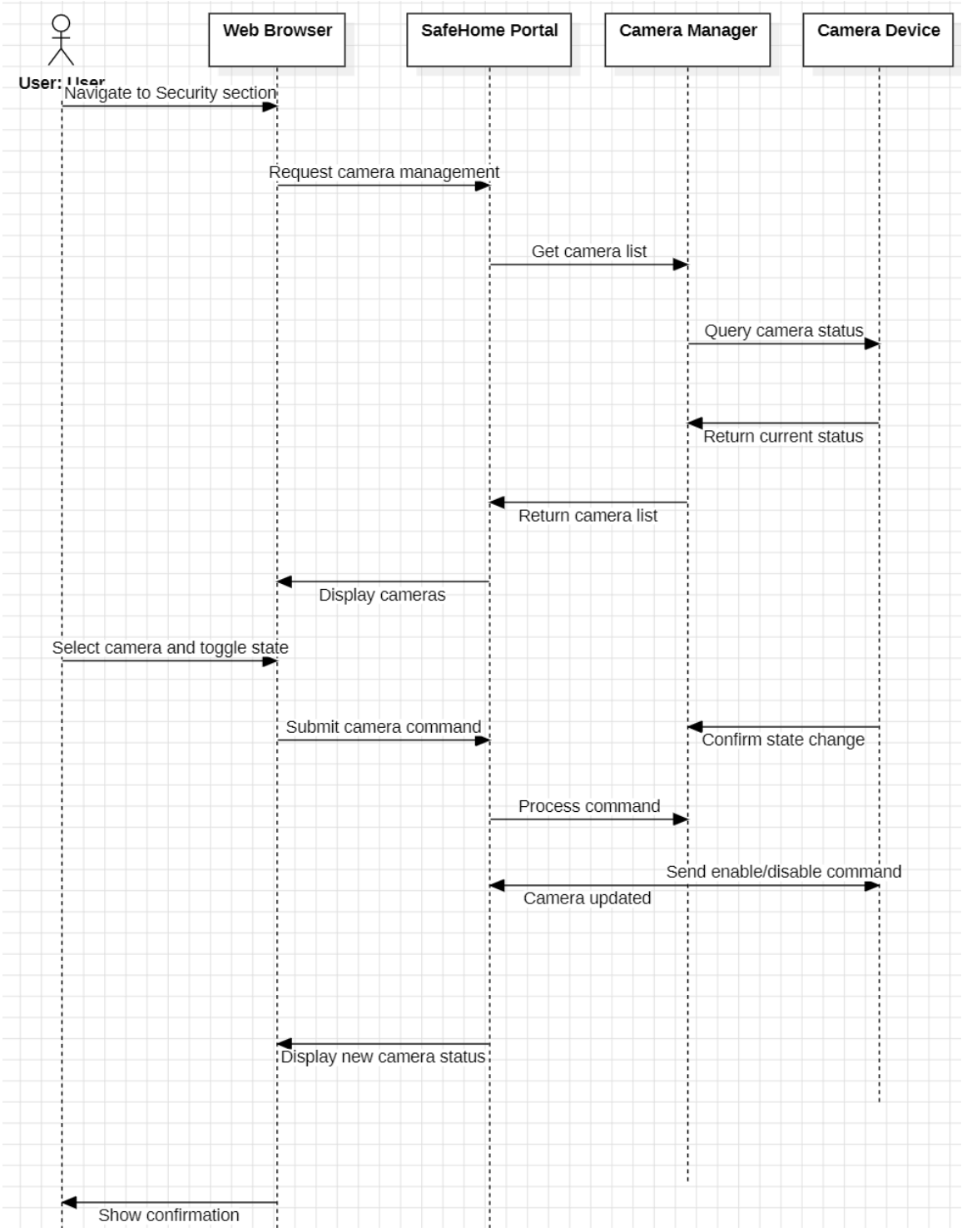
### b. Arm/disarm safety zone selectively



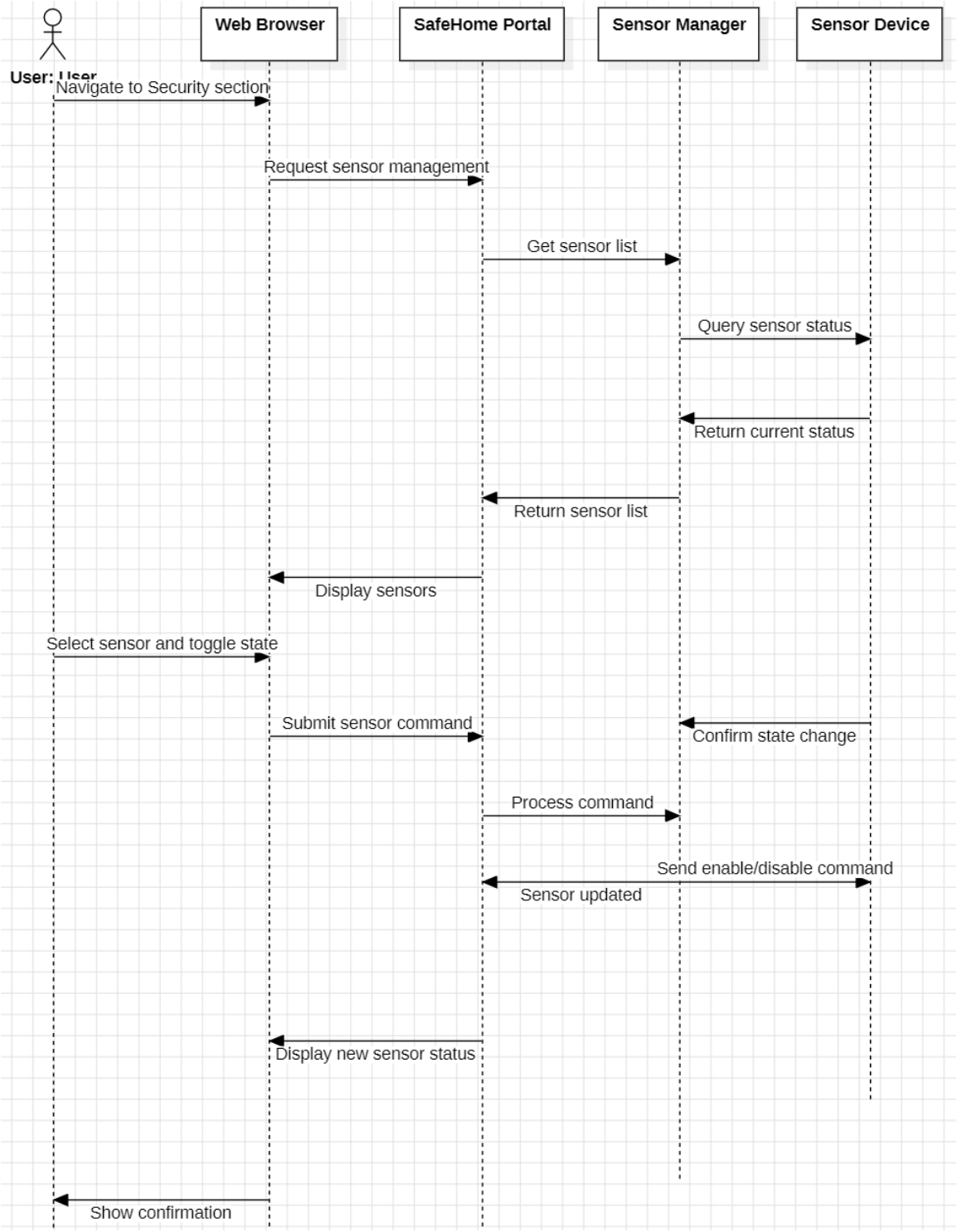
## c. Alarm condition encountered



### d. Enable/disable camera

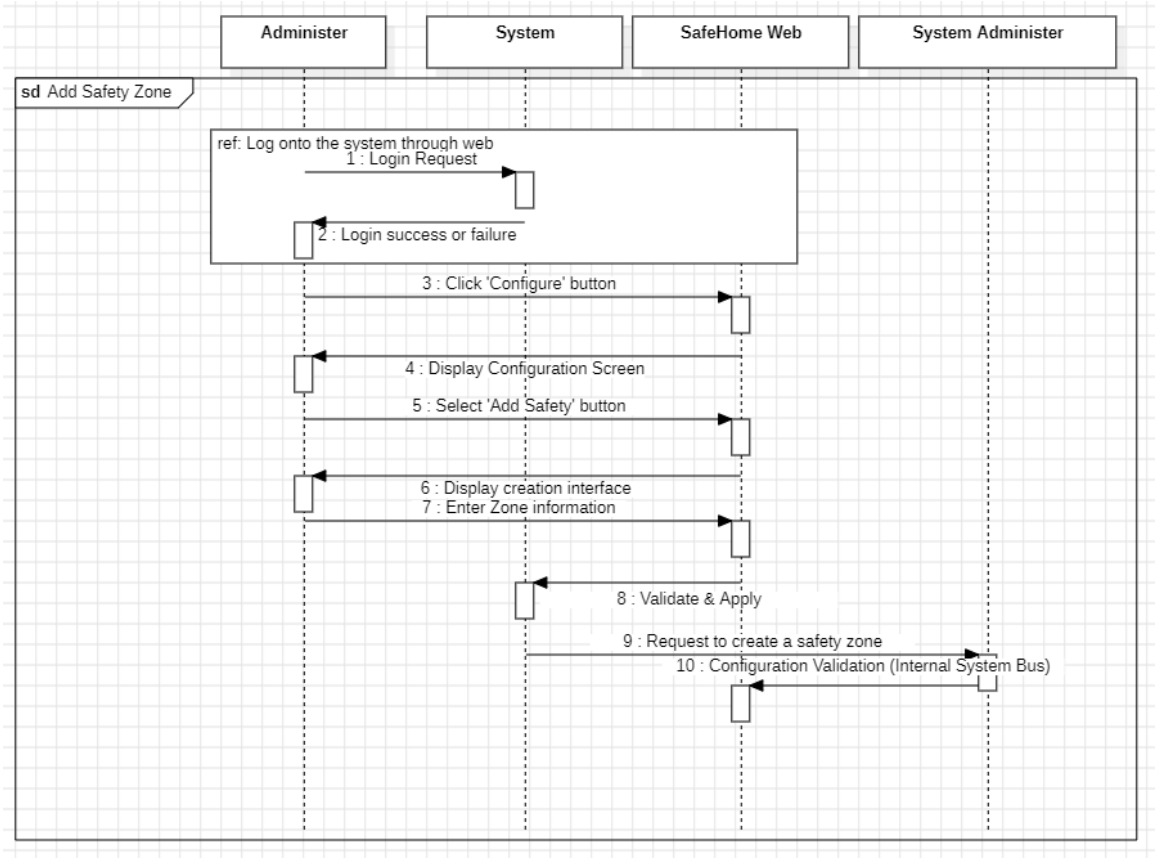


### e. Enable/disable sensor

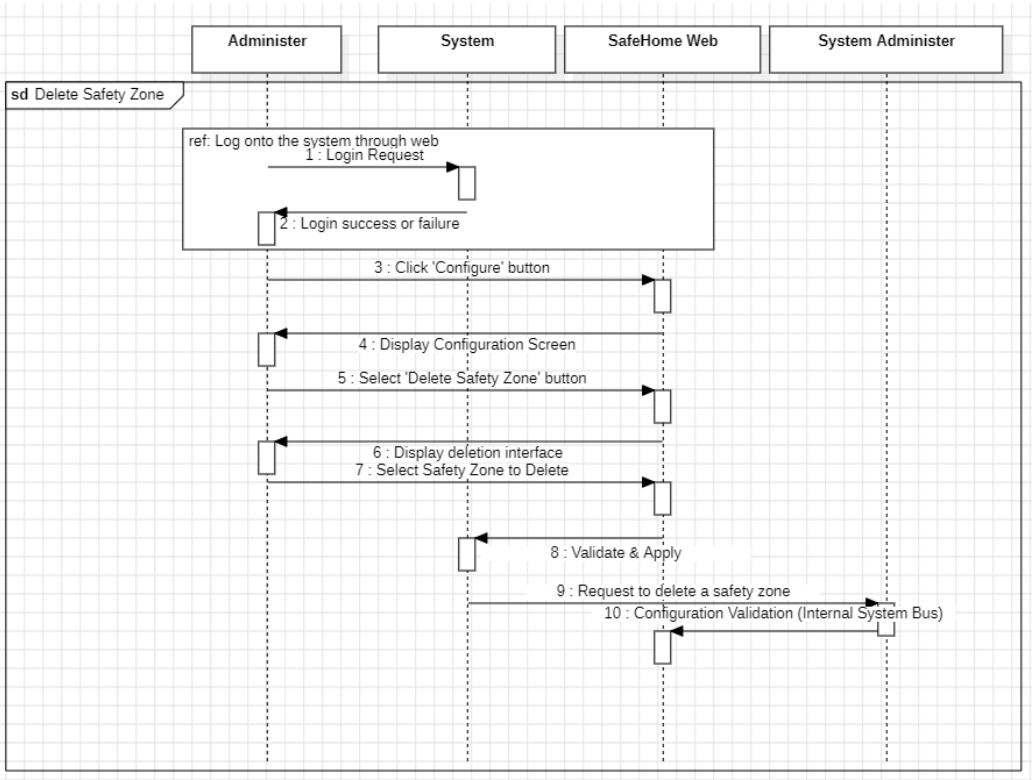


# 3. System Configuration & Manage Access

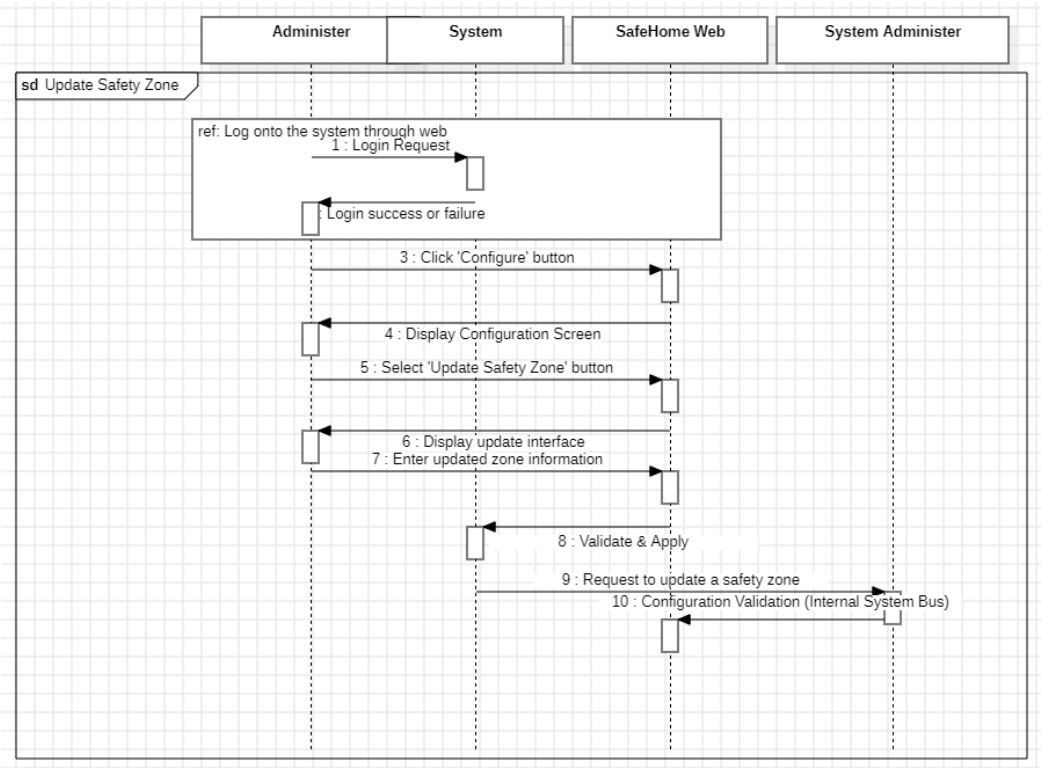
## a. Add Safety Zone



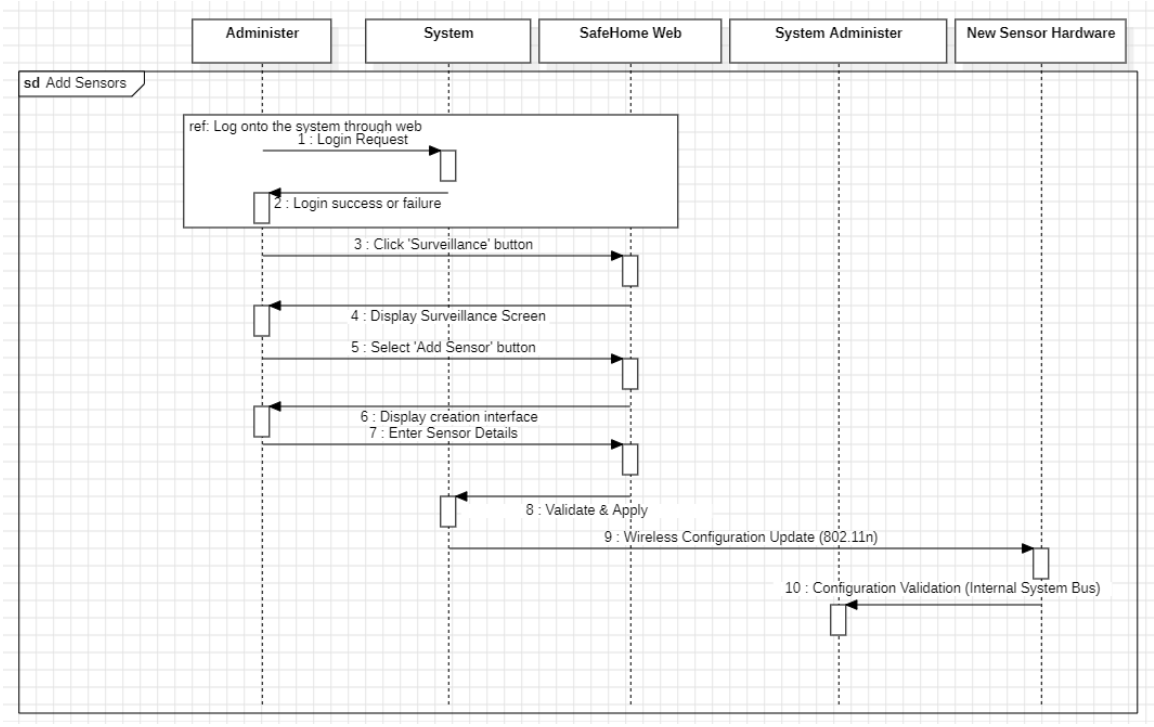
## b. Delete Safety Zone



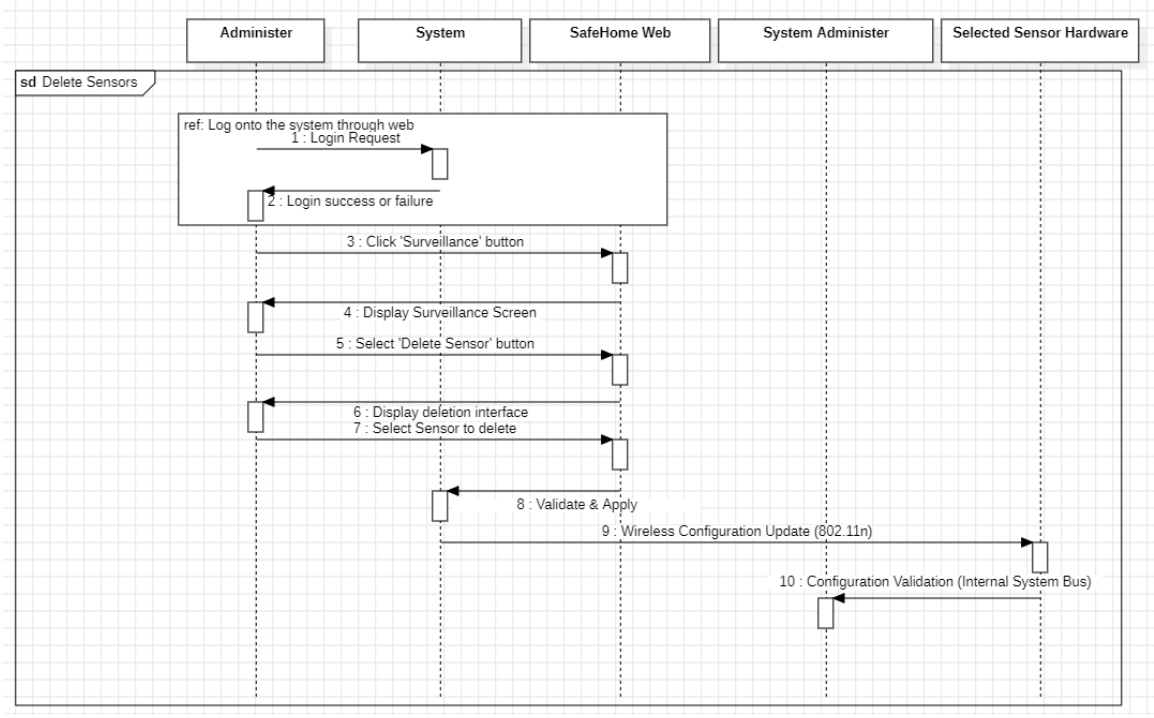

## c. Update Safety Zone



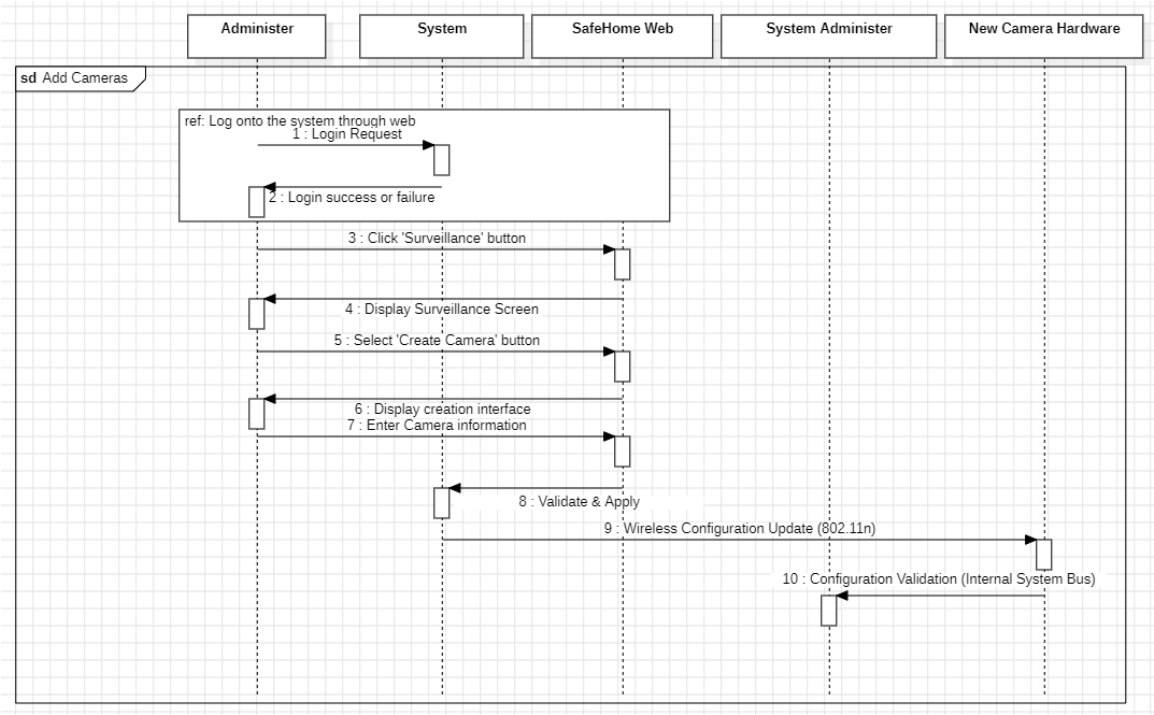
## d. Add Sensors



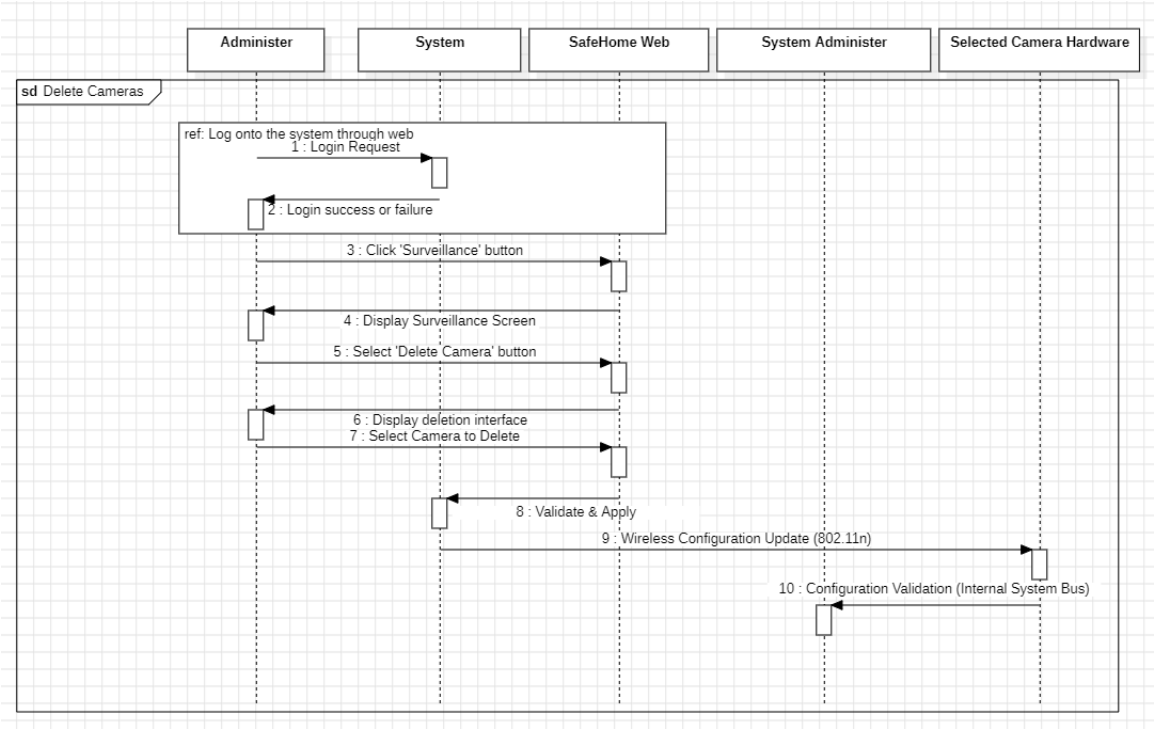

## e. Delete Sensors



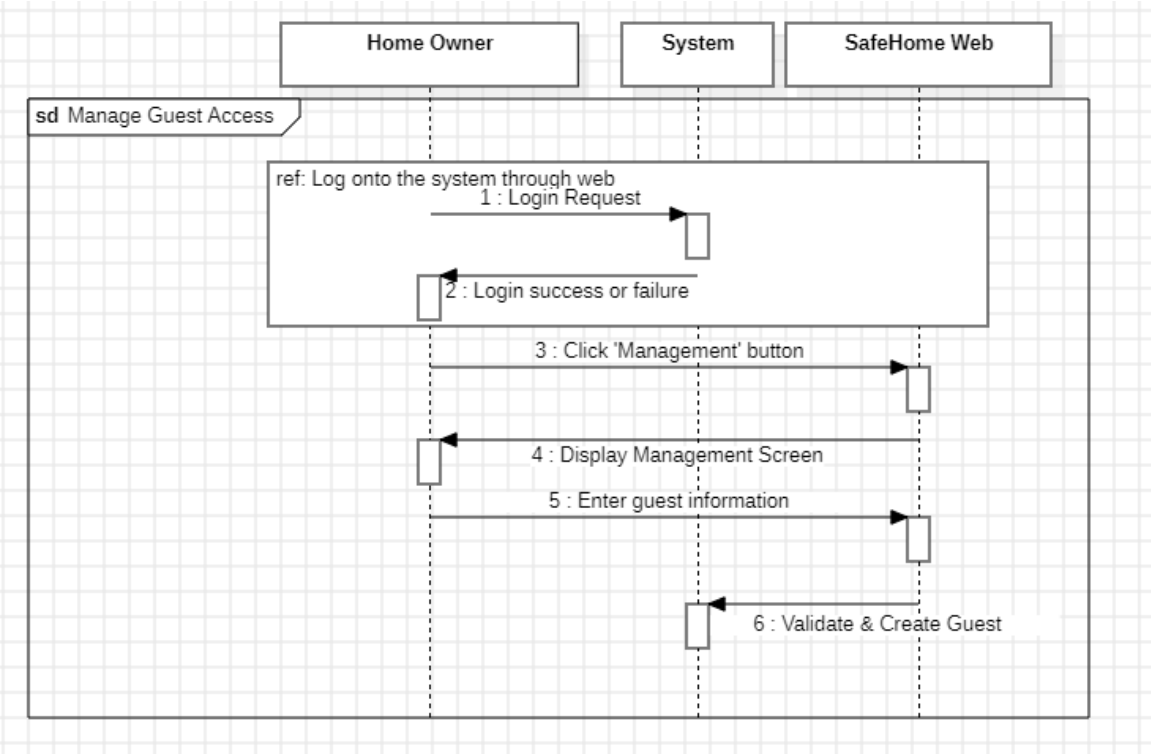
## f. Add Cameras




## g. Delete Cameras

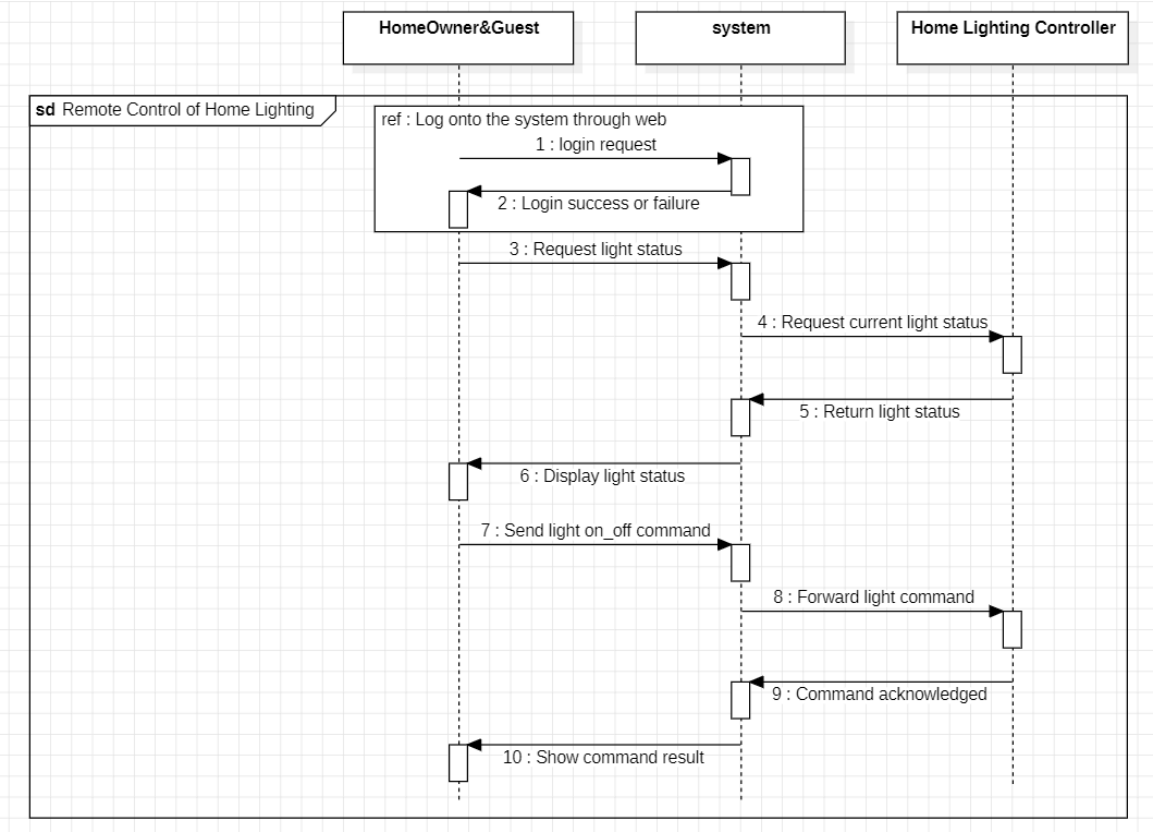


## h. Manage Guest Access

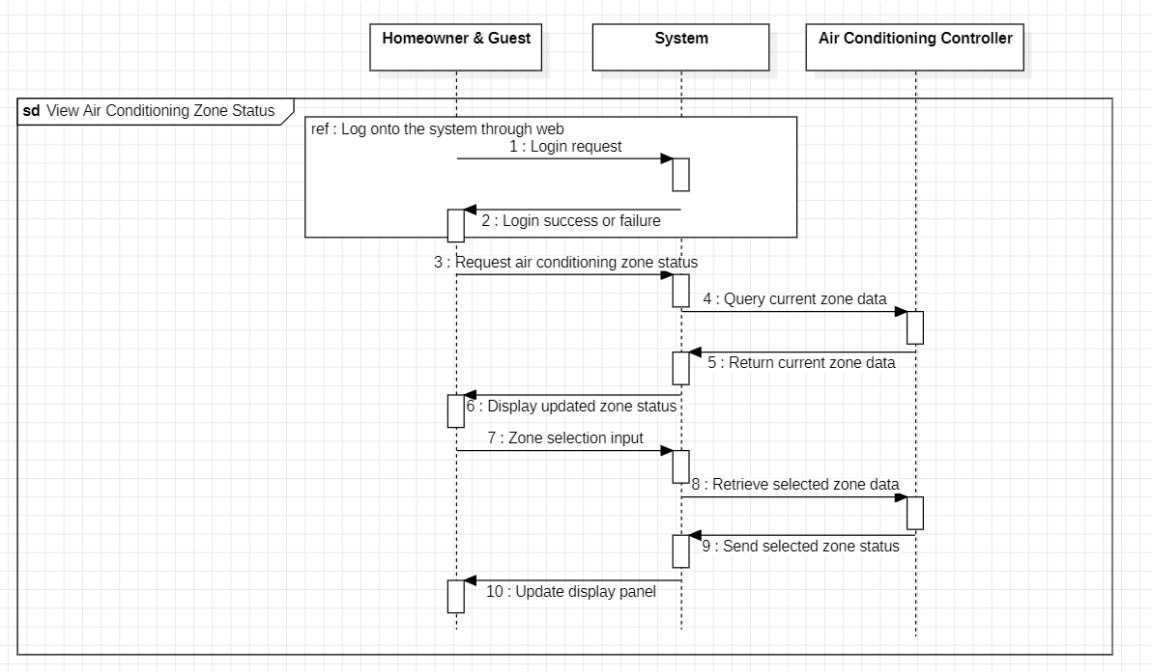


# 4. Remote Control Sequence Diagram

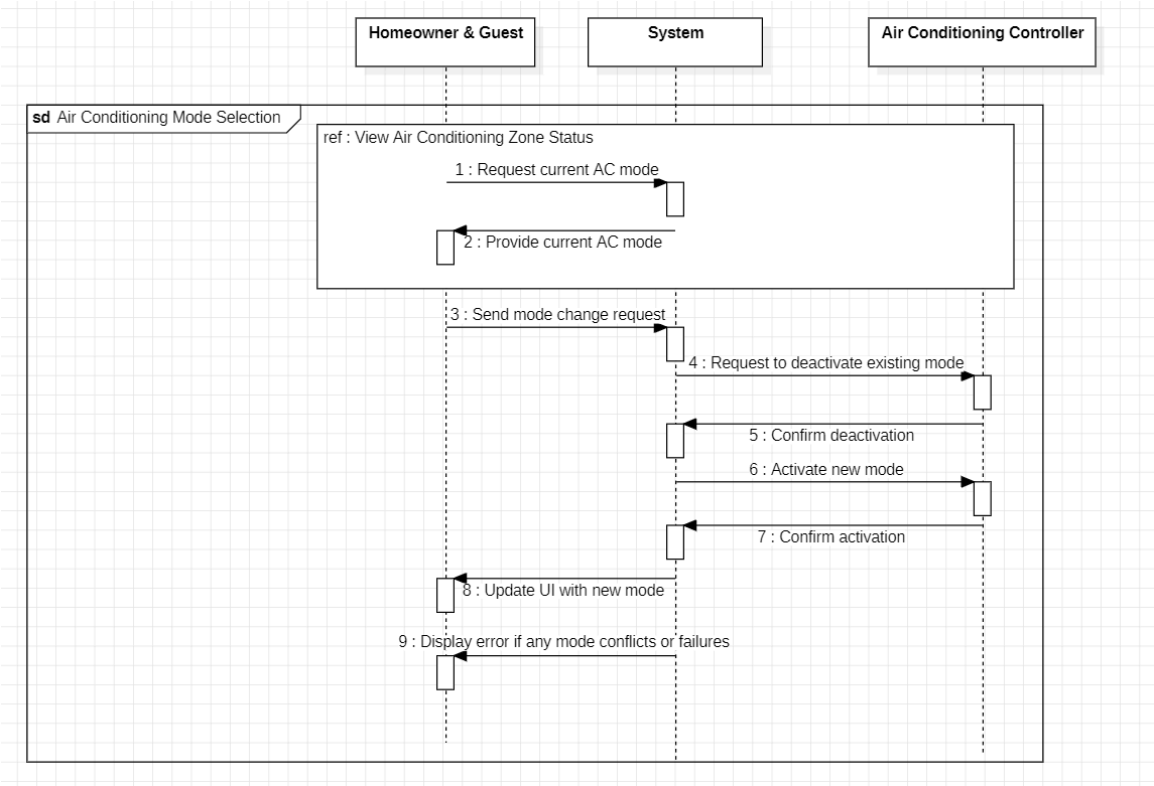
## a. Remote Control of Home Lighting



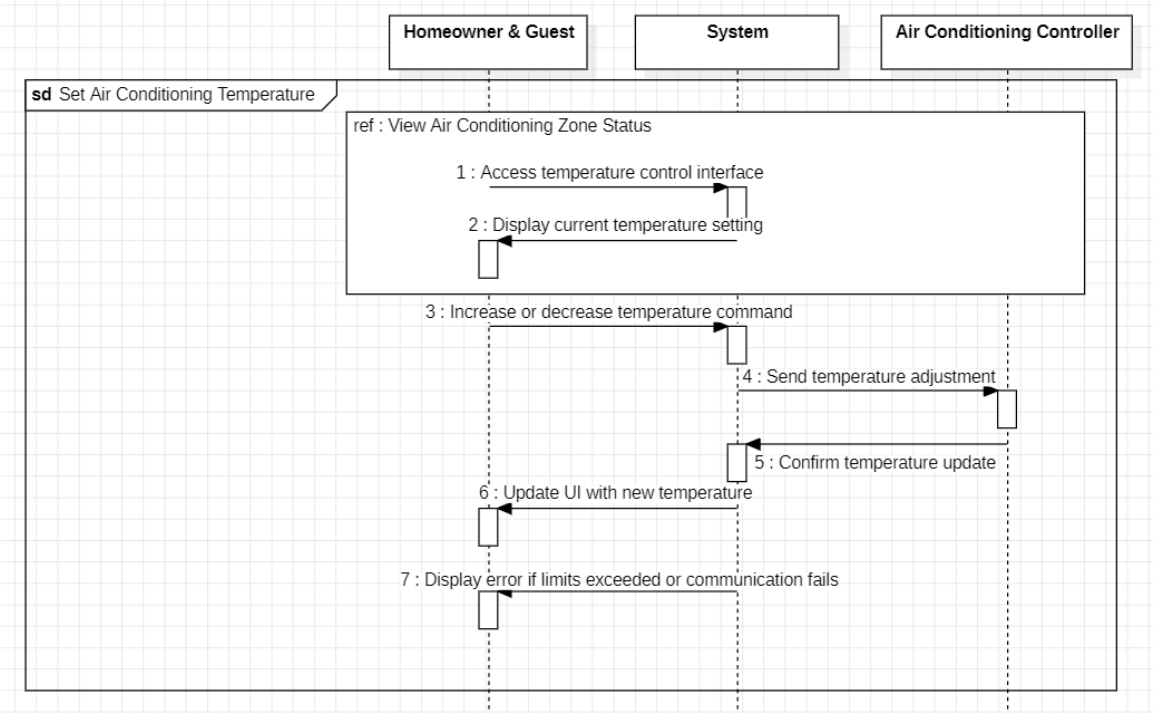

## b. View Air Conditioning Zone Status



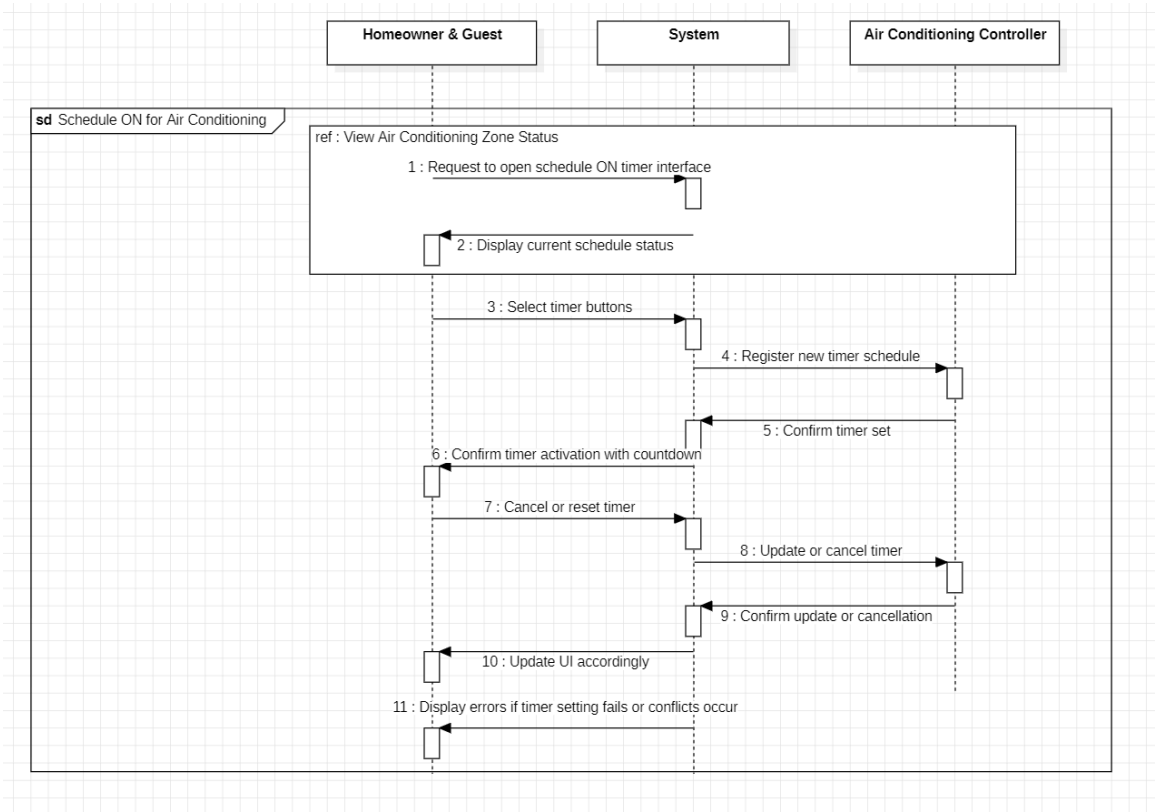
## c. Air Conditioning Mode Selection



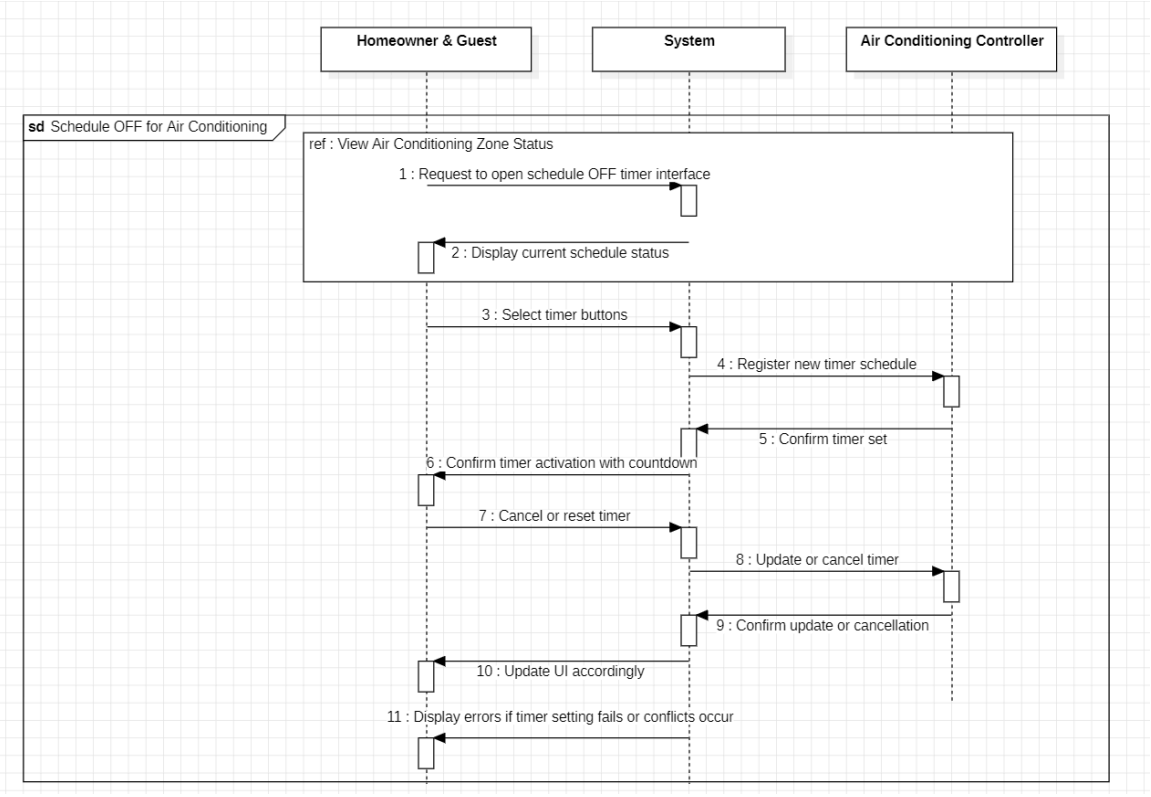

## d. Set Air Conditioning Temperature



## e. Schedule ON for Air Conditioning

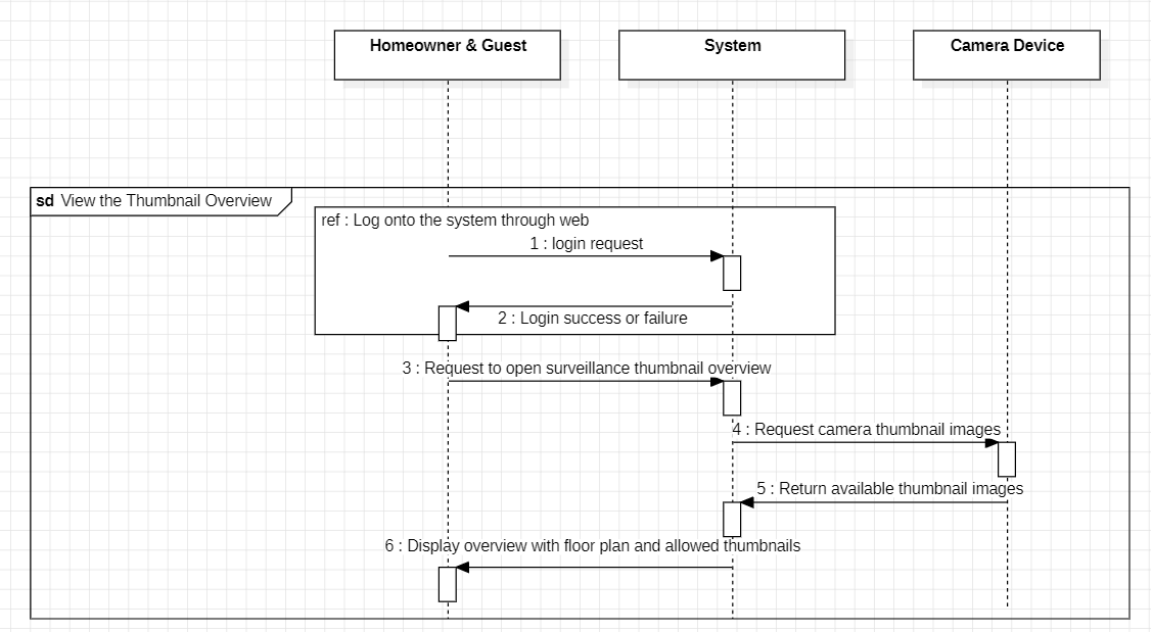



## f. Schedule OFF for Air Conditioning

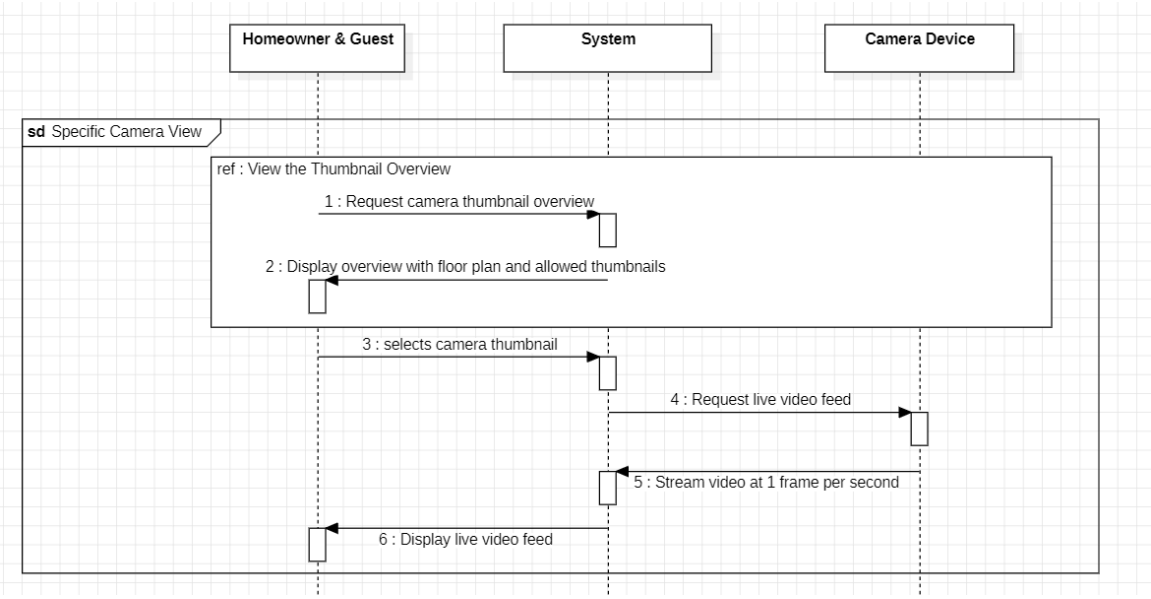


# 5. Surveillance Sequence Diagram

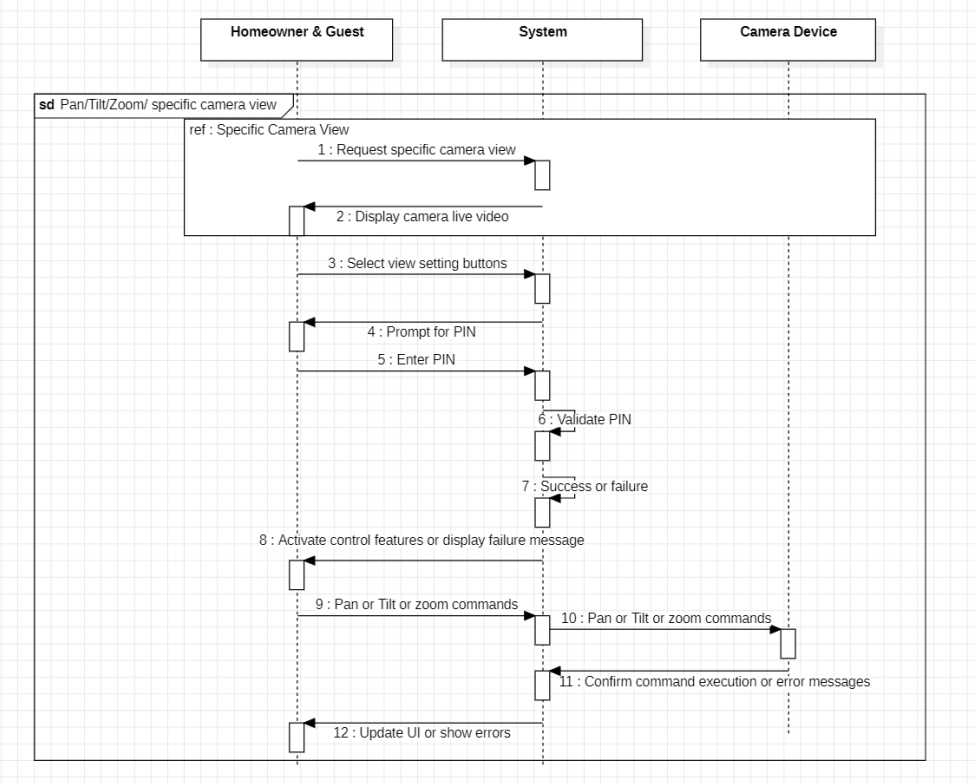
## a. View the Thumbnail Overview



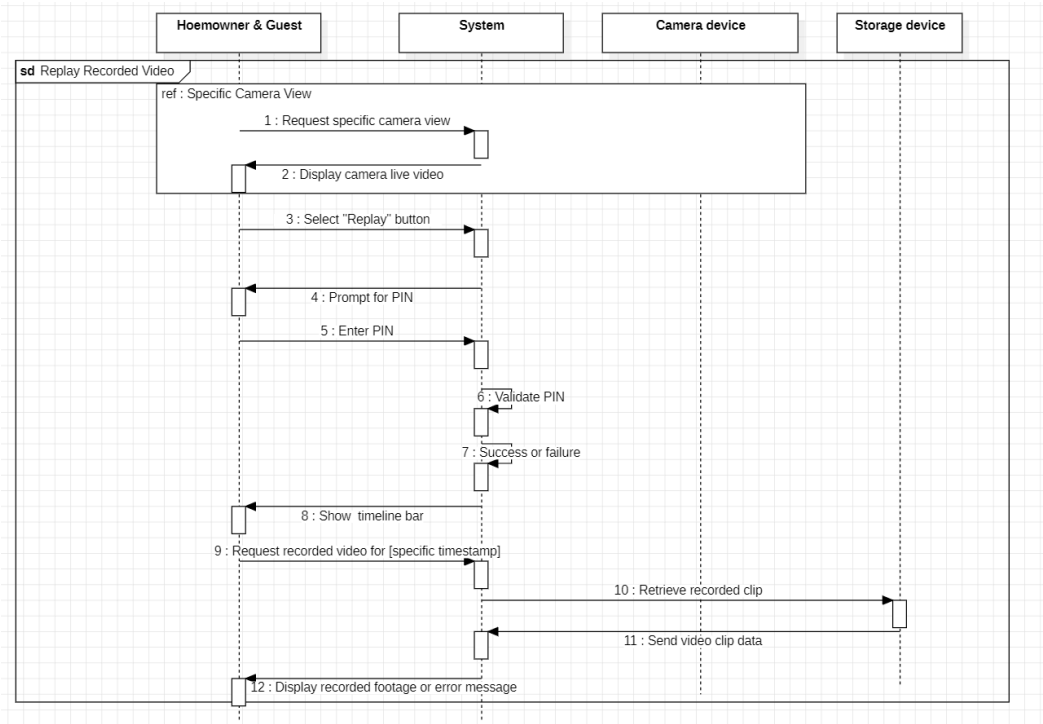

## b. Specific Camera View



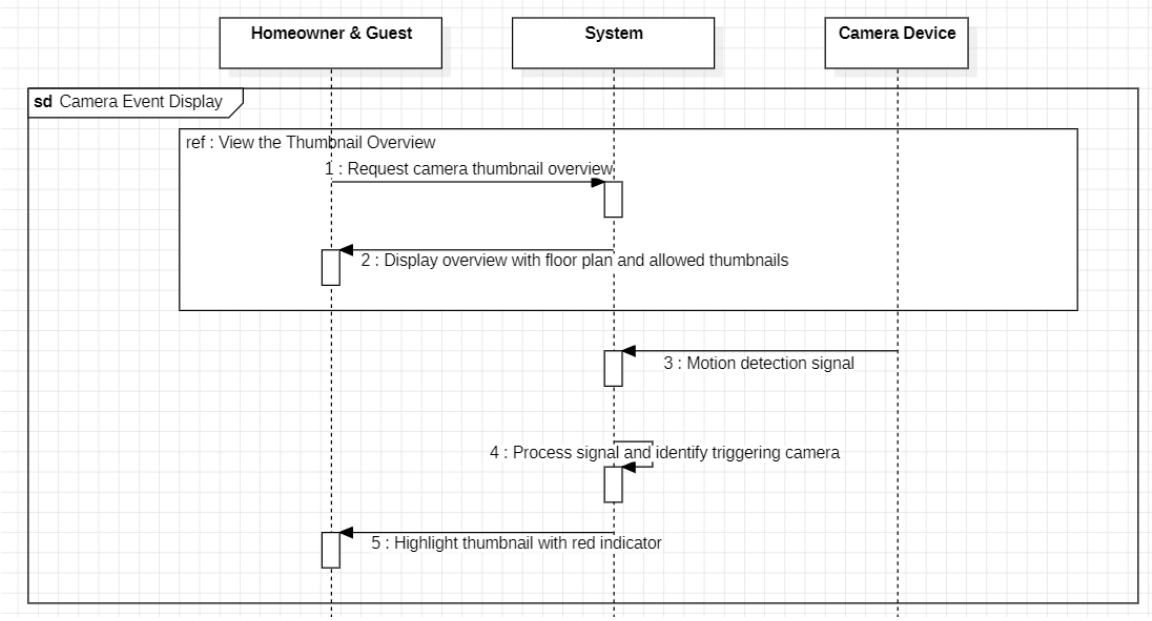
## c. Pan/Tilt/Zoom/ specific camera view




## d. Replay Recorded Video



### e. Camera Event Display




# VIII. Who did what

| Minseok Jo |
|---|
| 1. Writing Project Schedule<br>2. Use case scenario for Remote Control<br>3. Use case scenario for Surveillance Use Cases<br>4. Use case diagram for Remote Control<br>5. Use case diagram for Surveillance Use Cases<br>6. Sequence diagram for Remote Control<br>7. Sequence diagram for Surveillance Use Cases<br>8. Writing Meeting logs<br>9. Writing assumptions |
| Jonghwa An |
| 1. Writing overview<br>2. Use case scenario for Common functions<br>3. Use case scenario for Security functions<br>4. Use case diagram for Common functions<br>5. Use case diagram for Security functions<br>6. Sequence diagram for Common functions<br>7. Sequence diagram for Security functions<br>8. Finding reference from SEPA<br>9. Writing assumptions |
| Jien Lee |
| 1. Writing Prototype GUI |

2. Made figma for prototype GUI
3. Use case scenario for System Configuration & Access Management
4. Use case diagram for System Configuration & Access Management
5. Sequence diagram for System Configuration & Access Management
6. Modifying contents
7. Modifying form
8. Writing assumptions

# IX. Meeting logs

### *First Meeting (Project Direction Discussion)*

| **Date & Time** | **October 24, 2025 (Fri), 13:00 – 15:00** |
|---|---|
| Location | 교양분관 study room |
| Attendees | MInseok Jo, Jonghwa An, Jien Lee |
| Meeting Purpose | Discuss project direction, define functions, assign roles |

| **Topic** | **Details** |
|---|---|
| Project Methodology | The team discussed possible development process models, including agile approaches such as Extreme Programming (XP). While agility could promote faster iteration and adaptability, the team concluded that the limited project duration and clearly defined assignment requirements made the Waterfall model more suitable. |
| Cooperation Tools | Figma will be used to plan and visualize system functions. Documents will be shared and updated through Google Drive. The code will be shared and collaboratively managed through Git. |
| Main Functions | - System Control (startup, login, etc.) - Security Functions - Surveillance Functions - Safe Zone Configuration |
| Role Assignment | - Jien Lee: Safe Zone Configuration use case documentation<br>- Jonghwa An: Common/system-level functions and Security documentation<br>- Minseok Jo: surveillance use cases documentation |
| Next Steps | Each member will complete their assigned use case documentation before the next meeting. Refinement and diagram creation will follow after mentor feedback. |

| | |
|---|---|
| Schedule | Next Team Meeting: October, 2025 (Mon), 11:00 PM at Kyobun Study Room (Monitor available; HDMI cable prepared) |

### *Second Meeting (detail the use cases and design the overall UI)*

| Category | Details |
|---|---|
| Date & Time | October 27, 2025 (Mon), 23:00 – 1:00 (2h) |
| Attendees | Minseok Jo, Jonghwa An, Jien Lee |
| Purpose | To review diagrams, refine use cases for each system component, decide role structure (Admin, Owner, Guest), and finalize design and task distribution for upcoming submission. |
| Key Tools | Figma (UI design), StarUML (sequence diagrams), Git (code collaboration), Google Drive (document sharing), Python (function implementation). |
| Main Discussion Points | **1.** Role Definition:The team debated whether to introduce a separate Admin role or merge it with the Home Owner role. Consensus reached to include an Admin account for managing device registration, configuration, and permissions, improving system security by separating control authorities.<br>**2.** Functional Review:Members revisited major functions—Common Functions, Security, Configuration (Safe Zone), Surveillance, and a newly added Remote Control module (for temperature and light adjustments).<br>**3.** System Flow:Confirmed that system access requires login; unauthorized attempts or invalid credentials trigger security exceptions. Discussed failure scenarios (internet disconnection, sensor malfunction, invalid input) for sequence diagram inclusion.<br>**4.** User Interface Discussion:Reviewed and revised existing UI layouts. Decided that Admin, Home Owner, and Guest users will each have different screen permissions. Figma will be used to design separate screens for each role, reflecting corresponding functional access.<br>**5.** Safe Zone Function:Agreed this will handle creating, updating, and deleting security zones. Only Admins can configure them. Home Owners may toggle individual sensors within zones; Guests can temporarily deactivate sensors via limited access codes.<br>**6.** Surveillance Function:Decided to integrate both thumbnail grid and single-camera monitoring views. Added features—recording timeline playback, pan/tilt control, and password pattern authentication for specific cameras. Continuous recording will be assumed, with automatic deletion after a certain duration.<br>**7.** Remote Control Function:Introduced as the fifth feature for controlling indoor devices such as temperature and lighting. Planned simple UI with mode buttons and temperature adjustments.<br>**8.** Design and Implementation Plan:UI redesigns will include map-based visualization for camera locations. The project will remain web-based, |

| | |
|---|---|
| | consistent with the provided dialogue template. Functional code will be implemented in Python as small modules rather than full integration. |
| Decisions Made | - Separate Admin role added for configuration and permission control.<br>- Role-specific interfaces (Admin / Owner / Guest) approved.<br>- Safe Zone, Security, Surveillance, and Remote Control finalized as core modules.<br>- Continuous recording assumption added to system assumptions. - Web-based architecture confirmed (browser-accessible control panel). |
| Assignments | -Minseok Jo: Write the Overview section and organize the meeting minutes (Meeting Log).<br>-Jien Lee:Develop Figma UI for Configuration (Safe Zone), Remote Control, Surveillance and common function; finalize color theme and layout.<br>- All: Complete respective Use Case Documentation and Diagrams, Sequence Diagrams. |
| Next Steps | - Complete all use cases and sequence diagrams by the next meeting.<br>- Update shared documents on Drive by Tuesday night.<br>- Review diagrams and finalize references at the next session. |
| Next Meeting | Wednesday, October 29, 2025, 5:00 PM – In-person meeting at campus study room. |

### *3rd Meeting: System Features Finalization and UI/Use Case Refinement*

| **Category** | **Details** |
|---|---|
| Date & Time | October 29, 2025 (Wednesday), 5:00 PM – 8:00 PM (3h) |
| Attendees | Minseok Jo, Jonghwa An, Jien Lee |
| Meeting Purpose | Discuss final details on surveillance system features, UI consistency, role-based access differentiation, use cases refinement, and finalize assignments for upcoming deliverables. |
| Key Discussion Points | - Decision to exclude camera-specific passwords due to complexity.<br>- Recording storage to be managed by system/server, with configurable retention period.<br>- Activation and deactivation controls remain under security management.<br>- Role-based UI variations: Home Owner, Admin, Guest roles clearly differentiated.<br>- Control Panel reconsidered; agreed to treat it as web-based tablet interface for simplicity.<br>- Guest accounts created and managed solely by Home Owners with customizable access duration.<br>- Safe Zones managed primarily by Admin with limited Home Owner modification rights. |

| | |
|---|---|
| | - Exception handling to be added for unauthorized access attempts.<br>- Use cases will specifically delineate access and UI flow differences between Home Owner and Authorized Guest.<br>- UI items and control elements standardized, minor additions to support remote control (lights, AC).<br>- Sequence diagrams and updated Figma UI due by next meeting.<br>- Final referencing and documentation to be completed before submission deadline. |
| Decisions Made | - Camera password feature removed.<br>- Recording backup and retention managed by server.<br>- Control Panel functionality integrated into web UI.<br>- Guest roles defined as Authorized Guest with restricted access strictly controlled by Home Owner.<br>- Exception scenarios clearly documented.<br>- UI to support clear role-based permission presentation.<br>- Roles include Admin, Home Owner, and Authorized Guest with distinct function boundaries.<br>- Remote Control functionality focused on temperature, lighting adjustments. |
| Assignments | -Minseok Jo:Complete Overview and meeting log; finalize remote control use cases and diagrams. -Member 2:Finalize UI designs in Figma, complete configuration and guest access sections. -Member 3:Wrap up surveillance use cases and sequence diagrams, update Team Log. -All members:Submit completed diagrams, documents, and UI updates before next meeting. |
| Next Meeting | Thursday, October 30, 2025, 6:30 PM (tentative) for final review and submission preparation. |

### *4th Meeting: Progress Update & Diagram Strategy Discussion*

| **Category** | **Details** |
|---|---|
| Date & Time | October 30, 2025 (Thursday), 6:00 PM – 8:00 PM (2h) |
| Attendees | Minseok Jo, Jonghwa An, Jien Lee |
| Purpose | Share progress on system features, discuss diagram drawing techniques, tool usage (StarUML, Figma), and assign tasks for completing sequence and use case diagrams. |

| | |
|---|---|
| Discussion Highlights | - Progress shared: The team reported ongoing work on Safe Zone, Security, and Remote Control functions, with some diagrams and documents still in progress.<br>- Diagram Creation: Decided to use StarUML for sequence diagrams, and for ease, split diagrams by actor roles (Home Owner, Admin).<br>- Diagram style: Discussed standardization for sequence diagrams' structure and visual clarity, especially for onboarding new team members.<br>- Tool Sharing: Team members shared how they used StarUML and Figma, with promises to finalize and upload diagrams before the next meeting.<br>- Use case diagrams: Agreed to choose a simplified, consistent tool, possibly switching to Figma or another visual tool for clarity.<br>- Overall, emphasized the importance of clear documentation, role delineation, and consistent formatting for diagrams and documents. |
| Decisions Made | - Use StarUML for sequence diagrams, split by roles to simplify understanding.<br>- Finalize diagrams, documents, and UI mockups by next meeting.<br>- Confirm role-based UI differences in the documentation. |
| Task Assignments | -Minseok Jo:Complete and review sequence diagrams, update meeting logs, assist with role-specific use cases.<br>-Jien Lee:Finalize Figma UI, document role distinctions, prepare diagrams for upload.<br>-Jonghwa An:Draw detailed sequence diagrams, help with diagram formatting, update team logs.<br>-All:Review and prepare diagrams/documents for the upcoming deadline. |
| Next Meeting | October 31, 2025 (Friday) 2 PM, time to be confirmed for final review and submission preparation. |

### *5th Meeting: Assumptions Finalization and Diagram Progress Update*

| **Category** | **Details** |
|---|---|
| Date & Time | October 31, 2025 (Friday), 2:00 PM – 4:00 PM (2h) |
| Attendees | Minseok Jo, Jonghwa An, Jien Lee |
| Meeting Purpose | Finalize assumptions document, share progress on surveillance and remote control features, discuss diagram completion and layout, and prepare referencing and document structure before submission. |

| | |
|---|---|
| Discussion Highlights | - Prioritized completing the assumptions section to avoid reference page overflow.<br>- Decided to record system-uploaded videos in units (considering 1 min or 1 hour as upload intervals).<br>- Recorded all references; small additions to control panel assumptions made.<br>- Discussed ambiguity points using GPT assistance for clarity.<br>- Surveillance feature updates include pan, tilt, zoom, and video playback additions.<br>- Emphasized unifying password policy (4-digit default) and using web-based control panels.<br>- Roles and permissions refined: Home Owner controls guest accounts, Admin handles configuration.<br>- Alarm and alert systems discussed, proposing popup notifications for triggered events.<br>- Data logs to be stored on server, accessible for review.<br>- Reviewed page numbering strategy to stabilize document layout.<br>- Minor content cleanup: removing unused sensor testing data and unrelated selling page sections.<br>- Exception handling refined for concurrent commands and failed authentication delays.<br>- Next steps: finish assumptions section, finalize diagrams, update UI designs and references.<br>- Expressed intent to complete all remaining tasks before next day's deadline. |
| Decisions Made | - Assumptions to reflect system-controlled video upload and deletion.<br>- Remote control functions to continue including temperature and lighting management.<br>- Password and security controls standardized across user roles.<br>- Control Panel described as web interface with internet access. |
| Task Assignments | -Minseok Jo:Draft and finalize assumptions document, oversee remote control use cases and diagrams, assist with overall document referencing.<br>-Jien Lee:Complete Figma UI updates, manage document page numbering and referencing.<br>-Jonghwa An:Finalize sequence diagrams, update team logs, assist with alarm and alert documentation.<br>-All Members:Submit completed sections, diagrams, and references |