Software Requirement Specification (SRS)

I. Table of Contents

II. Project Schedule

Beginning of the project	Oct 20, 2025
Writing requirement specification for the Safehome product	Oct 20 - Oct 31, 2025
Writing design specification for the Safehome product	Nov 1 - Nov 14, 2025
Implementing and testing Safehome implementation	Nov 15 - Dec 1, 2025
Testing the Safehome implementations of the other teams	Dec 2 - Dec 8, 2025
Final Safehome project submission	Dec 9 - Dec 20, 2025

Aa ID	Name of Process	Begins	Ends	Σ Working Period
1	Writing requirement specification for the Safehome product	@2025년 10월 20일	@2025년 10월 31일	11d
2	Writing design specification for the Safehome product	@2025년 11월 1일	@2025년 11월 14일	13d
3	Implementing and testing Safehome implementation	@2025년 11월 15일	@2025년 12월 1일	16d
4	Testing the Safehome implementations of the other teams	@2025년 12월 2일	@2025년 12월 8일	6d
5	Final Safehome project submission	@2025년 12월 9일	@2025년 12월 20일	11d

III. Prototype GUI

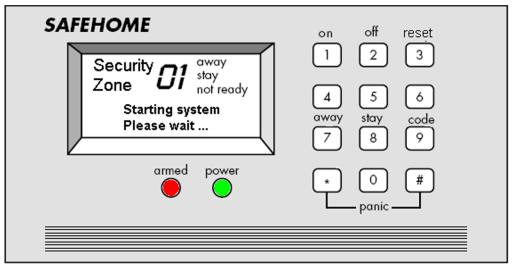


Fig 1. Control Panel

: The above signals will be referred to as the ARM indicator
and the Power indicator from now on.

Fig 2. Login Screen

Fig 3. MainFunctions

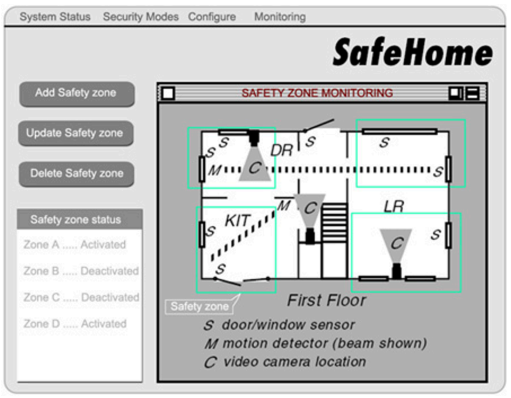


Fig. 4 Security Function – Safety zone

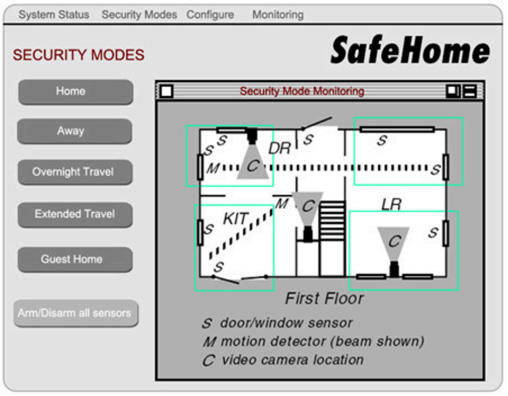


Fig. 5 Security Function – Security Mode

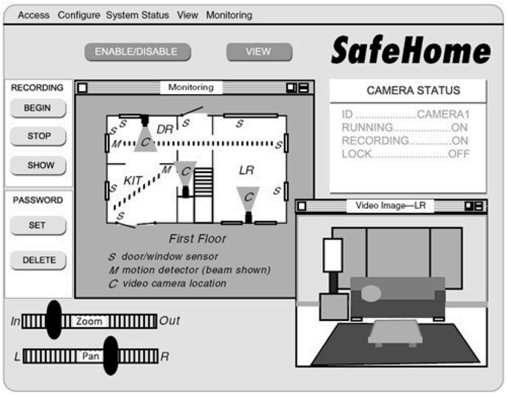


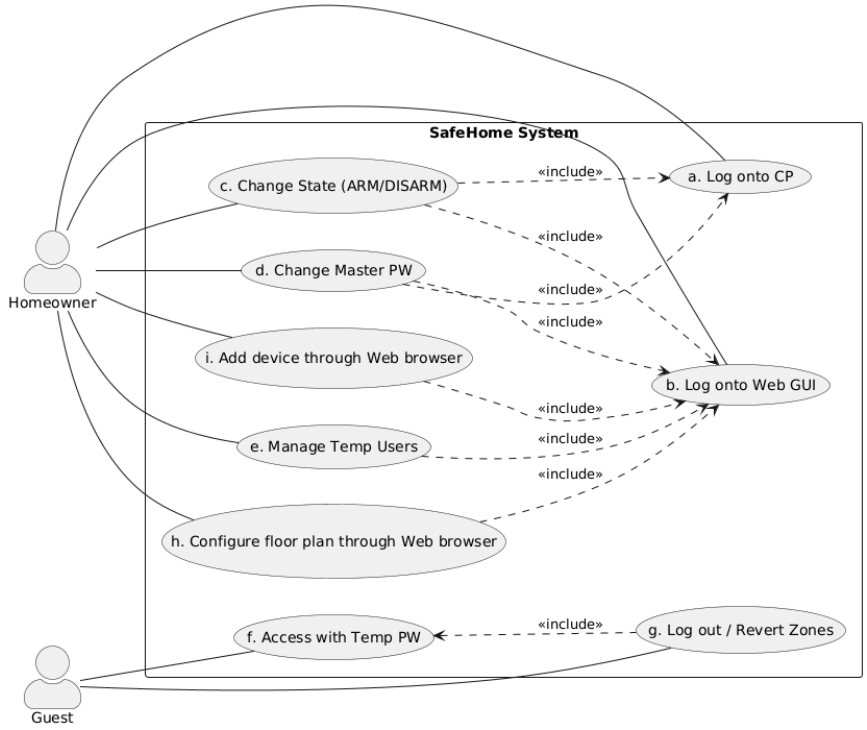
Fig. 6 Surveillance Function

IV. Assumptions

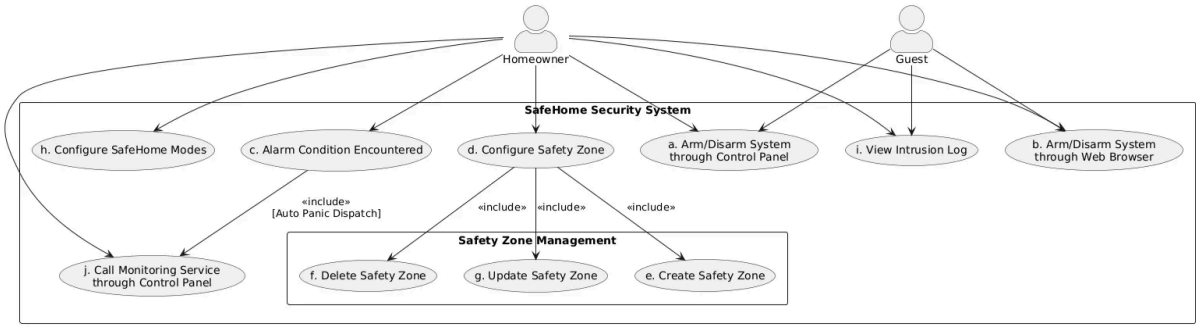
1. The Control Panel and System is provided with stable power, audio equipment, and both wired and wireless internet connections.
2. Within a single household, devices can connect to the same network via the wireless internet connection.
3. In the planning phase, actors are represented as System, Control Panel, Web Browser, Sensor, Camera, and Home Appliance, abstracting the detailed implementation of servers and hardware.
4. Internet may be used for functions such as user authentication and emergency contact to the monitoring center.
5. Physical reset disallowed; PC authentication required for recovery.
6. In the VII. Sequence Diagram part, boxes are used to handle branches or exception cases.

V. Use Case Diagrams

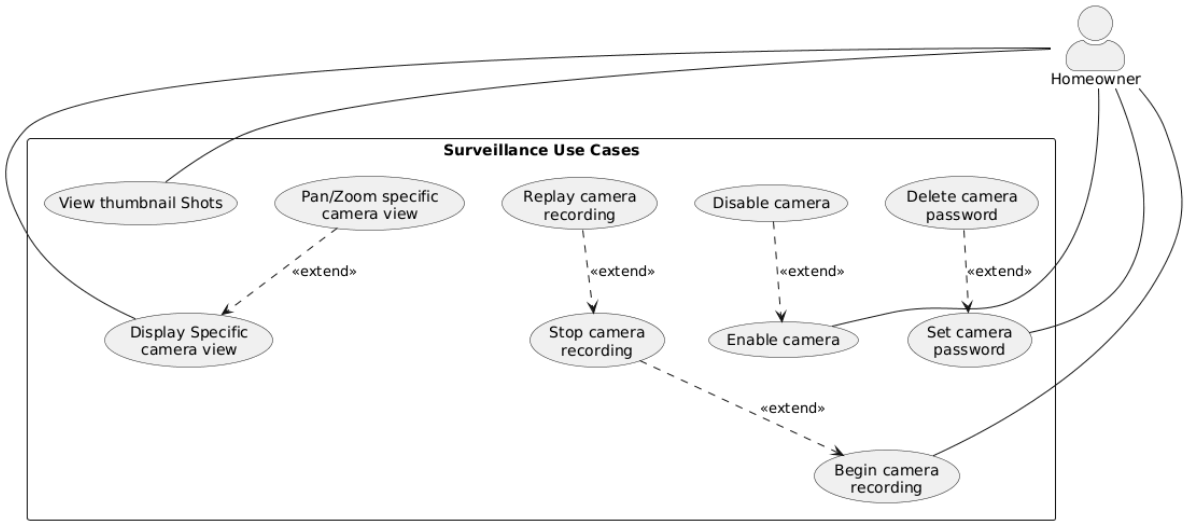
1. Common Functions



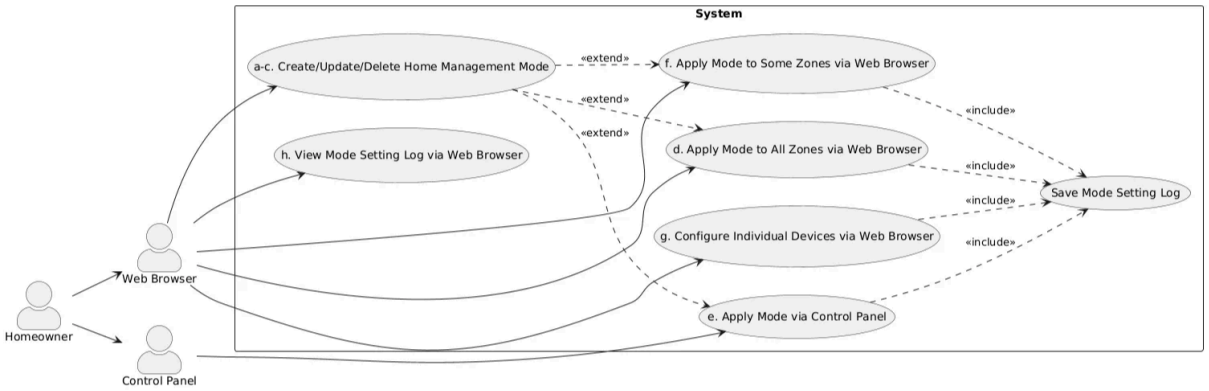
2. Security Functions



3. Surveillance Functions



4. Home management Functions



VI. Use Case

1. Common Use Cases

a. Log onto the System through Control Panel

Use case: Log onto the System through Control Panel

Primary actor: Homeowner

Goal in context: To log onto the SafeHome system through the Control Panel to access all system functions.

Preconditions:

- The system has been configured.
- The Master Password (4 digits) must be obtained.

Trigger: The homeowner decides to log onto the system.

Scenario:

1. The homeowner uses the Control Panel.
2. The homeowner enters the 4-digit Master Password.
3. The System validates the password successfully.

4. The System displays accessible functions (dashboard/config) on the Control Panel.

Exception:

- **3a. Password incorrect or not recognized:**
    1. The System prompts the homeowner to re-enter the password.
    2. After 3 consecutive failed attempts, the System locks access for a predefined duration (default: 5 minutes, user-configurable) and exits the use case.

Priority: Essential

When available: First increment

Frequency of use: Frequent

Channel to actor: Control Panel

b. Log onto the System through Web Browser

Use case: Log onto the System through Web Browser

Primary actor: Homeowner

Goal in context: To securely access the full system configuration and dashboard remotely via a web interface.

Preconditions:

- The homeowner's device is connected to the home network.
- The System is reachable.
- The Master ID and Password must be obtained.

Trigger: The homeowner attempts to access the system's web interface.

Scenario:

1. The homeowner submits the ID and Master Password via the web browser.
2. The System validates the credentials.
3. The System loads configuration data (floor plan, zones) and renders the full dashboard.
4. The System displays the dashboard on the homeowner's web browser.

Exception:

- **2a. Invalid Credentials:** The System displays an "Authentication Failed" message and reloads the login page.

Priority: Essential

When available: First increment

Frequency of use: Frequent

Channel to actor: Web Browser - Embedded Web Server

Reference: SEPA dialog slide 20-21

c. Change System State (ARM / DISARM)

Use case: Change Global System State

Primary actor: Homeowner

Goal in context: To change the global system security status between ARM and DISARM.

Preconditions:

- The homeowner is logged in or enters the Master Password when prompted.

Trigger: The homeowner decides to activate or deactivate monitoring.

Scenario:

1. The homeowner selects the desired state (ARM or DISARM) and enters the Master Password.
2. The Control Panel or Web Browser GUI sends the request and password to the System.
3. The System validates the password.
4. The System updates the global state and starts or stops monitoring accordingly.
5. The System displays confirmation of the new state.

Exception:

- **3a. Invalid Password:** The System displays “Incorrect Password” and maintains the current state.

Priority: Essential

When available: After log on in use case a or b

Frequency of use: Frequent

Channel to actor: Control Panel / Web Browser - Embedded Web Server

Reference: SEPA dialog slide 21

d. Change Master Password

Use case: Change Master Password

Primary actor: Homeowner

Goal in context: To update the Master Password for future access and authentication.

Preconditions:

- The homeowner is logged into the system.

Trigger: The homeowner navigates to the password change menu.

Scenario:

1. The homeowner enters the Old Master Password and the New Master Password.
2. The System validates the Old Password.
3. The System updates the stored credentials with the hashed New Password.
4. The System reloads authentication settings.
5. The Control Panel displays “Password Successfully Changed.”

Exception:

- **2a. Invalid Old Password:** The System rejects the change and retains the existing credentials.

Priority: High - security related common function

When available: After log on in use case b

Frequency of use: Frequent

Channel to actor: Web Browser - Embedded Web Server

Reference: Meeting logs 2nd Meeting

e. Manage Temporary Users

Use case: Manage Temporary User Accounts

Primary actor: Homeowner

Goal in context: To create, modify, or delete temporary user accounts with defined access limits.

Preconditions:

- The homeowner is logged in via the Web Browser.

Trigger: The homeowner accesses the User Management menu.

Scenario:

1. The homeowner selects an option: **Add**, **Modify**, or **Delete** a temporary user.
2. For **Add** or **Modify**, the homeowner enters the Guest Password, Expiration Date, and Assigned Zones.
3. The homeowner submits the data to the System.
4. The System validates the input.
    - For Add: The System creates a new Guest record.
    - For Modify: The System updates the existing record.
    - For Delete: The System removes the specified Guest record.
5. The System securely stores or updates the user database.
6. The System confirms successful completion on the Web Browser.

Exception:

- **4a. Missing or Invalid Input (Add/Modify):** The System displays an error message and cancels the operation.
- **4b. User Not Found (Delete):** The System displays “User Record Not Found.”

Priority: High

When available: After log on in use case b

Frequency of use: Not Frequent

Channel to actor: Web Browser - Embedded Web Server

Reference: SEPA dialog slide 20

f. Access System with Temporary Password (Guest Login)

Use case: Access System with Temporary Password

Primary actor: Guest

Goal in context: To allow temporary access using a Guest Password, enabling temporary DISARM of assigned zones.

Preconditions:

- A valid Temporary Password (4 digits) exists and is not expired.
- The System is currently ARMED.

Trigger: The guest decides to log onto the system.

Scenario:

1. The guest uses the Control Panel.
2. The guest enters the 4-digit Guest Password.
3. The System validates the password and retrieves assigned zones.
4. The System temporarily DISARMs only the assigned zones.

5. The Control Panel displays partial DISARM confirmation.

Exception:

- **3a. Incorrect Password:**
    1. The System requests re-entry.
    2. After 3 failed attempts, the System locks access for 5 minutes.
- **3b. Password Expired:** The System displays “Access Denied: Password Expired.”

When available: After temporary user is created in use case e

Frequency of use: Frequent

Channel to actor: Control Panel

Reference: SEPA dialog slide 20

g. Log Out / Revert Zones (Guest Logout)

Use case: Log Out and Revert Zone Exclusion

Primary actor: Guest

Goal in context: To securely log out from temporary access and restore full monitoring of all zones.

Preconditions:

- The Guest is currently logged in via Control Panel.

Trigger: The guest presses “Log Out” on the Control Panel.

Scenario:

1. The guest presses “Log Out.”
2. The Control Panel sends a request to revert excluded zones.
3. The System terminates the session.
4. The System re-arms all previously disarmed zones.
5. The Control Panel displays “System Restored.”

Open issue:

1. Should the system always restore to “ARM”, or revert to the pre-login state?

When available: After temporary user accessed to system in use case h

Frequency of use: Frequent

Channel to actor: Control Panel

h. Configure Floor Plan through Web Browser

Use case: Configure Floor Plan through Web Browser

Primary actor: Homeowner

Goal in context: To register or update a floor plan that defines spatial layout for configuring zones and device placement.

Preconditions:

- The homeowner has successfully logged into the system via Web Browser.
- Each floor plan name must be unique.

Trigger: The homeowner decides to register or modify the home layout.

Scenario:

1. The homeowner accesses Main Functions via Web Browser.
2. The homeowner clicks “Configure.”
3. The System displays configuration options: Floor Plan, Safety Zone, and Devices.
4. The homeowner selects “Add Floor Plan.”
5. The System opens the Floor Plan registration form.
6. The homeowner enters floor name and description, and selects a registration method.
    - (The method—image upload or drawing editor—remains under discussion.)
7. The System checks for duplicate names.
8. If valid, the System stores the plan in the database.
9. The System displays “Floor Plan Successfully Added.”
10. The Web Browser requests the updated list.
11. The System returns all registered plans.
12. The Web Browser updates the screen.

Exception:

- **6a. Missing Required Information:** The System displays “Please enter all required information.”
- **7a. Duplicate Name:** The System displays “A floor plan with this name already exists.”

Priority: High — Required before Safety Zone or Device configuration.

Open issues:

1. Registration method (image vs. drawing).
2. Multi-floor database structure.
3. Validation for corrupted uploads.

Connection: Must be completed before “Configure Safety Zone through Web Browser.”

i. Add Device through Web Browser

Use case: Add Device through Web Browser

Primary actor: Homeowner

Goal in context:

To register a new device (sensor, camera, or appliance), assign its location, and define its properties.

Preconditions:

- The homeowner is logged into the system via Web Browser.
- The device is powered on and connected to the same home network.
- The System can detect nearby broadcasting devices.

Trigger: The homeowner decides to add a new device via the configuration interface.

Scenario:

1. The homeowner navigates to “Configure” → “Add Device.”
2. The System scans the local network for available devices.
3. The System displays detected devices.

4. The homeowner selects a device.
5. The System displays the floor plan.
6. The homeowner selects the device's physical location.
7. The System requests confirmation.
8. The homeowner confirms.
9. The System prompts for device details (name, type, power mode).
10. The homeowner enters details and saves.
11. The System stores configuration and updates the registry.
12. The System displays confirmation and updates the floor plan.

Exception:

- **3a. No Devices Detected:** The System suggests checking power or network connection.
- **6a. Connection Lost During Registration:** The System returns to the device detection screen.
- **9a. Device Already Registered:** The System retrieves existing configuration for confirmation or update.

Priority: High — Core setup function after initial configuration.

Frequency of use: Occasional — when new devices are added.

Channel to actor: Web Browser Interface

2. Security Use Cases

a. ARM/DISARM through Control Panel

Use case: ARM/DISARM through Control Panel

Primary actor: Homeowner or Guest

Goal in context:

To arm or disarm the home security system through the Control Panel, either for the entire house or selected zones depending on user authority.

Preconditions:

- The Control Panel is powered and connected to the System.
- At least one safety zone exists.
- The user (Master or Guest) has valid credentials.
- All related devices and sensors are online.

Trigger:

The user decides to arm or disarm the system using the Control Panel.

Scenario:

1. The user presses **7 (ARM)** or **8 (DISARM)** on the Control Panel.
2. The Control Panel displays "# + Enter Password."
3. The user enters "# + [Password]."
4. The Control Panel sends the command and password to the System.
5. The System validates the password and determines the user type.

6. **If Master user:**
   a. The Control Panel displays zone selection.
   b. The user selects one or more zones.
   c. The Control Panel sends zone data to the System.
   d. The System executes ARM/DISARM for the selected zones.
7. **If Guest user:**
   a. The System executes ARM/DISARM only for pre-assigned zones.
8. The System updates all device states and returns the result.
9. The Control Panel displays “System is now [ARM/DISARM]” and updates LEDs.

Exceptions:

3a. Incorrect Password.
   .1 The Control Panel displays “Incorrect Password.”
   .2 The system allows up to five retries.
   .3 After five failures, lock

6a. Conflicting device settings within selected zones.
   .1 If conflict occurs in the same layer, alert user.

7a. Communication error with one or more devices in selected zones.
   .1 The system retries configuration updates.
   .2 If retries fail, the system logs the issue and displays a warning.

9a. Control Panel–System communication failure.
   .1 The Control Panel displays “Connection Error.”
   .2 The System queues the update for retry.

Priority:

High

Frequency of use:

Frequent (daily)

Channel to actor:

Control Panel interface

Open issues:

Whether zone selection should timeout automatically after authentication.

b. ARM/DISARM through Web Browser

Use case: ARM/DISARM through Web Browser

Primary actor: Homeowner

Goal in context:

To remotely arm or disarm the security system using the web interface, synchronizing with the Control Panel.

Preconditions:

- Homeowner has valid PC ID and Password.

- All zones and devices are connected.
- The Control Panel is online.

Trigger:

The homeowner decides to arm or disarm the system via web browser.

Scenario:

1. The homeowner logs into the web interface with PC ID and Password.
2. The System verifies credentials.
3. The System loads the Security tab.
4. The homeowner views zone list and current status.
5. The homeowner selects one or more zones or “Whole House.”
6. The homeowner clicks **ARM** or **DISARM.**
7. The System validates and executes the command.
    - If ARM → starts countdown (default 30 seconds, user-configurable).
    - If DISARM → executes immediately.
8. The System updates sensors and devices.
9. The System notifies the Control Panel to update LED indicators.
10. The Web Browser displays “System is now [ARM/DISARM].”

Exceptions:

1a. Invalid credentials.
.1 Login fails; error message shown.
.2 After five attempts, user account is temporarily locked.

Priority:

High

Frequency of use:

Frequent (remote access)

Channel to actor:

Web Browser interface

Open issues:

1. Whether ARM delay can be cancelled.
2. Whether push notification is sent after ARM delay.
3. Whether remote actions are timestamp-logged.

c. Alarm Condition Encountered

Use case: Alarm Condition Encountered

Primary actor: System

Supporting actors: Homeowner, Sensors, Control Panel

Goal in context:

To automatically trigger Panic Mode when intrusion occurs during Armed state, activating the siren and dispatching the monitoring service.

Preconditions:

- The System is Armed.
- Sensors are operational.
- Control Panel is connected.

Trigger:

A sensor detects an intrusion (e.g., door opened).

Scenario:

1. The sensor sends an event signal to the System.
2. The System checks Armed state.
3. If Armed → triggers Panic Mode.
4. The siren is activated via Control Panel:

   "PANIC MODE ACTIVE — Press # + MasterPW to cancel."
5. The System executes the monitoring service routine automatically.
6. The System records the event (source and timestamp).
7. If Disarmed → logs the intrusion event only.

Alternative Flow — Cancel Panic:

8a. The homeowner presses "# + MasterPW."

8b. The Control Panel sends the cancellation request.

8c. The System verifies the Master Password.

8d. If correct → stops the siren, logs "Cancelled."

8e. If incorrect → displays "Cancellation Failed."

Exceptions:

1a. Sensor malfunction.
.1 System logs fault and notifies homeowner.
.2 Faulty sensor excluded until reset.

4a. Siren malfunction.
.1 System displays "Siren Failure."
.2 System logs fault and continues silent monitoring.

Priority:

High

Frequency of use:

Occasional

Channel to actor:

Sensors → System → Control Panel

Open issues:

1. Whether siren volume and duration should be configurable.
2. Whether remote alerts should be implemented.
3. Whether security dispatch can be recalled after activation.

d. Configure Safety Zone

Use case: Configure Safety Zone

Primary actor: Homeowner

Goal in context:

To manage safety zones through the web browser interface, including creating, updating, deleting, and reviewing zones based on the registered floor plan and device configuration.

Preconditions:

- The homeowner has successfully logged into the system through the Web Browser.
- At least one floor plan must exist before safety zone configuration can begin.
- All devices (sensors, cameras, home appliances) are registered and active.

Trigger:

The homeowner decides to organize or modify the home's safety zones for security management and device mapping.

Scenario:

1. The homeowner accesses the Main Functions via the Web Browser.
2. The homeowner clicks the "Configure" button to open the configuration menu.
3. The Web Browser sends a request to the System for the list of existing zones, registered devices, and floor plan data.
4. The System returns the requested data to the Web Browser.
5. The Web Browser displays the Configure Functions tab, showing management options: "Add Safety Zone," "Update Safety Zone," "Delete Safety Zone," and the Floor Plan View.
6. If no floor plan is registered, the Web Browser displays a message: "No Floor Plan Configured" along with a "Configure Floor Plan" button that redirects to the floor plan registration screen.
7. If a floor plan is available, the Web Browser displays the layout with existing zones outlined and device locations shown.
8. When the homeowner clicks "Add Safety Zone," the Web Browser executes the **Create New Safety Zone** use case (UC5).
9. When the homeowner clicks "Update Safety Zone," the Web Browser executes the **Update Existing Safety Zone** use case (UC7).
10. When the homeowner clicks "Delete Safety Zone," the Web Browser executes the **Delete Safety Zone** use case (UC6).
11. After all desired modifications are completed, the homeowner clicks "Save / Apply."
12. The Web Browser sends all pending updates (created, modified, or deleted zones) to the System.
13. The System validates the changes and updates the configuration database.
14. The System returns a confirmation message: "Configuration Saved Successfully."
15. The Web Browser displays the confirmation message to the homeowner.

Exceptions:

6a. Missing floor plan.
.1 System blocks configuration.
.2 Displays "Please configure a floor plan first."

12a. Duplicate zone name.
.1 System shows “Zone name already exists.”
.2 Saving disabled until renamed.

12b. Device assignment conflict.
.1 System detects devices linked to multiple zones.
.2 Prompts user to revise assignments.

13a. Communication error during save.
.1 System retries save.
.2 If fail persists, logs “Configuration Sync Failure.”

Priority:

High

When available:

After the “Configure Floor Plan” module has been implemented and at least one floor plan is registered.

Frequency of use:

Occasional

Channel to actor:

Web Browser interface

Open issues:

1. Whether multi-floor configurations should display all floors in one view or per floor.
2. Whether changes should auto-save or require manual “Save / Apply.”
3. Whether unassigned devices should trigger automatic warnings after deletion or reassignment.

e. Create New Safety Zone

Use case: Create New Safety Zone

Primary actor: Homeowner

Goal in context:

To create and configure a new safety zone by defining its boundaries, assigning devices, and saving the configuration.

Preconditions:

- The homeowner has logged into the system via Web Browser.
- At least one floor plan exists.
- Devices are registered and available.

Trigger:

The homeowner decides to create a new safety zone.

Scenario:

1. The homeowner accesses the Configure Functions tab.
2. The homeowner selects the “Safety Zone” section.
3. The system displays the list of existing zones and the option to add a new one.
4. The homeowner clicks “Add Safety Zone.”
5. The system loads registered devices and displays the floor plan.

6. The homeowner enters zone information (name, floor, description).
7. The homeowner selects devices to include in the zone.
8. The system highlights selected devices.
9. The homeowner clicks “Save.”
10. The system validates input and detects any unassigned devices.
11. If valid, the system saves the new zone configuration.
12. The system displays “Safety Zone Successfully Created.”

Exceptions:

6a. Missing required fields.
.1 System displays “Please fill in all required fields.”
.2 Saving halted.

7a. Unassigned devices.
.1 System lists unassigned devices.
.2 User may continue or cancel.

10a. Duplicate zone name.
.1 System displays “Zone name already exists.”
.2 User must change name.

Priority:

High

When available:

After floor plan setup.

Frequency of use:

Occasional

Channel to actor:

Web Browser interface

Open issues:

1. Whether devices can belong to multiple zones.
2. Whether overlapping zones are allowed.
3. Whether automatic device assignment based on location should be supported.

f. Delete Safety Zone

Use case: Delete Safety Zone

Primary actor: Homeowner

Goal in context:

To remove an existing safety zone and detach its associated devices.

Preconditions:

- The homeowner is logged in.
- At least one safety zone exists.

Trigger:

The homeowner decides to delete a zone.

Scenario:

1. The homeowner opens the Configure tab.
2. The system lists existing zones.
3. The homeowner selects a zone to delete.
4. The system displays a confirmation:

   “Are you sure you want to delete this zone? Devices linked to this zone will lose their association.”
5. The homeowner confirms deletion.
6. The system verifies zone existence.
7. The system deletes the zone record.
8. The system detaches devices linked to the deleted zone.
9. The system updates the floor plan and zone list.
10. The system displays “Zone successfully deleted.”

Exceptions:

3a. Zone not found.
.1 System displays “Zone not found or already deleted.”
.2 Logs invalid attempt.

8a. Device detachment failure.
.1 System retries detachment.
.2 If still fails, shows “Some devices could not be detached.”
.3 Logs issue for admin review.

Priority:

Medium

When available:

After Create and Update functionalities.

Frequency of use:

Occasional

Channel to actor:

Web Browser interface

Open issues:

1. Whether password confirmation is required for deletion.
2. Whether a soft-delete option should be implemented.
3. How to handle devices belonging to multiple zones.

g. Update Existing Safety Zone

Use case: Update Existing Safety Zone

Primary actor: Homeowner

Goal in context:

To modify existing safety zone details while maintaining device associations.

Preconditions:

- The homeowner has logged into the system.

- At least one zone exists.
- A floor plan is registered.

Trigger:

The homeowner decides to update a zone configuration.

Scenario:

1. The homeowner accesses the Configure tab.
2. The system displays zones on the floor plan.
3. The homeowner selects a zone to edit.
4. The system loads details and device associations.
5. The homeowner updates the zone name or assigned devices.
6. The system visually updates changes.
7. The homeowner clicks “Save.”
8. The system validates the configuration.
9. If valid, the zone record is updated in the database.
10. The system refreshes the zone display and confirms “Zone successfully updated.”

Exceptions:

5a. Missing information.
.1 System displays “Please enter all required fields.”
.2 Saving disabled until correction.

8a. Unassigned devices.
.1 System lists devices not linked to any zone.
.2 User can assign or ignore.

9a. Update communication failure.
.1 System retries update.
.2 If fail persists, shows “Update Failed – Please Retry.”
.3 Logs error as “Configuration Sync Failure.”

Priority:

High

When available:

After Create and Delete functionalities.

Frequency of use:

Occasional

Channel to actor:

Web Browser interface

Open issues:

1. Whether version history should be maintained.
2. Whether overlapping zones require re-validation.
3. Whether unassigned devices should auto-reassign.

h. Apply Mode through Control Panel

Use case: Apply Mode through Control Panel

Primary actor: Homeowner

Goal in context:

To apply a predefined or custom Home Management mode (Home, Away, Custom) to a selected zone using the Control Panel.

Preconditions:

- The Control Panel and System are connected.
- Master Password is registered.
- At least one zone and mode exist.
- Custom modes are pre-registered via Web Browser.

Trigger:

The homeowner decides to apply a mode to a selected zone.

Scenario:

1. The homeowner presses “9” on the Control Panel.
2. The Control Panel displays “# + Enter Master Password.”
3. The homeowner enters “# + [Password].”
4. The Control Panel sends authentication to the System.
5. The System verifies the password.
6. If correct:
   a. The Control Panel shows “Select Zone.”
   b. The homeowner selects one zone.
   c. The Control Panel displays available modes: Home (1), Away (2), Custom (3+).
   d. The homeowner selects a mode.
   e. The Control Panel sends Zone ID and Mode ID to the System.
   f. The System retrieves and applies mode configuration.
   g. The System updates security and home appliance states.
   h. The Control Panel displays “Mode Successfully Applied.”
7. If incorrect:
   “Incorrect Password – Remaining Attempts: [n].”
   After five failures, System lock occurs until manual reset.

Exceptions:

3a. Incorrect Master Password.
   .1 Control Panel shows “Incorrect Password.”
   .2 Allows five retries, then system lock.

5a. Communication failure with System.
   .1 Control Panel displays “Connection Error.”
   .2 System retries transmission.
   .3 If fails, manual reattempt required.

6a. Missing mode configuration.

.1 System displays “Mode Configuration Not Found.”

.2 User directed to configure via web browser.

Priority:

High

When available:

After integration of Home Management and Security modules.

Frequency of use:

Frequent (daily use).

Channel to actor:

Control Panel interface

Open issues:

1. Whether multiple zones can be selected at once.
2. Whether failed mode applications should auto-retry.
3. Whether mode logs should be separate from intrusion logs.

i. View Intrusion Log

Use case: View Intrusion Log

Primary actor: Homeowner

Goal in context:

To review intrusion events detected by the system and manage log entries.

Preconditions:

- The homeowner has logged in.
- Intrusion events exist in the database.
- Cameras and sensors are linked to zones.

Trigger:

The homeowner decides to review or delete intrusion logs.

Scenario:

1. When a sensor detects an intrusion, the System identifies the zone.
2. The System starts camera recording in the affected zone.
3. The System stores the intrusion log with Zone ID, Sensor ID, Timestamp, and Video Reference.
4. Later, the homeowner opens “Monitoring → Intrusion Log.”
5. The System displays intrusion log entries.
6. The homeowner selects a log to review.
7. The System displays event details and footage.
8. The homeowner may choose to delete a log.
9. The System prompts for PC Password.
10. The homeowner enters the password.

11. The System verifies credentials.
12. If correct → deletes log and confirms “Log Deleted Successfully.”
13. If incorrect → displays “Incorrect Password – Deletion Cancelled.”

Exceptions:

9a. Incorrect PC password.
.1 System displays “Incorrect Password.”
.2 Lock system after five consecutive failures.

10a. Database connection error.
.1 System displays “Deletion Failed – Please Retry Later.”
.2 Queues deletion request for retry.

3a. Missing or unavailable camera feed.
.1 System stores event as “Video Unavailable.”
.2 Displays “Camera Offline – Video Reference Missing.”

Priority:

Medium

When available:

After implementation of Alarm and Monitoring modules.

Frequency of use:

Occasional

Channel to actor:

Web Browser interface

Open issues:

1. Whether logs expire automatically.
2. Whether partial deletion is supported.
3. Whether Guests can view but not delete logs.

j. Call Monitoring Service through Control Panel

Use case: Call Monitoring Service through Control Panel

Primary actor: Homeowner

Supporting actors: Control Panel, System

Goal in context:

To allow the homeowner to manually trigger Panic Mode from the Control Panel during an emergency, activating the siren, displaying a panic alert, dispatching the monitoring service, and logging the event as a manual trigger.

Preconditions:

- The Control Panel and System are powered on, connected, and operational.
- The homeowner has physical access to the Control Panel.
- The System can be in either Armed or Disarmed state.

Trigger:

The homeowner simultaneously presses “* + #” on the Control Panel to manually activate Panic Mode.

Scenario:

1. The homeowner presses “* + #” on the Control Panel.
2. The Control Panel sends a **Manual Panic Trigger** signal to the System.
3. The System immediately activates **Panic Mode**, regardless of the current Armed/Disarmed state.
4. The System commands the Control Panel to display the message:

   “PANIC MODE ACTIVE — Press # + MasterPW to cancel.”
5. The System activates the siren and executes the **Monitoring Service Routine**, dispatching security personnel.
6. The System records a panic log entry including:
   - Trigger Type: Manual
   - Source: Control Panel
   - Status: Active

Alternative Flow — Cancel Panic:

7a. The homeowner decides to cancel Panic Mode after a false or accidental activation.

7b. The homeowner presses “# + [Master Password]” on the Control Panel.

7c. The Control Panel sends a **Cancel Panic Request** with Master Password to the System.

7d. The System verifies the password.

7e. If the password is correct:

- The System stops the siren.
- The Control Panel displays “Panic Cancelled.”
- The System updates the log: “Cancelled by User.”
- The dispatch request remains active for safety.

  7f. If the password is incorrect:
- The System displays “Incorrect Password — Cancellation Failed.”

Exceptions:

2a. Control Panel communication failure.
.1 Local siren and display still activate.
.2 Once reconnected, System syncs and logs the event.

5a. Dispatch transmission failure.
.1 System retries up to three times.
.2 If retries fail, notifies homeowner post-recovery.
.3 Logs event as “Dispatch Retry Failure.”

6a. Database logging error.
.1 System stores panic event in temporary cache.
.2 Syncs automatically when database reconnects.

Priority:

High — Core emergency safety feature.

When available:

First release after Panic Mode automation is implemented.

Frequency of use:

Rare — Only during real emergencies or accidental triggers.

Channel to actor:

Control Panel interface (physical input and display).

Open issues:

1. Whether remote alerts (SMS, app notification) should be sent upon manual panic activation.
2. Whether multiple manual Panic triggers within a short time should be limited.
3. Whether the Control Panel should support voice or sound confirmation when Panic Mode is active.

3. Surveillance Use Cases

a. **Display Specific camera view**

Use case: Display Specific camera view

Primary actor: Homeowner

Goal In Context: To see specific camera's view

Preconditions: System should be ready, and internet should be set; appropriate user ID and passwords must be obtained.

Trigger: Homeowner decides to take a look of a camera.

Scenario:

1. The homeowner logs onto the system – see use case : "Log onto the system through web browser"
2. The homeowner selects "surveillance" from the major function buttons.
3. The system displays the selection page (Selection page contains the floor plan and thunbnail shots).
4. The homeowner selects a camera icon from the floor plan.
5. The system asks a password if the selected camera has a password.
6. The homeowner enters the password.
7. The system validates the password.
8. The system displays the state of the selected camera.
9. The homeowner selects the "view" button.
10. The system displays video output within the viewing window at one frame per second.

Exceptions:

2a. Surveillance function not configured for this system - system displays appropriate error message; see use-case: "Configure surveillance function"

3a. A floor plan is not available or has not been configured--display appropriate error message and see use-case: "configure floor plan."

5a. If the camera does not have a password, go to procedure 8.

7a. The password is incorrect or not recognized - if input tries are less than five then prompts for reentry. Otherwise log out from system.

9a. If the camera is disabled, "view" button is disabled – see use case : "Enable camera"

When available: First increment

Frequency of use: Many times per day

Channel to actor: PC-based system with web browser

Secondary actor: Support technician, Webmaster, Camera

Channels to secondary actors:

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

Open Issues:

1. Will system response via the Internet be acceptable given the bandwidth required for camera views?
2. Will we develop a capability to provide video at a higher frames-per-second rate when high bandwidth connections are available?
3. What if the homeowner forgets the specific password for the camera?
4. What if a specific camera is broken?

b. **Pan/Zoom specific camera view**

Use case: Pan/Zoom specific camera view

Primary actor: Homeowner

Goal In Context: To move and zoom specific camera's view

Preconditions: The homeowner looks at specific camera view - see use case: "display specific camera view."

Trigger: Homeowner decides to pan or zoom specific camera view.

Scenario:

1. The homeowner drags "Pan" to "L" if the homeowner wants to turn camera left, "R" if the homeowner wants to turn camera right.
2. The system displays video output with changed camera's view within the viewing window at one frame per second.
3. The homeowner drags "Zoom" to "In" if the homeowner wants to zoom in camera, "Out" if the homeowner wants to zoom out camera.
4. The system displays video output with changed camera's view within the viewing window at one frame per second.

Exceptions:

When available: First increment

Frequency of use: Many times per day

Channel to actor: PC-based system with web browser

Secondary actor: Camera

Channels to secondary actors: wireless connectivity

c. **Begin camera recording**

Use case: Begin camera recording

Primary actor: Homeowner

Goal In Context: To begin camera recording

Preconditions: The system displays the state of the selected camera; selected camera is not recording now.

Trigger: Homeowner decides to begin camera recording.

Scenario:

1. The homeowner presses “BEGIN” of “RECORDING”
2. The camera starts to record.
3. The system displays updated UI with recording part is “RECORDING...ON”

Exceptions:

1a. If selected camera is disabled, then “BEGIN” is not activated.

1b. If selected camera is recording now, then “BEGIN” is not activated.

2a. If the recorded DB is filled by video 80% of the capacity, system displays “The Recorded DB is filled with 80% capacity”.

2b. If the recorded DB storage is full, system notices that the storage is full and stops recording.

3a. Recording should be continued in background even if the homeowner moves to another pages.

When available: First increment

Frequency of use: Once a month

Channel to actor: PC-based system with web browser

Secondary actor: Camera

Channels to secondary actors: wireless connectivity

Open Issues:

1. How should be recording storage managed?

d. **Stop camera recording**

Use case: Stop camera recording

Primary actor: Homeowner

Goal In Context: To stop camera recording

Preconditions: The system displays the state of the selected camera; selected camera is recording now.

Trigger: Homeowner decides to stop camera recording.

Scenario:

1. The homeowner presses “STOP” of “RECORDING”
2. The camera stops to record.
3. The system displays updated UI with recording part is “RECORDING...OFF”

Exceptions:

1a. If selected camera is not recording now, then “STOP” is not activated.

When available: First increment

Frequency of use: Once a month

Channel to actor: PC-based system with web browser

Secondary actor: Camera

Channels to secondary actors: wireless connectivity

Open Issues:

1. What state will be specific camera if the power suppliment cuts suddenly?

e. **Replay camera recording**

Use case: Replay camera recording

Primary actor: Homeowner

Goal In Context: To replay camera recording

Preconditions: The system displays the state of the selected camera; selected camera has at least 1 video recorded before.

Trigger: Homeowner decides to replay camera recording.

Scenario:

1. The homeowner presses “SHOW” of “RECORDING”.
2. The system displays the list of previous recorded videos.
3. The homeowner clicks specific file to want to replay.
4. The system plays video in display.

Exceptions:

1a. If selected camera is disabled, then “SHOW” is not activated.

2a. If selected camera has no recorded video, then the system displays “There is no recorded video” during 3 seconds and ends.

When available: First increment

Frequency of use: Once a month

Channel to actor: PC-based system with web browser

Secondary actor: Recorded DB

Channels to secondary actors: Internet database connection

Open Issues:

1. What playback controls are available such as pause, fast-forward and rewind?
2. How is the recording list organized and displayed?
3. What if the video file has only broken pieces?

f. Set camera password

Use case: Set camera password

Primary actor: Homeowner

Goal In Context: To set camera’s password

Preconditions: The system displays the state of the selected camera.

Trigger: Homeowner decides to set camera password.

Scenario:

1. The homeowner clicks “SET” of “PASSWORD”.
2. If there is already camera PW, then system displays “Enter the original camera PW”.
3. The homeowner enters the camera PW.
4. The system validates the camera PW is correct.
5. The system displays “Enter the new camera PW”.
6. The homeowner enters the new camera PW.
7. The system diplays “Re-Enter the new camera PW”.

8. The homeowner re-enters the new camera PW.
9. The system validates two camera PWs are same.
10. The system displays “The camera PW sets”.

Exceptions:

1a. If selected camera is disables, then “SET” is not activated.

2a. If there is not the camera PW, then proceeds to step 5.

4a. If the homeowner is wrong for answering the camera password under 5 trial, then return to step 2. Otherwise, the system is logged out from the web server.

8a. If 2 new camera PWs are not same, then return to step 5.

When available: First increment

Frequency of use: Once a 3 months

Channel to actor: PC-based system with web browser

Secondary actor: System

Channels to secondary actors: PC-based system

Open Issues:

1. What are the complexity requirements for the new password?
2. Is there a password recovery mechanism if the homeowner forgets the original password?

g. **Delete camera password**

Use case: Delete camera password

Primary actor: Homeowner

Goal In Context: To delete camera’s password

Preconditions: The system displays the state of the selected camera; selected camera already has a camera PW.

Trigger: Homeowner decides to delete camera password.

Scenario:

1. The homeowner clicks “DELETE” of “PASSWORD”.
2. The system displays “Enter the original camera PW”.
3. The homeowner enters the camera PW.
4. The system validates the camera PW is correct.
5. The system displays “The camera PW is deleted” during 3 seconds.

Exceptions:

1a. If selected camera is disabled, then “DELETE” is not activated.

2a. If the camera PW is not existed already, the system displays “There is no camera PW already”.

4a. If the homeowner is wrong for answering the camera password under 5 trial, then return to step 2. Otherwise, the system is logged out from the web server.

When available: First increment

Frequency of use: Once a 3 months

Channel to actor: PC-based system with web browser

Secondary actor: System

Channels to secondary actors: PC-based system

Open Issues:

1. What if the homeowner forgets the camera PW they are trying to delete?

h. **View thumbnail shots**

Use case: View thumbnail shots

Primary actor: Homeowner

Goal In Context: To see thumbnail Shots

Preconditions: Homeowner is logged onto the system via web browser.

Trigger: Homeowner decides to view thumbnail shots.

Scenario:

1. Homeowner selectes “surveillance”.
2. System displays the selection page (Selection page contains the floor plan and thunbnail shots).

Exceptions:

2a. If the specific camera has a camera PW, then the thumbnail shot is blurred.

When available: First increment

Frequency of use: Many times per day

Channel to actor: PC-based system with web browser

Secondary actor: System

Channels to secondary actors: PC-based system

Open Issues:

1. How often are the thumbnail shots refreshed?

i. **Enable camera**

Use case: Enable camera

Primary actor: Homeowner

Goal In Context: To make camera working

Preconditions: The system displays the state of the selected camera; specific camera is disabled.

Trigger: Homeowner decides to enable camera.

Scenario:

1. Homeowner clicks “ENABLE/DISABLE”.
2. If specific camera has a camera PW, then ask the homeowner the camera PW.
3. The homeowner enters the camera PW.
4. The system validates the camera PW.
5. System enables camera.
6. System displays “This camera is enabled” for 3 seconds.

Exceptions:

1a. If the state of specific camera is ebabled, the system will disable specific camera.

2a. If specific camera doesn’t have a camera PW, then proceeds to step 5.

4a. If the homeowner is wrong for answering the camera password under 5 trial, then return to step 2. Otherwise, the system is logged out from the web server.

When available: First increment

Frequency of use: Infrequent

Channel to actor: PC-based system with web browser

Secondary actor: Camera

Channels to secondary actors: wireless connectivity

Open Issues:

1. What if the homeowner forgets the camera PW?

j. **Disable camera**

Use case: Disable camera

Primary actor: Homeowner

Goal In Context: To make camera not working

Preconditions: The system displays the state of the selected camera; specific camera is enabled.

Trigger: Homeowner decides to disable camera.

Scenario:

1. Homeowner clicks “ENABLE/DISABLE”.
2. If specific camera has a camera PW, then ask the homeowner the camera PW.
3. The homeowner enters the camera PW.
4. The system validates the camera PW.
5. System disables camera.
6. System displays “This camera is disabled” for 3 seconds.

Exceptions:

1a. If the state of specific camera is disabled, the system will enable specific camera.

2a. If specific camera doesn’t have a camera PW, then proceeds to step 5.

4a. If the homeowner is wrong for answering the camera password under 5 trial, then return to step 2. Otherwise, the system is logged out from the web server.

When available: First increment

Frequency of use: Infrequent

Channel to actor: PC-based system with web browser

Secondary actor: Camera

Channels to secondary actors: wireless connectivity

Open Issues:

1. What if the homeowner forgets the camera PW?

4. Home Management Use Cases

a. Create a New Home Management Mode on Web Browser

Use case: Create a New Home Management Mode

Primary actor: Homeowner

Goal in context:

To create a new Home Management Mode that defines security and home appliance settings for the entire house, selected zones, or individual devices.

Preconditions:

- The homeowner is logged into the system via the web browser.
- All controllable devices and zones are registered and accessible.

Trigger:#

The homeowner decides to create a new mode to automate or customize the home environment.

Scenario:

1. The homeowner accesses the Home Management menu via the web browser.
2. The system displays a list of existing Home Management Modes and the option to create a new one.
3. The homeowner selects “Create New Mode.”
4. The system prompts the homeowner to enter a mode name, optional description, and base mode (Home / Away).
5. The homeowner optionally specifies:
   - Security mode linkage for selected zones (e.g., automatically arm certain zones when active)
   - Home appliance settings (lighting, HVAC, appliance power, AV devices)
   - Schedule settings (e.g., activate at 10 PM, deactivate at 8 AM)
6. The homeowner reviews the configuration summary.
7. The homeowner confirms creation.
8. The system stores the new mode configuration and displays a confirmation message.

Exceptions:

5a. Selected zone contains unregistered devices.

.1: The system warns the user and allows skipping or retrying registration.

5b. Selected zone contains offline devices.

.1: The system alerts that changes will be applied once devices are online.

6a. Invalid or conflicting settings (e.g., same device assigned contradictory states across modes).

.1: The system will override setting in the order device > zone > base. If a conflict occurs on the same layer, alert the user.

6b. Invalid settings (e.g., turning off refrigerator)

.1: System rejects the input

Priority: Medium priority. Enables automation and user convenience.

When available: Second increment (after system setup and login).

Frequency of use: Occasional, mainly during setup or lifestyle changes.

Channel to actor: Web browser interface

b. Update Home Management Mode on Web Browser

Use case: Update Home Management Mode

Primary actor: Homeowner

Goal in context:

To modify an existing Home Management Mode that defines security and appliance settings for the entire house, selected zones, or individual devices.

Preconditions:

- The homeowner is logged into the system via the web browser.
- At least one mode exists.
- All devices and zones are registered and accessible.

Trigger:

The homeowner decides to edit an existing Home Management Mode.

Scenario:

1. The homeowner accesses the Home Management menu via the web browser.
2. The system displays a list of existing modes.
3. The homeowner selects a mode to edit.
4. The system retrieves and displays the selected mode's configuration.
5. The homeowner modifies mode name, base mode, zone settings, or device configurations.
6. The homeowner optionally updates security linkage or schedule settings.
7. The system validates the configuration for conflicts and consistency.
8. The homeowner reviews the updated summary.
9. The homeowner confirms the update.
10. The system saves the new configuration and displays confirmation.

Exceptions:

4a. For the default modes (Home / Away), security configuration cannot be overridden in default modes. Only home appliance configurations can be added.

5a. The homeowner attempts to modify a zone containing unregistered devices.

.1: The system warns the user and allows skipping or retrying registration.

5b. The homeowner modifies settings for offline devices.

.1: The system alerts that changes will be applied once devices are online.

7a. Conflicting device or zone settings are detected.

.1: The system will override setting in the order device > zone > base. If a conflict occurs on the same layer, alert the user.

Priority: Medium priority. Core customization function.

When available: Second increment (after mode creation).

Frequency of use: Moderate, mainly during adjustments.

Channel to actor: Web browser interface

Open issues:

1. Should version history be maintained for modified modes?

c. Delete Home Management Mode on Web Browser

Use case: Delete Home Management Mode

Primary actor: Homeowner

Goal in context:

To delete an existing Home Management Mode that is no longer needed, ensuring that no active zones depend on it.

Preconditions:

- The homeowner is logged into the system via the web browser.
- At least one mode exists.

Trigger:

The homeowner decides to delete an existing mode.

Scenario:

1. The homeowner accesses the Home Management menu via the web browser.
2. The system displays the list of modes.
3. The homeowner selects a mode to delete.
4. The system checks whether any zones are currently linked to the selected mode.
5. If none are linked, the system prompts for confirmation.
6. The homeowner confirms deletion.
7. The system deletes the mode from the database.
8. The system displays a confirmation message.

Exceptions:

3a. The default modes (Home / Away) cannot be deleted.

4a. One or more zones are currently linked to the selected mode.

.1: The system displays a warning message that the mode cannot be deleted while it is applied to active zones.

.2: The system provides a list of the dependent zones and guides the homeowner to unassign or change their modes first.

4b. The selected mode does not exist or was already deleted by another session.

.1: The system alerts the homeowner and refreshes the mode list.

Priority: Medium priority. Maintains consistency and prevents invalid configurations.

When available: Second increment (after creation and update).

Frequency of use: Occasional, mainly during cleanup.

Channel to actor: Web browser interface

Open issues:

1. Should deleted modes be recoverable from backup (soft delete)?

d. Apply Home Management Mode to All Zones via Web Browser

Use case: Apply Home Management Mode to All Zones

Primary actor: Homeowner

Goal in context:

To apply a selected Home Management Mode to all zones, updating device and security configurations consistently.

Preconditions:

- The homeowner is logged into the system via the web browser.
- All zones and devices are registered and accessible.
- The selected mode has valid configurations.

Trigger:

The homeowner decides to activate a Home Management Mode for the entire house.

Scenario:

1. The homeowner opens the Home Management interface.
2. The system displays available modes.
3. The homeowner selects a mode.
4. The system retrieves mode configuration (base, zone, device).
5. The system applies configuration to all zones with priority: device > zone > base.
6. Each zone updates security and device states.
7. The system notifies the Control Panel.
8. The Control Panel verifies each zone's arm/disarm status.
9. If all devices are armed, the "ARM" light turns on; otherwise, it remains off.
10. The system displays a confirmation message.

Exceptions:

5a. Some zones or devices fail to respond.

.1: The system retries applying the configuration to unresponsive devices.

.2: If retries fail, the system displays a warning to the user.

6a. Security device is unregistered.

.1: Alert the issue to user.

8a. Control Panel communication failure.

.1: The system queues the update and retries until acknowledgment is received.

Priority: Medium priority. Applies full-home configurations.

When available: Second increment (after mode creation).

Frequency of use: Occasional, typically when leaving or returning home.

Channel to actor: Web browser

Secondary actor: Control Panel

Channel to secondary actor: System

Open issues:

1. Should partial application be allowed if some zones are offline?

e. Apply Home Management Mode via the Control Panel

Use case: Apply Home Management Mode via the Control Panel

Primary actor: Homeowner

Goal in context:

To apply a selected Home Management Mode directly from the Control Panel, synchronizing security and appliance settings across the house.

Preconditions:

- The homeowner has physical access to the Control Panel.
- The Control Panel is connected to all zones and devices.
- The selected mode is predefined and not editable.

Trigger:

The homeowner decides to activate a mode via the Control Panel.

Scenario:

1. The homeowner enters the Control Panel interface.
2. The homeowner selects a mode:
    - Away mode → 7#MasterPW
    - Home mode → 8#MasterPW
    - Custom mode → 9#MasterPW + mode number
    - Select zone → Above key + #zone number
3. The Control Panel verifies Master Password and mode details.
4. Upon successful authentication, the configuration is retrieved.
5. The Control Panel applies the configuration to all zones.
6. The system arms or disarms devices according to mode.
7. The Control Panel checks each zone's security status.
8. If all devices are armed, the "ARM" light turns on; otherwise, it remains off.
9. The Control Panel applies appliance settings.
10. The Control Panel displays confirmation.

Exceptions:

2a. Selected mode does not exist

.1: The system indicates that the mode application has failed.

4a. Master password authentication fails.

.1: The system limits the maximum number of retries
***Reference in SRS VI-1 Log onto the system through control panel**

6a. Some zones or devices fail to respond.

.1: The system retries applying the configuration to unresponsive zones or devices.

.2: If retries fail, the system logs the issue and displays a warning message.

8a. A zone fails to arm due to a malfunctioning device.

.1: The system keeps the ARM light off and displays a warning.

9a. Communication error with one or more zones.

.1: The system keeps the M light off and displays a warning. The homeowner can delete a disabled device through the web browser.

Priority: Medium priority. Supports daily operation.

When available: Second increment (after browser-based mode management).

Frequency of use: Frequent—used daily.

Channel to actor: Control Panel

f. Apply Home Management Mode to Selected Zones via Web Browser

Use case: Apply Home Management Mode to Selected Zones

Primary actor: Homeowner

Goal in context:

To apply a selected mode to specific zones while leaving others unchanged.

Preconditions:

- The homeowner is logged into the system via the web browser.
- All zones and devices are registered and accessible.
- The selected mode exists with valid configurations.

Trigger:

The homeowner decides to apply a mode to selected zones.

Scenario:

1. The homeowner opens the Home Management interface.
2. The system displays available modes.
3. The homeowner selects a mode.
4. The homeowner selects one or more zones.
5. The system retrieves configuration.
6. The system applies settings to selected zones following priority: device > zone > base.
7. The system updates security and appliance settings.
8. The UI displays the applied mode per zone.
9. The system displays a confirmation message.

Exceptions:

6a. Selected zone contains unregistered or offline devices.

.1: The system warns the user and allows skipping or retrying registration.

6b. conflicting device settings within selected zones.

.1: The system will override setting in the order device > zone > base. If a conflict occurs on the same layer, alert the user.

6c. Invalid device settings within selected zones. (e.g. turn off the refrigerator)

.1: System rejects the input

7a. Communication error with one or more devices in the selected zones.

.1: The system retries configuration updates.

.2: If retries fail, the system logs the issue and displays a warning message.

Priority: Medium priority. Zone-specific automation.

When available: Second increment (after mode creation and full application).

Frequency of use: Frequent—used daily.

Channel to actor: Web browser

Open issues:

1. Should partial application be allowed if some devices in the selected zones are offline?

g. Configure Individual Devices via Web Browser

Use case: Configure Individual Devices via Web Browser

Primary actor: Homeowner

Goal in context:

To allow manual configuration and status viewing of individual devices independent of Home Management Modes.

Preconditions:

- The homeowner is logged into the system via the web browser.
- All devices are registered, accessible, and connected.

Trigger:

The homeowner decides to adjust specific device settings manually.

Scenario:

1. The homeowner opens the Home Management interface.
2. The system displays all registered devices grouped by zone.
3. The homeowner selects a device.
4. The system displays current status and available settings.
5. The homeowner adjusts settings (lighting, HVAC, appliance power, AV devices).
6. The system updates the device and displays confirmation.
7. The homeowner repeats for additional devices as needed.
8. The system displays updated statuses.

Exceptions:

5a. Selected device is offline
.1 : system warns and allows retry.

5b. Invalid configuration values entered
.1 : system rejects the input and prompts for correction.

Priority: Medium priority. Supports manual control.

When available: Second increment (after device registration).

Frequency of use: Occasional—temporary or special adjustments.

Channel to actor: Web browser

h. View Home Management Mode Setting Log via Web Browser

Use case: View Home Management Mode Setting Log via Web Browser

Primary actor: Homeowner

Goal in context:

To view a log of mode applications including actor, scope, and result for auditing or troubleshooting.

Preconditions:

- The homeowner is logged into the system via the web browser.
- Home Management Modes have been applied at least once.
- The system records mode application events.

Trigger:

The homeowner decides to review past mode applications.

Scenario:

1. The homeowner opens the Home Management interface.
2. The system provides an option to view mode logs.
3. The homeowner selects a date range or filter criteria (actor, zone, device, success/failure).
4. The system retrieves the relevant logs.
5. The system displays each entry with timestamp, actor, scope, settings applied, and result.
6. The homeowner scrolls, sorts, or exports the log.

Exceptions:

4a. Log retrieval fails
.1 : system displays error and allows retry.

4b. No records founds
.1 : system displays “No log entries found.”

Priority: Medium priority. Supports auditing and awareness.

When available: Second increment (after mode application and device configuration).

Frequency of use: Occasional—verification or troubleshooting.

Channel to actor: Web browser

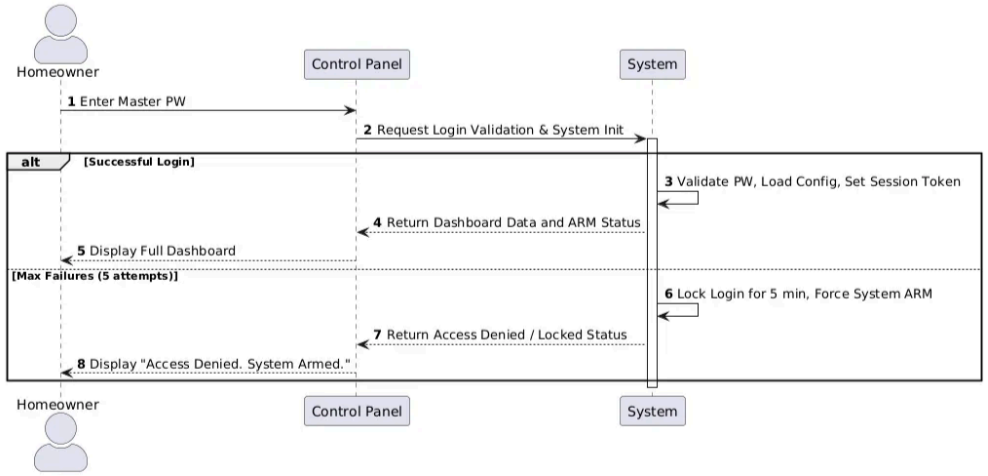
Open issues:

1. How long should the system keep the logs?

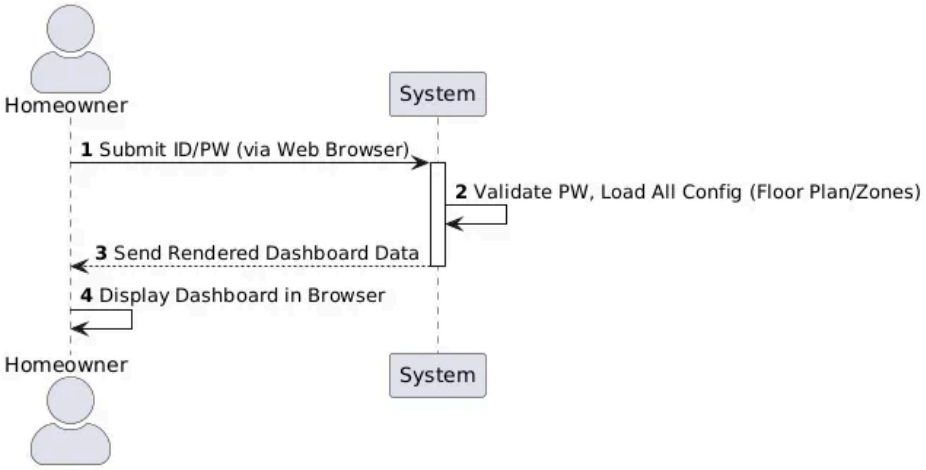
VII. Sequence Diagram

1. Common **Sequence Diagram**

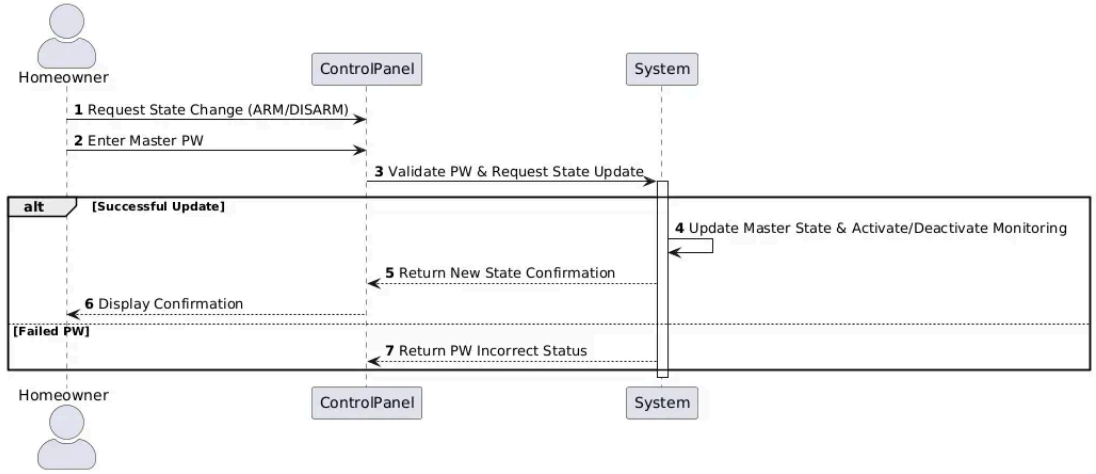
a. Log onto the system through control panel



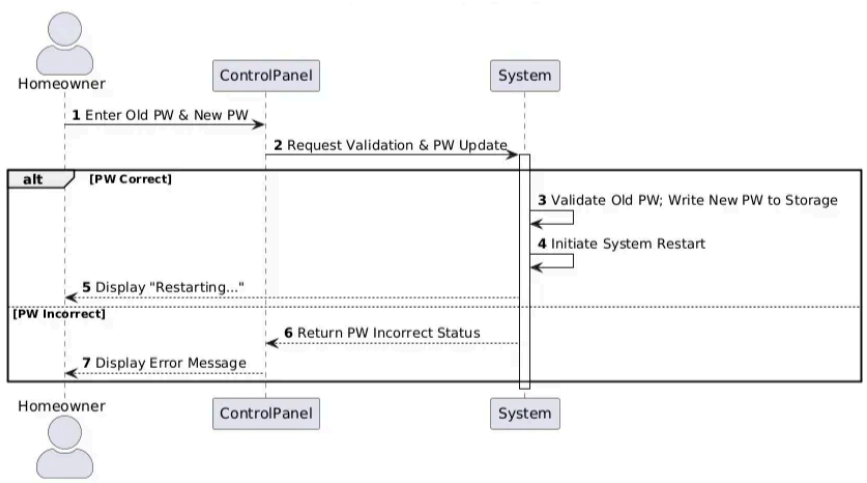
b. Log onto the system through web browser



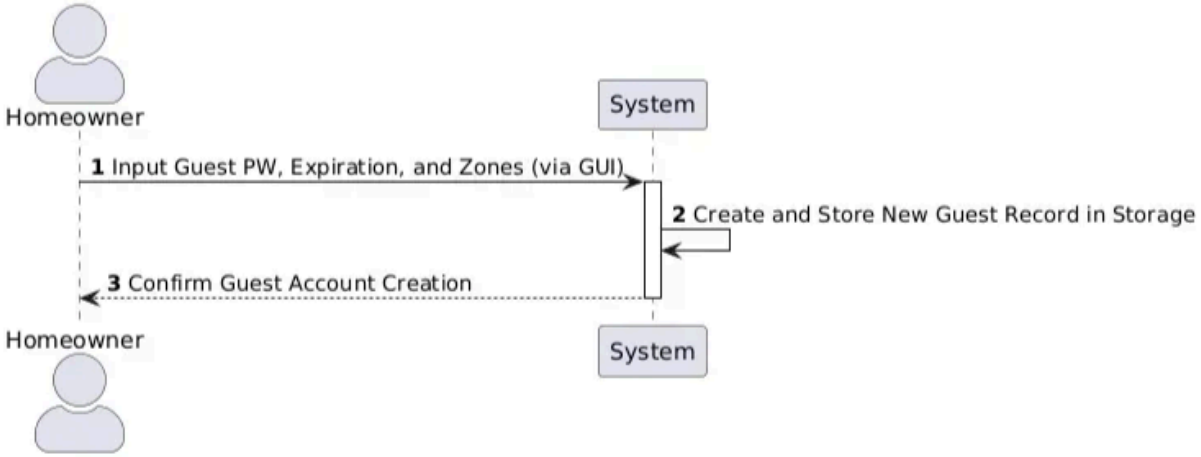
c. Change System State (ARM / DISARM)



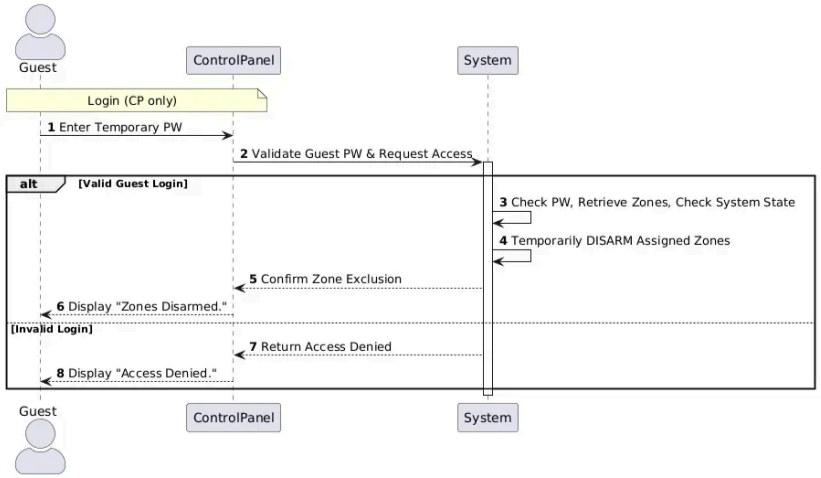
d. Change Master PW



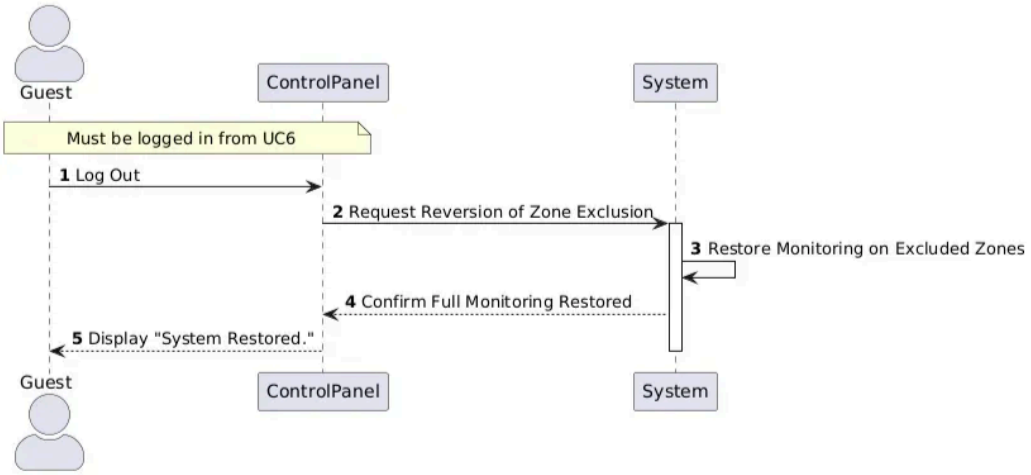
e. Manage Temporary Users



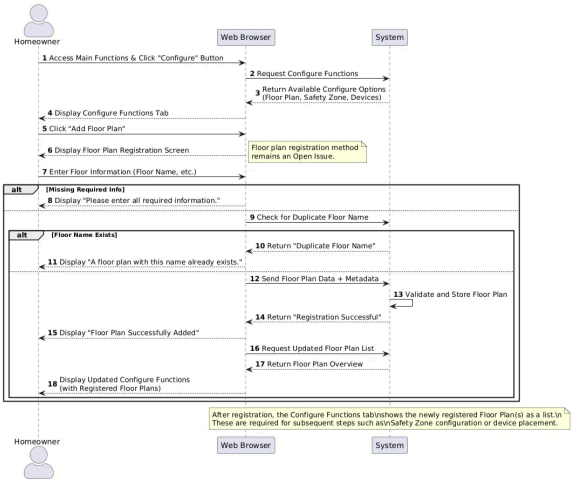
f. Access system with Temporary Password (Guest Login)



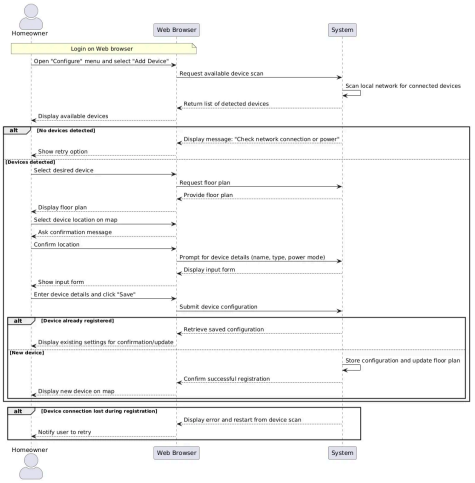
g. Log out / Revert Zones (Guest Logout)



h. Configure floor plan through Web browser

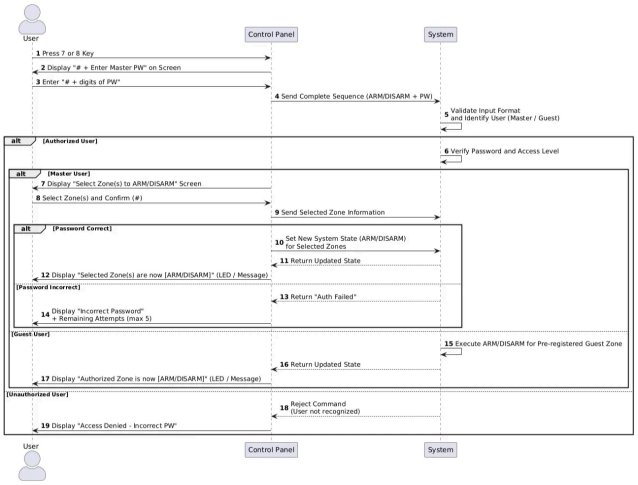


i. Add device through Web browser



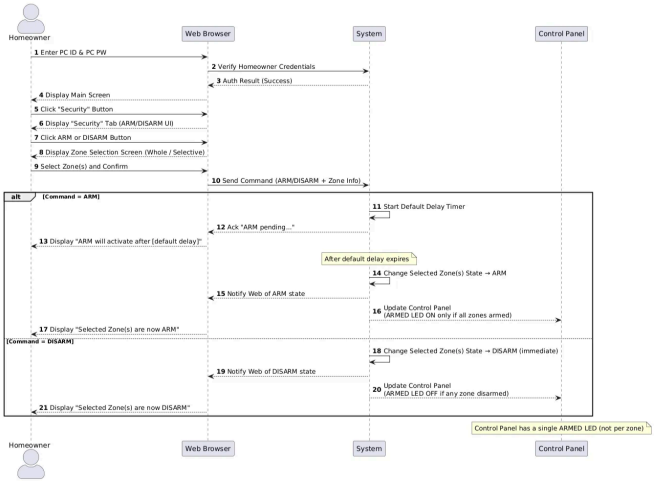
2. Security **Sequence Diagram**

a. Arm/disarm system through control panel

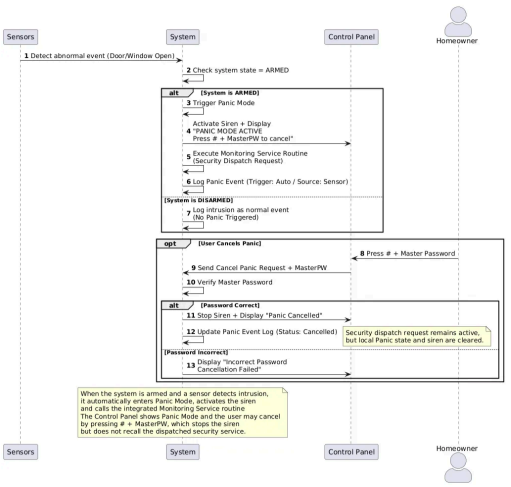


*The changes here will also affect **SRS VII-4-5 – Apply Home Management Mode via Control Panel**

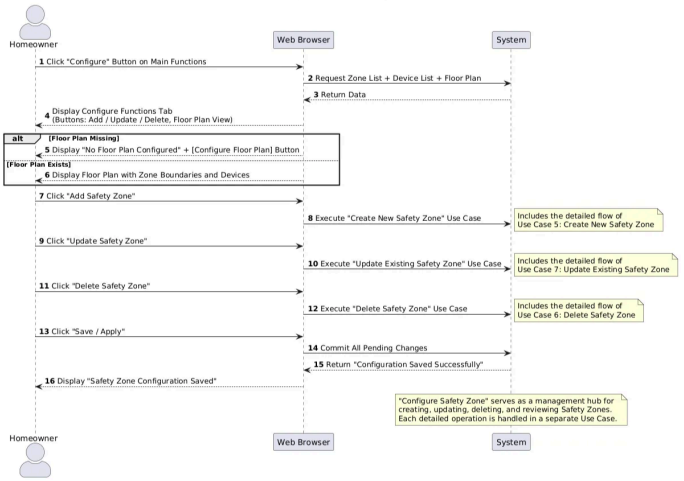
b. Arm/disarm system through web browser



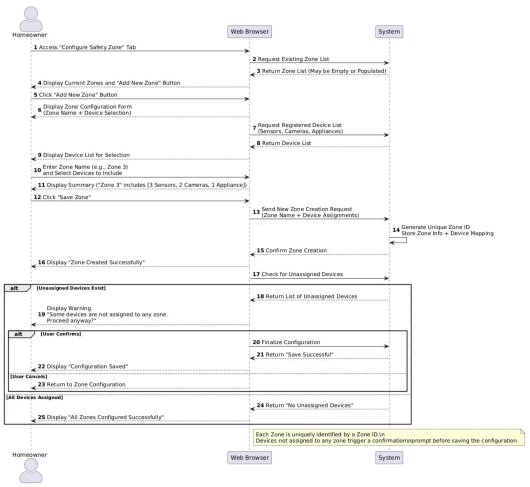
c. Alarm condition encountered



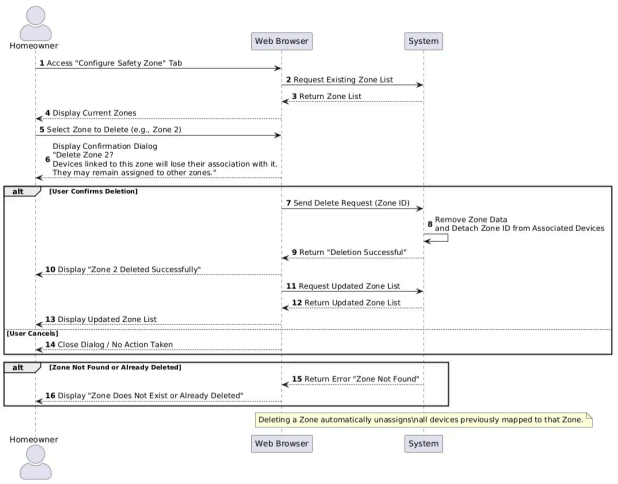
d. Configure Safety Zone



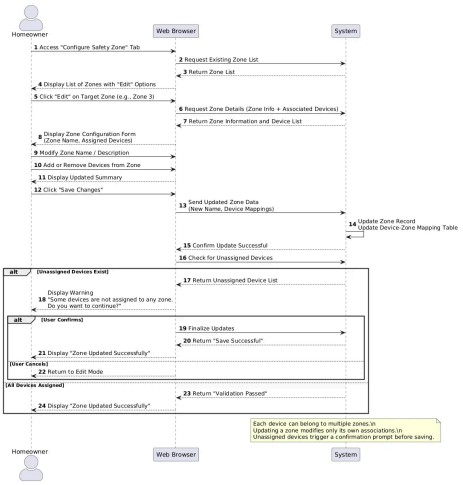
e. Create new safety zone



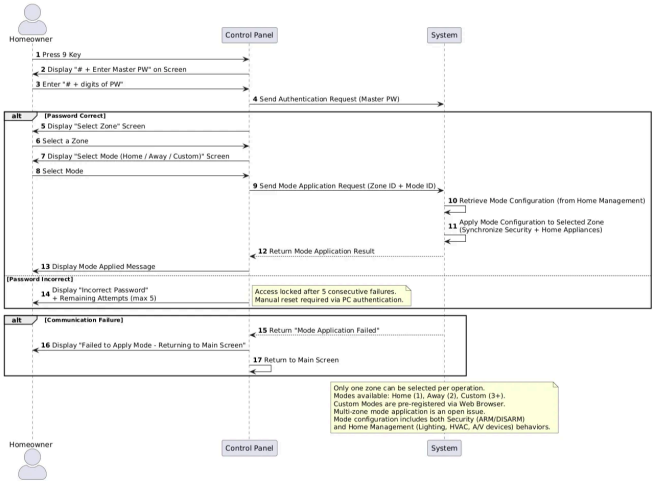
f. Delete Safety zone



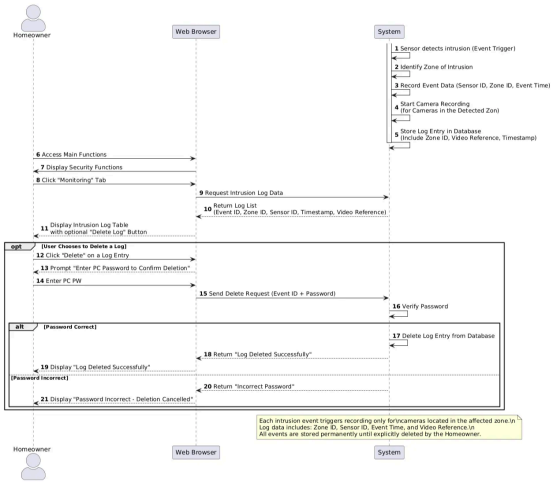
g. Update an exist safety zone



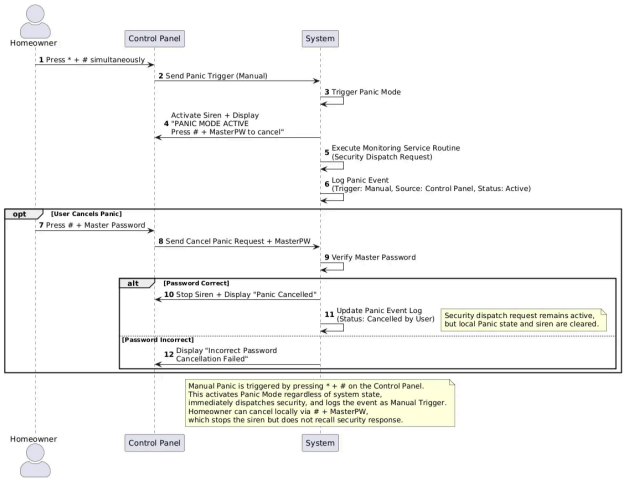
h. Configure Safehome modes



i. View intrusion log

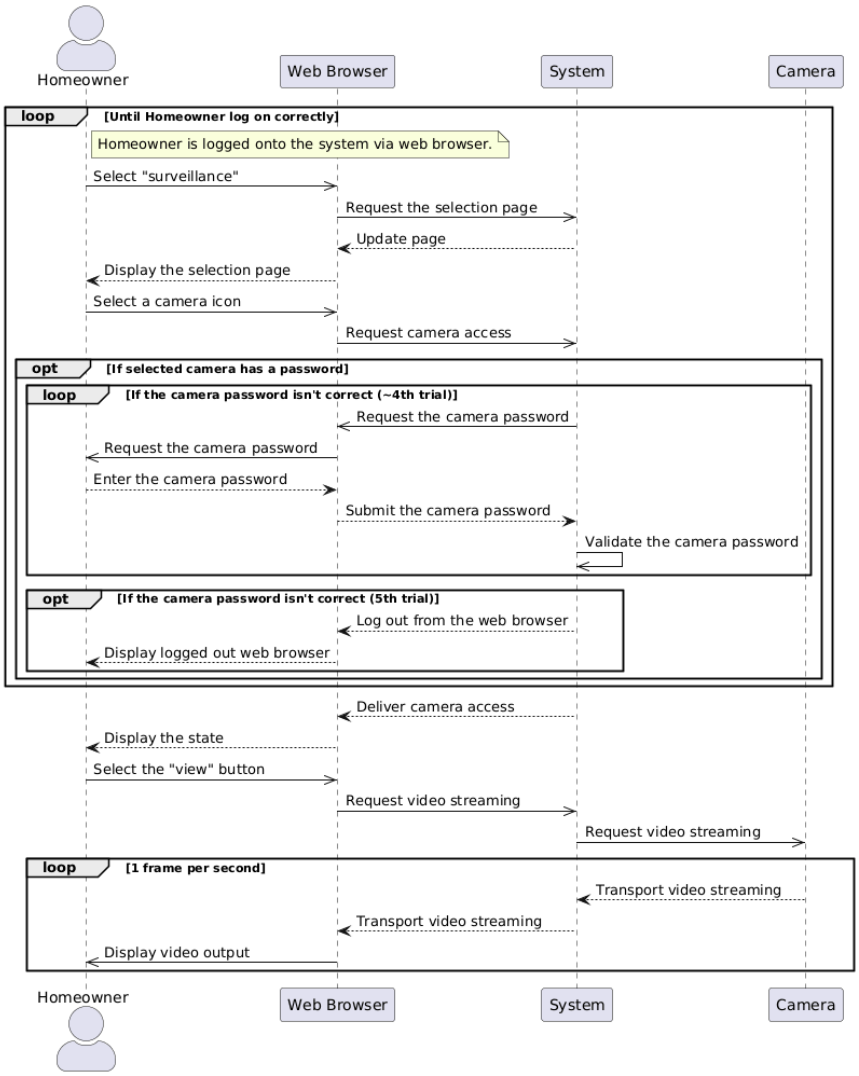


j. Call monitoring service through control panel

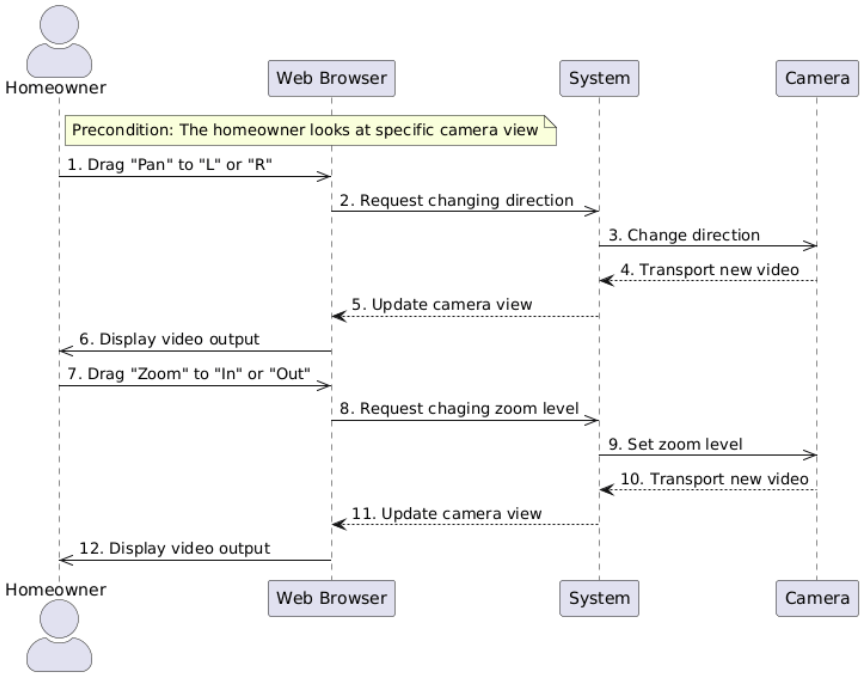


3. Surveillance **Sequence Diagram**

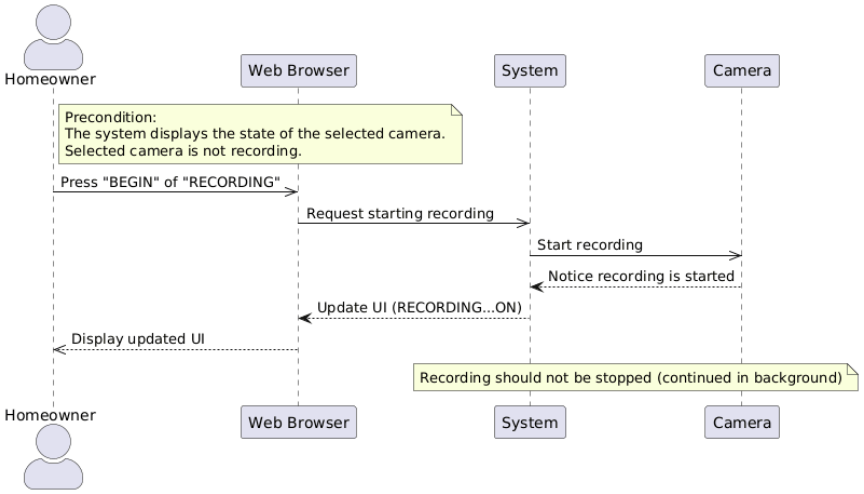
a. **Display Specific camera view**



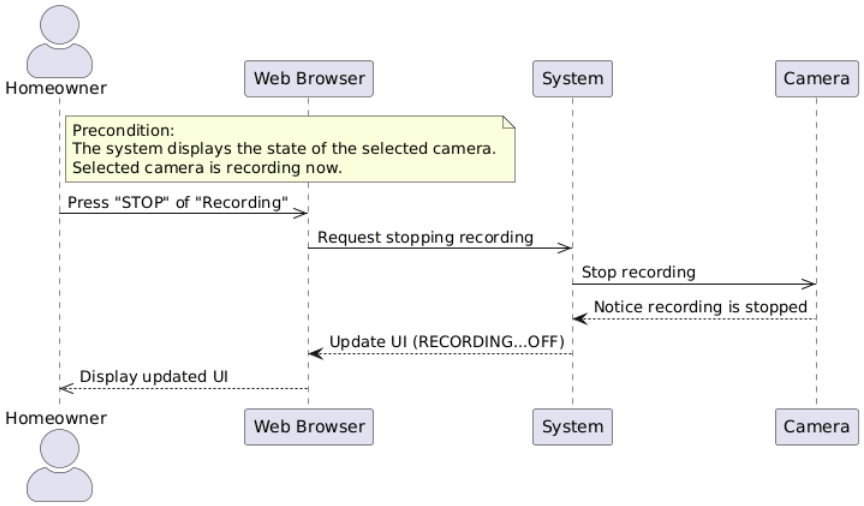
b. Pan/Zoom specific camera view



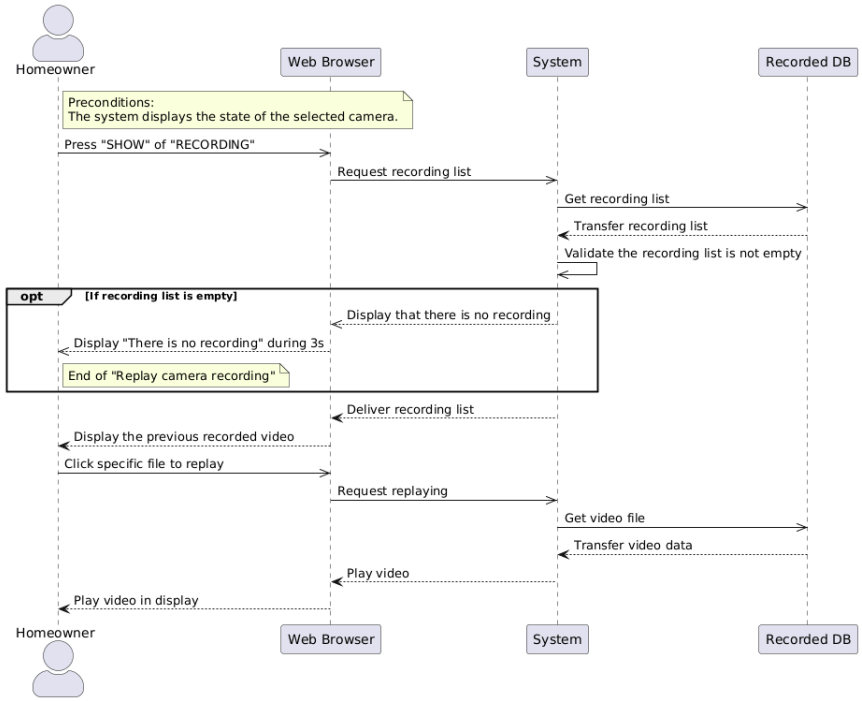
c. Begin camera recording



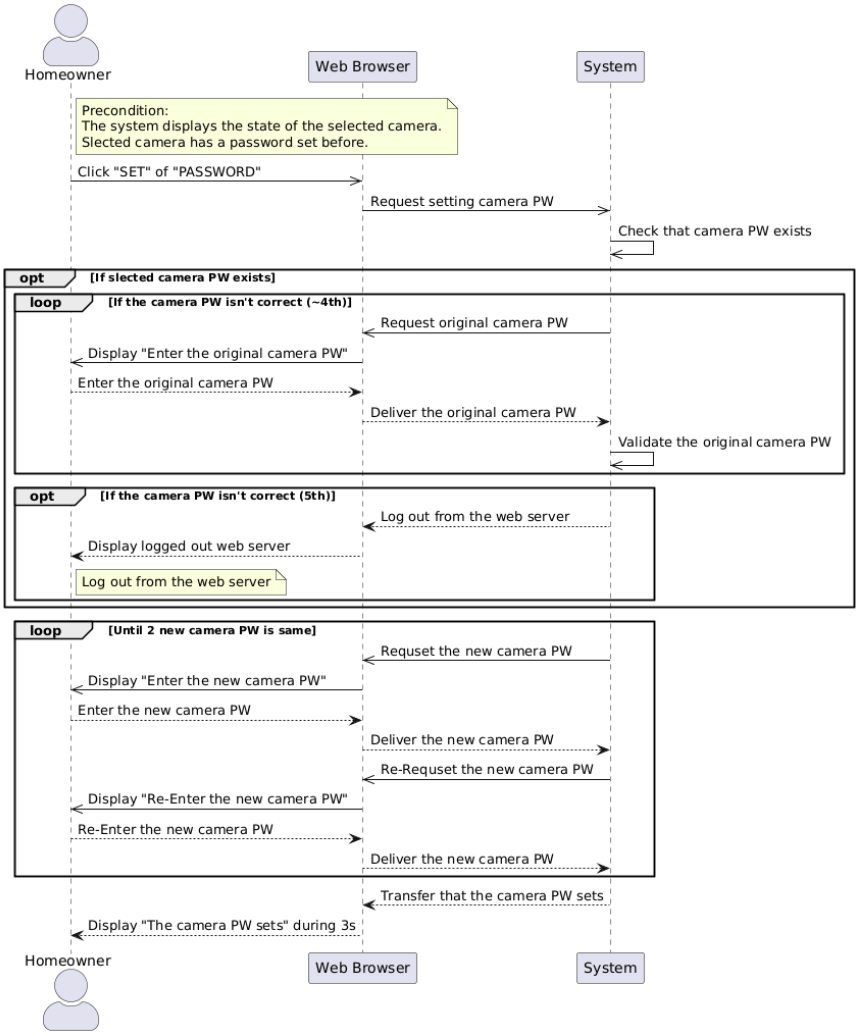
d. Stop camera recording



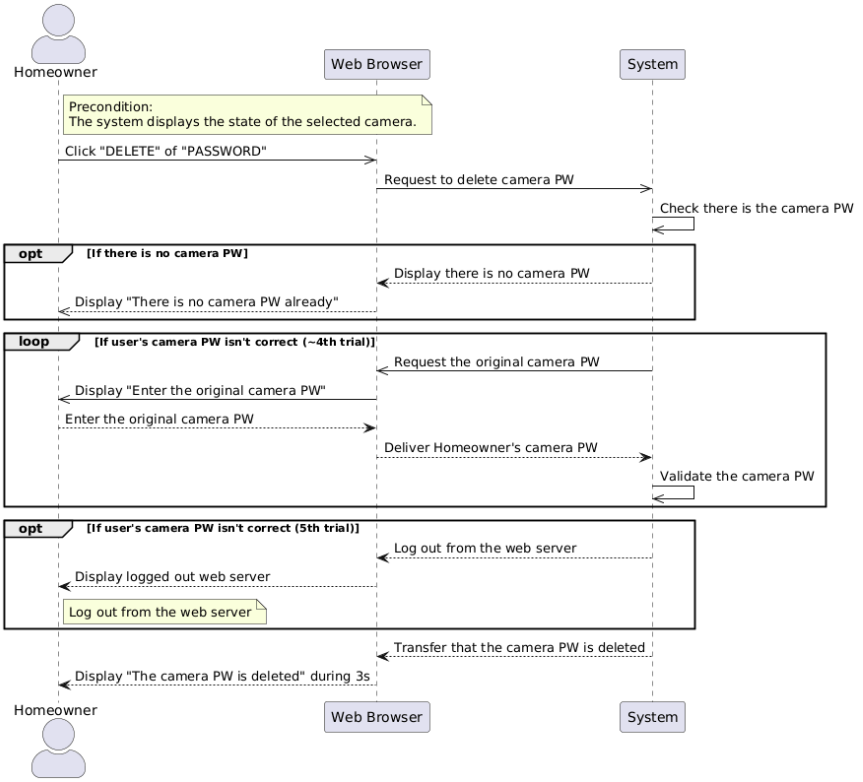
e. **Replay camera recording**



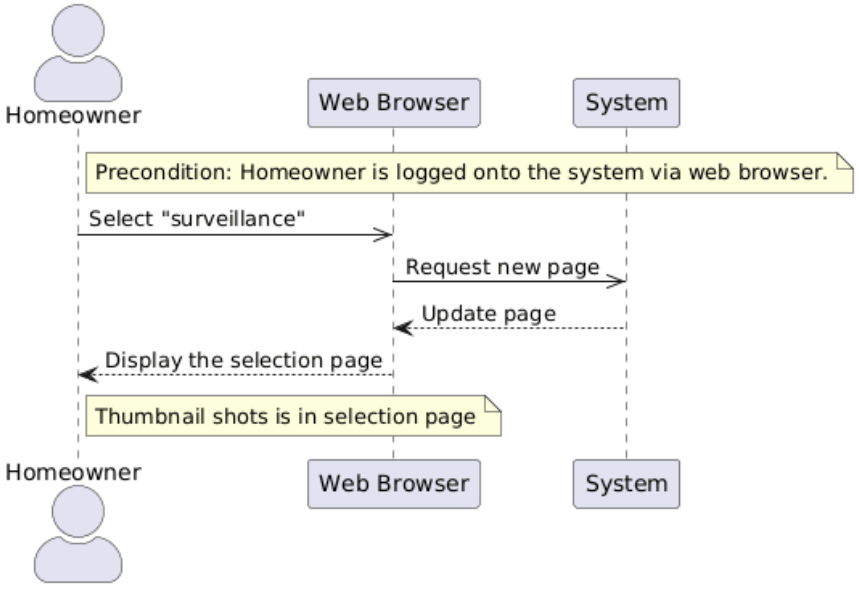
f. **Set camera password**



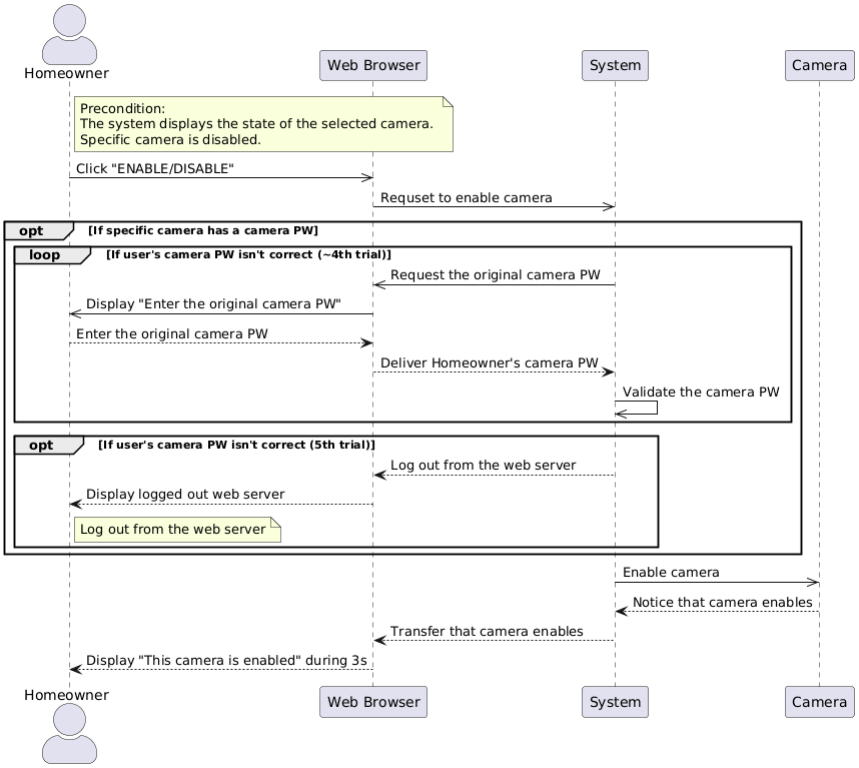
g. **Delete camera password**



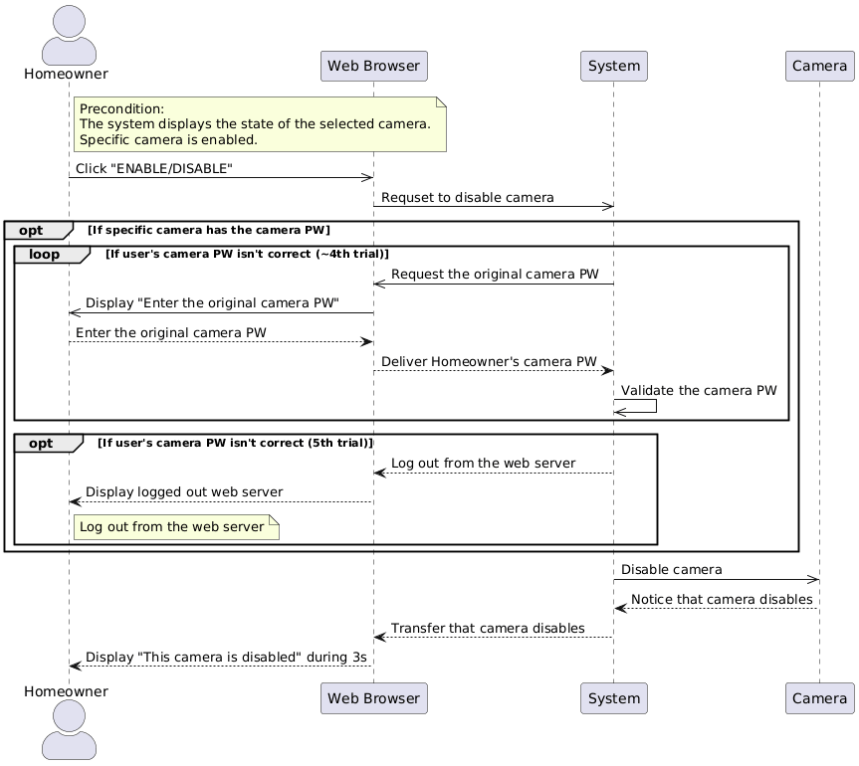
h. **View thumbnail shots**



i. **Enable camera**

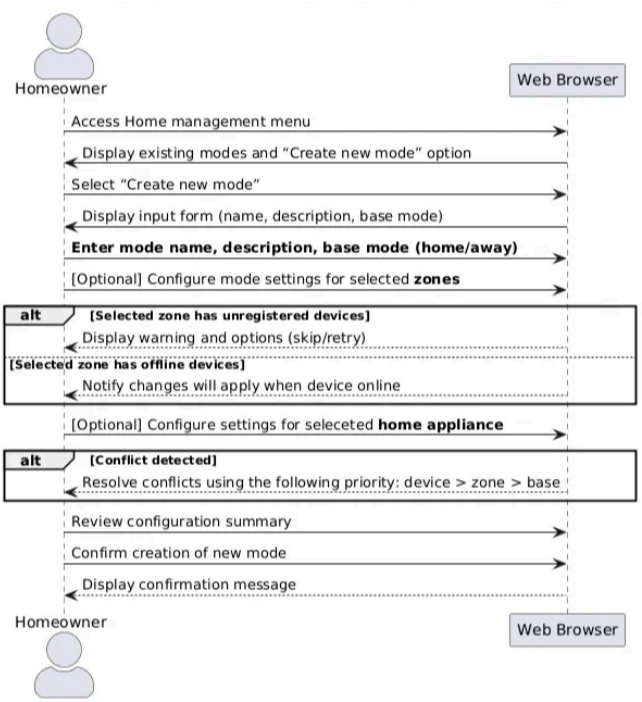


j. **Disable camera**



4. Home management **Sequence Diagram**

a. Create a new Home management mode on web browser

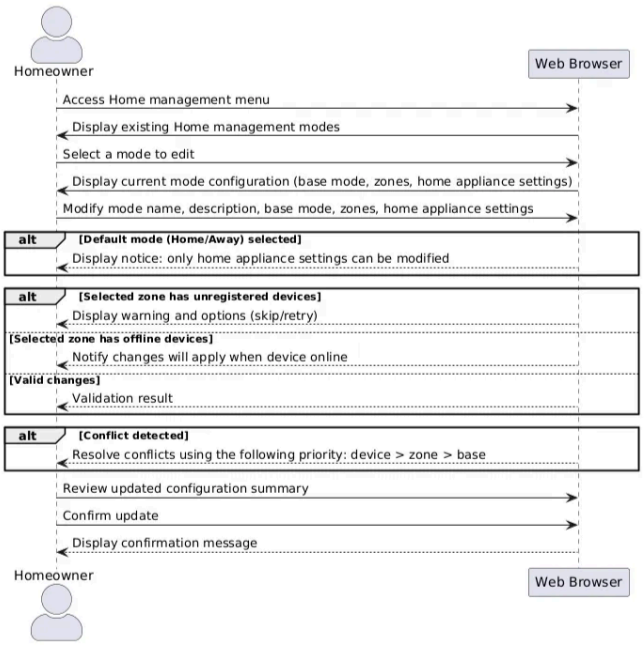


*By default, Home/Away and random schedule modes(for overnight travel & extended travel) are provided, as

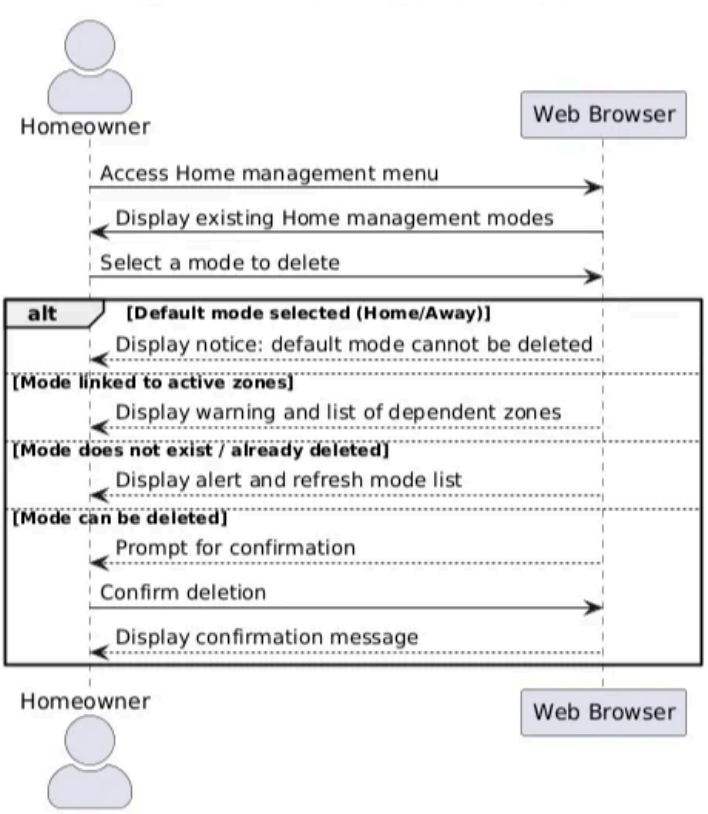
Referenced in the SafeHome dialog (slide 39).

Reference in Second Meeting log 2025.Oct.27 - Randomized lighting control logic (9 AM–9 PM random intervals)

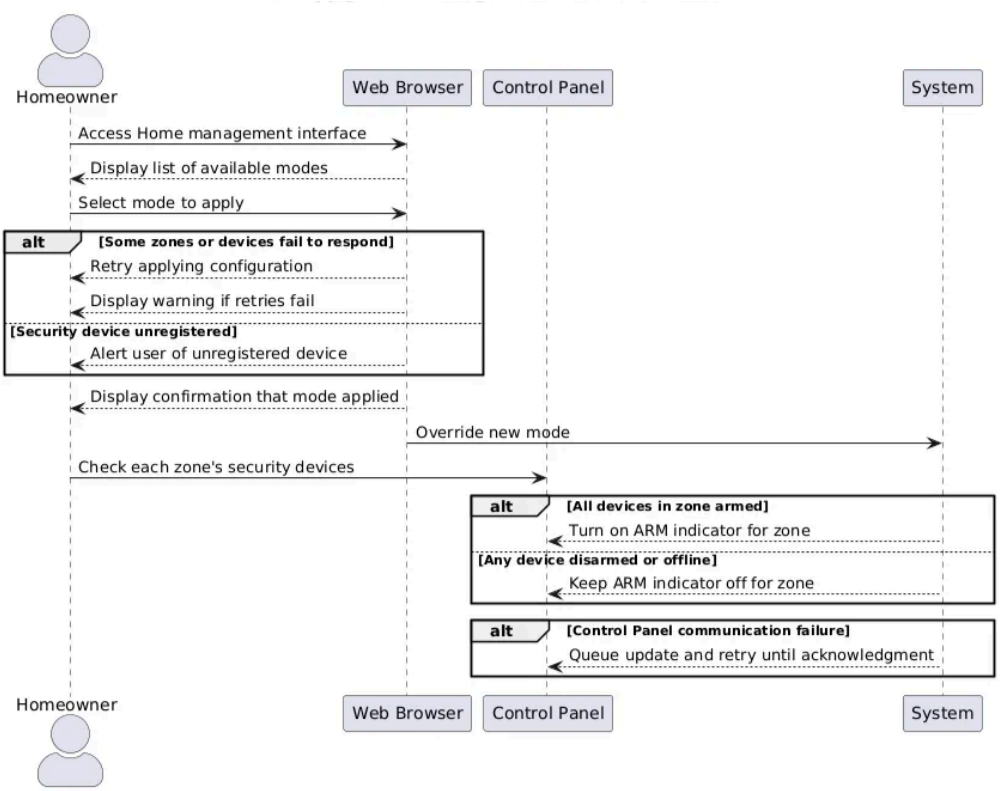
b. Update Home management mode



c. Delete home management mode

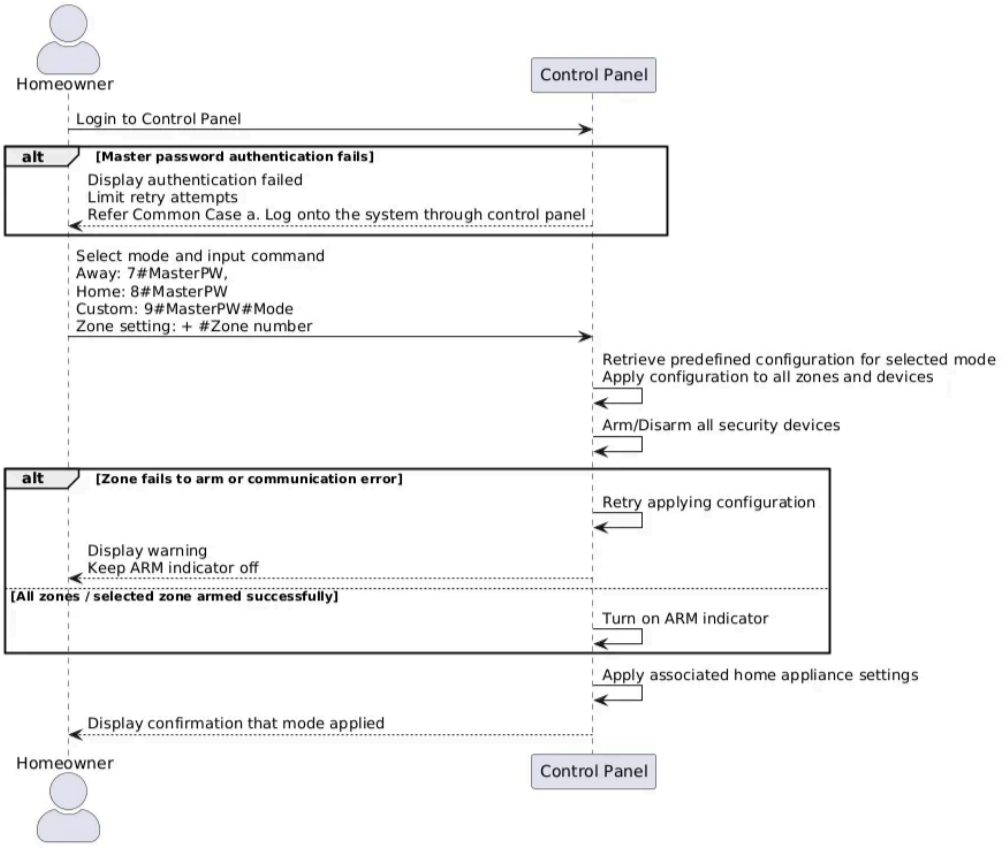


d. Apply Home management mode to all zones

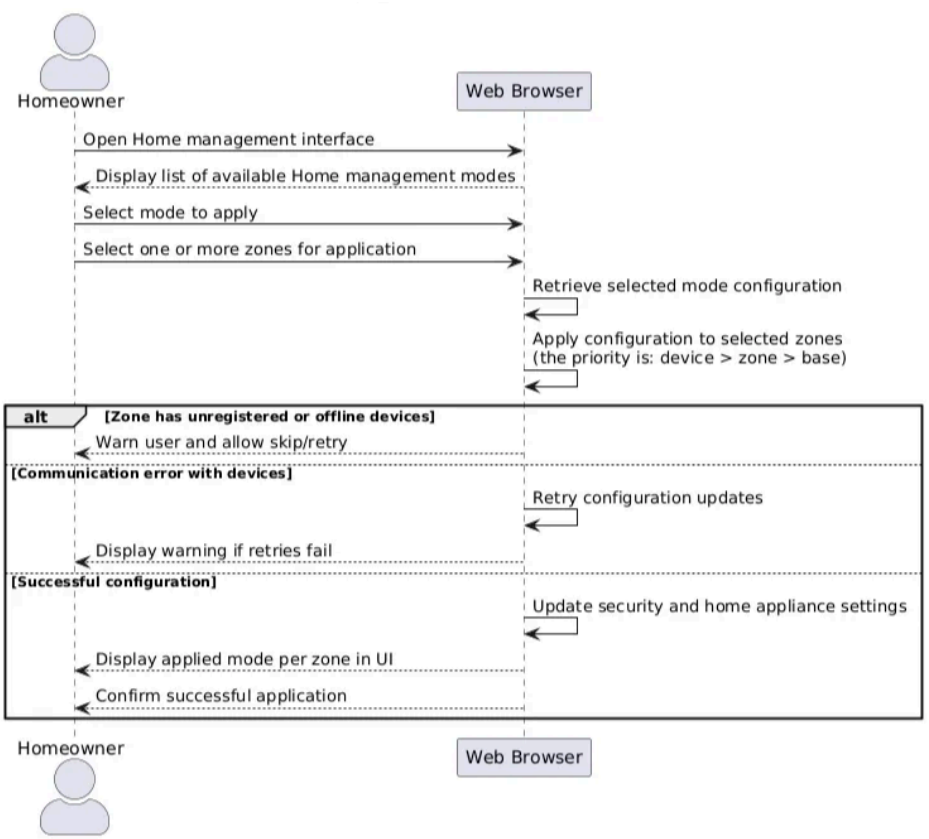


Reference in SafeHome dialog slide: slide 39

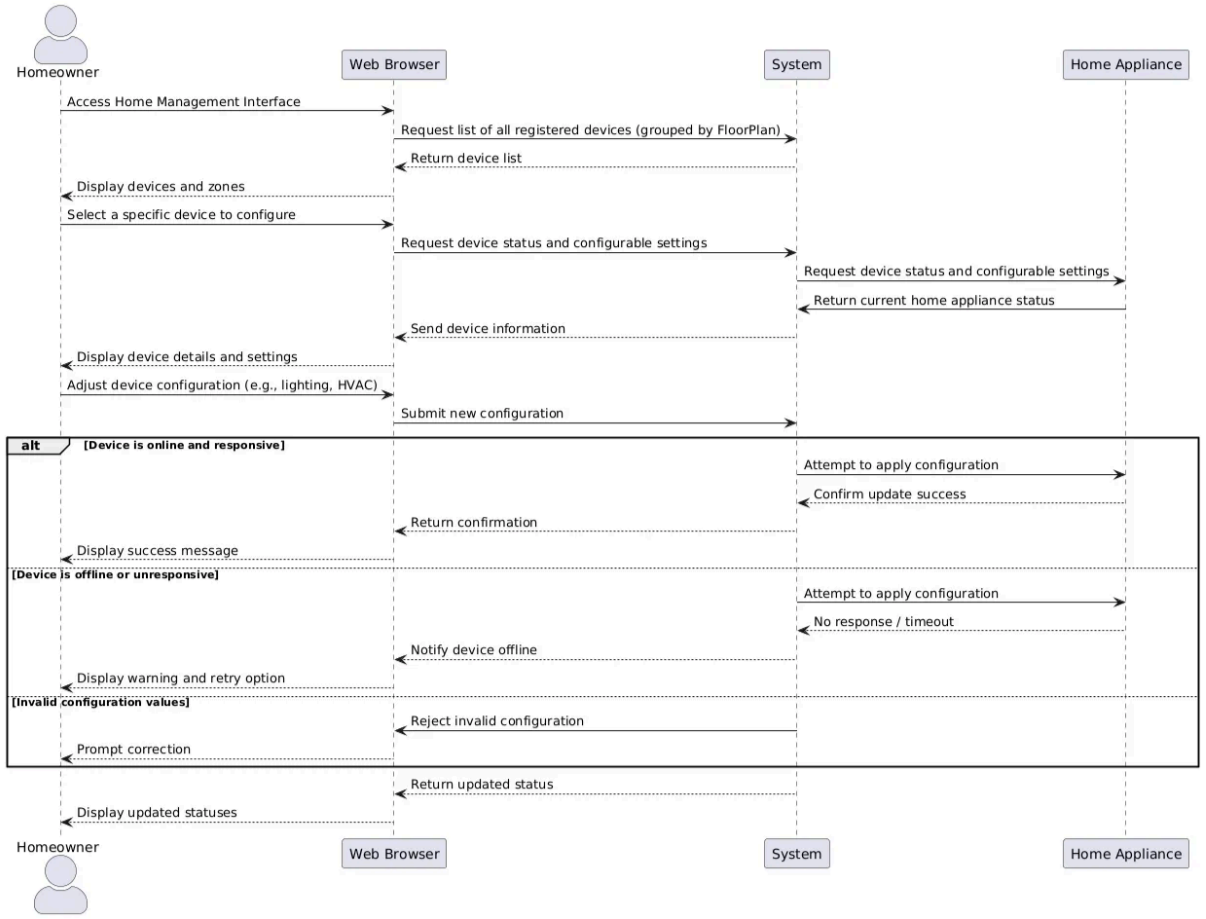
e. Apply Home management mode via Control Panel



f. Apply Home management mode to selected zones via Web Browser

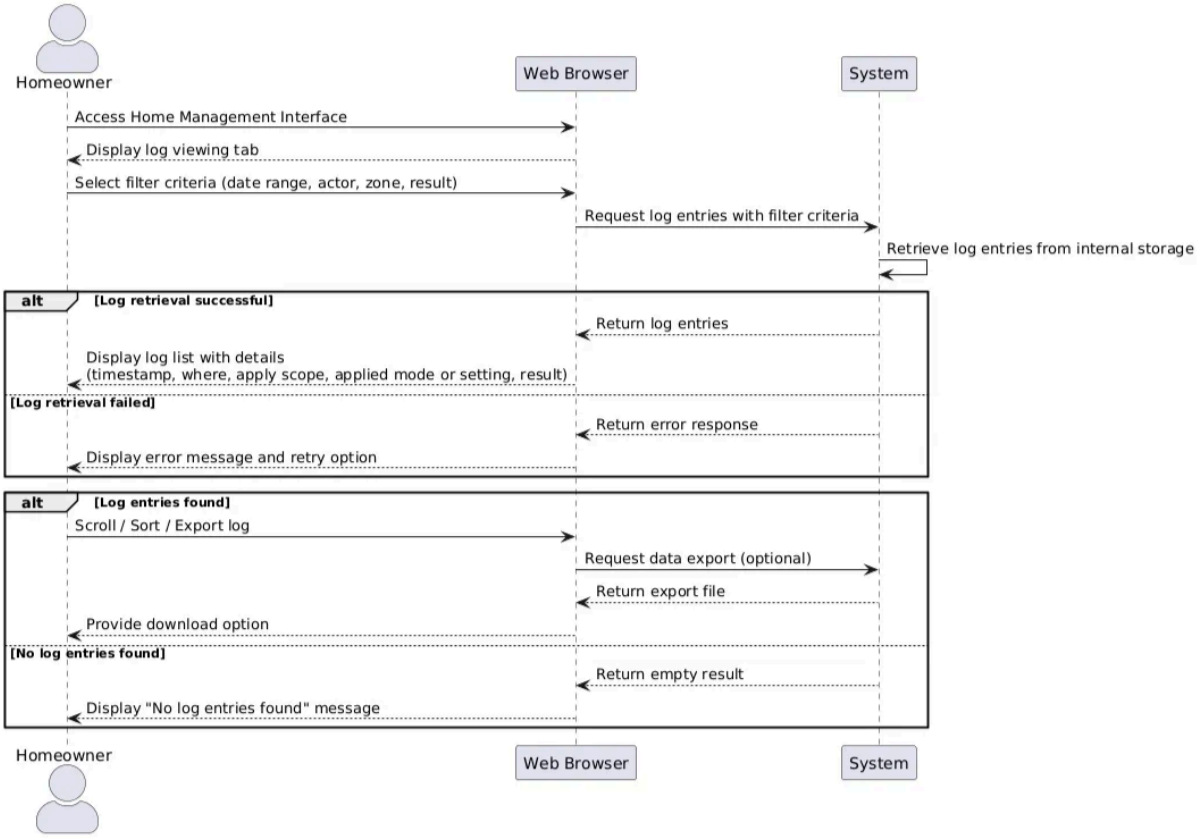


g. Configure Individual Devices via a Web Browser



Reference in SafeHome dialog slide: slide 38-39

h. View Home Management Mode Setting log via a Web Browser



VIII. Who did what

Collaborative Effort

- We discussed ambiguous points and potential exception cases together.
- We put in significant effort, engaging in thorough discussions and critical evaluations to improve the requirement specification.
- Actively provided enthusiastic feedback on parts of the diagrams they did not personally create.

Sumin Lee(20200468)

- Defined detailed Security cases for the Common function.
- Adjusted the details of the Security sequence diagrams.
- Refined the Security use case diagram and identified relevant references.
- Recorded and summarized the meeting minutes.

Yeongjun Joo(20210623)

- Define detailed Surveillance cases for the Common function.
- Adjust details of the Surveillance sequence diagrams.
- Adjust details of the Surveillance use case diagram and locate relevant references.

Wonjoon Lee(20190480)

- Define detailed use cases for the Common function.

- Adjust details of the Common sequence diagrams.
- Adjust details of the Common use case diagram and locate relevant references.

Gyeongyeon Kim(20180048)

- Define detailed use cases for the Home Management function.
- Adjust details of the Home Management sequence diagrams.
- Adjust details of the Home Management use case diagram and locate relevant references.

IX. Meeting logs

1st Meeting

- **Date:** Oct 27(Mon), 2025
- **Duration:** 16:00 – 17:35 (approx. 95 minutes)
- **Location:** E9 Study Room 3B
- **Participants:** Gyeongyeon Kim, Wonjoon Lee, Sumin Lee, Yeongjun Joo
- **Recorder:** Sumin Lee
- **Meeting Agenda**
  1. Overall content review
  2. Review behavior for Common Use Cases
  3. Review behavior for Security Use Cases

Main Discussion Topics:

Definition of “core” module responsibilities within the system architecture

- Defined the **core module** as the unit directly controlling device actions such as alarms, lighting, and sensors.

Alarm state transition and sensor and camera linkage logic

- Reviewed the need for **exception handling** in alarm activation (e.g., communication loss, unregistered sensors).
- Discussed implementing a unified notification system for both **alarm events** and **system warnings** (e.g., storage, disconnection).

Handling of alarm-triggered camera recording

- Clarified that when an alarm is triggered, the linked cameras will start recording, and footage will be tagged with the alarm timestamp.
- Alarm-triggered camera recording to be implemented with timestamp tagging.

Clarification of zone alarm behavior in different modes / Mode hierarchy and inheritance

- Discussed that zone will exhibit different behaviors depending on mode type.
- Determined that mode settings should follow a **hierarchical inheritance** (System → Zone → Device), with device-specific overrides allowed when necessary.

Storage notification and policy for recording / Exception handling and user notification for storage limits

- Decided that the system should **notify the user once storage usage reaches 80%**, and when storage is full, new footage should not be saved until space is cleared.

- Storage warning notification at 80% capacity to be added.

Synchronization between security mode and automation mode / Integration of lock, lighting, and temperature sensors within alarm response

- Proposed adding linkage between lighting and alarm events to enhance response visibility.

Functionality and communication of the Panic button

- Agreed that the **Panic button** must only activate during a security incident and communicate status changes to the UI in real time.

2nd Meeting

- **Date:** Oct 27(Mon), 2025
- **Duration:** 19:07 – 20:24 (approx. 77 minutes)
- **Location:** E9 Study Room 4B
- **Participants:** Gyeongyeon Kim, Wonjoon Lee, Sumin Lee, Yeongjun Joo
- **Recorder:** Sumin Lee
- **Meeting Agenda**
  1. Review behavior for Surveillance Use Cases
  2. Review behavior for Home Management Use Cases
  3. Assignment of roles and responsibilities
- **Action Items**
  1. Wonjoon Lee: Create Common Use Case Diagram, write Common Use Cases, create Common Sequence Diagram
  2. Sumin Lee: Create Security Use Case Diagram, write Security Use Cases, create Security Sequence Diagram
  3. Yeongjun Joo: Create Surveillance Use Case Diagram, write Surveillance Use Cases, create Surveillance Sequence Diagram
  4. Gyeongyeon Kim: Create Home Management Use Case Diagram, write Home Management Use Cases, create Home Management Sequence Diagram

Main Discussion Topics:

Camera related functionality and policy

- Clarification of camera view snapshots at **1 frame per second**
- Clarified that **Thumbnail View** displays live, distinct from the floor plan view, which visualizes sensor and camera placement.
  - Established that password-protected cameras display **blurred thumbnails with a lock icon** until authentication is completed.
- Continuous recording vs. event-triggered recording and related storage policy
  - Agreed that cameras will operate under **continuous recording**, while users can selectively enable or disable recording through a **Begin/Stop interface**.

Password: setting, validation, and retry limit policies and confirmation steps / Handling of password input errors, retry count, and system responses (system lock, logout, or timer delay)

- Setting: enter and confirm password twice

- Deletion: verify existing password once before removal
- Incorrect attempts trigger retry limit and optional delay
    - Confirmed **5-attempt retry limit**, after which access is locked for a defined cooldown period (similar to smartphone behavior).
    - Considered but rejected physical reset options for security reasons; access reset must occur through PC login authentication.
    - Finalized rule that all cameras and control panels require password re-entry after session logout.

Storage warning and recording halt logic when reaching 80% capacity

- Determined that when storage utilization reaches **80%**, the system will issue a warning; when full, new footage will not be saved.
- Decided that storage status and alerts will be displayed on the **Control Panel or PC dashboard**, with storage percentage indicators for user awareness.

User-defined mode customization enabled (e.g., Extended Travel) under Home Management module

- Synchronization of lighting, HVAC, and multimedia devices
- **Arm/Disarm functions** in the **Control Panel** should be synchronized with “Home/Away/Stay” modes for consistency, but remain logically separable in implementation.
- Determined that lighting and temperature control under Home Management are independent of the alarm system but may operate concurrently under shared modes.
    - i.e. **randomized lighting control logic** (between 9AM ~ 9PM) for occupancy simulation during Travel modes.
- Established that **Home Management** module controls all connected devices (lighting, HVAC, A/V equipment), while **Security Module** manages sensors, cameras, and alarms.
- Agreed that the system should support **custom user-defined modes**, such as “Extended Travel,” allowing users to configure device behaviors per mode.
- Discussed that pre-defined templates (e.g., Home, Away) will be provided, but users may add or modify modes through the Web browser interface.

3rd Meeting

- **Date:** October 30(Thu), 2025
- **Duration:** 19:09 – 20:33 (approx. 84 minutes)
- **Location:** E9 Study Room 4B
- **Participants:** Gyeongyeon Kim, Wonjoon Lee, Sumin Lee, Yeongjun Joo
- **Recorder:** Sumin Lee
- **Meeting Agenda**
    1. Progress check and review for each member
    2. Terminology standardization

Main Discussion Topics:

Term standardization

- System Manger, System Controller, System, etc → ‘System’ for clarity and consistency across all sequence diagrams

    - Include Authentication Module, Mode Manager, Configuration Storage, Sensor Controller and Camera Controller
        - **Authentication Module** as the component responsible for validating credentials using data retrieved from **Configuration Storage**, which functions as the system database for both master and guest users
        - **Mode Manager** handles custom mode configurations and applies hierarchical control (System → Zone → Device)
        - **Sensor Controller** and **Camera Controller** will manage respective devices, with cameras also linked to sensors for event-triggered recording.
- Homeowner/Guest, Web Browser → Merge to 'Homeowner/Guest'

Intrusion Log

- Handling intrusion log storage (sensor ID, time, zone, and corresponding camera footage)
- Intrusion logs will record **sensor ID, time, zone, and camera footage recorded at that time**, enabling traceability through the system.
- Access control for viewing and deleting intrusion logs
    - Users must log in to view intrusion logs, but password re-entry is only required when deleting logs.
- "View Intrusion Log" and "Call Monitoring Service" features placed under Monitoring tab.
- Clarified that the **"View Intrusion Log"** tab will be included under the **Monitoring** section in the Control Panel, along with **"Call Monitoring Service."**
    - **Call Monitoring Service** is the system's automatic call to a security company when the **panic button** is pressed, signaling an emergency event.
        - Both alarm and panic button behavior linked to calling monitoring service
    - Control Panel should display alert messages (e.g., intrusion detected, window open) along with an audible alarm when an intrusion occurs.

Minor User Experience

- The floor plan should default to the most recently accessed floor, or to the 1st floor upon initial entry
- Camera thumbnail view: thumbnails should automatically appear upon entering the main screen without requiring an additional click.

Appendix A. Glossary

Term	Definition	Notes
System	Central software and hardware framework of SafeHome that integrates all Control Panels, Web Interfaces, and connected devices.	Core of the SafeHome platform.
Homeowner	Primary registered user who has full administrative privileges to access, configure, and operate all SafeHome functions.	Main actor in most use cases.
Guest	Temporary user with limited access, authenticated by a Guest Password or expiration-based credentials.	Defined under "Manage Temporary Users."

Term	Definition	Notes
Control Panel	Wall-mounted or central console for local operation of SafeHome functions such as ARM/DISARM, mode selection, and monitoring.	Operates independently of network access.
Web Browser	Interface accessible from a network-connected device that provides remote configuration and control.	Used for setup and management.
Master Password (MasterPW)	Four-digit code used by the Homeowner for authentication on the Control Panel.	Stored securely in hashed form.
PC ID / PC PW	Login information (ID + password) used by the Homeowner to access the web interface.	Required for browser login.
Guest PW	Four-digit access code allowing limited access through the Control Panel.	
Mode / Home Management Mode	Preset configuration defining security and home appliance settings for the entire house, selected zones, or devices.	Examples: Home, Away, Custom.
Base Mode	Fundamental template from which other modes inherit default configurations.	Typically “Home” or “Away.”
Zone	Logical grouping of rooms, sensors, and devices defined within the floor plan.	Used for both security and management.
Device	Any controllable hardware component connected to the SafeHome system.	Must be registered to be controlled.
Camera	Surveillance device capable of real-time monitoring, recording, and replay.	Configured in Surveillance Use Cases.
ARM / DISARM	Security states where sensors are active (ARM) or inactive (DISARM).	ARM = monitoring on; DISARM = off.
ARM Indicator Light	LED light on the Control Panel showing whether all zones are armed.	On = all armed; Off = some disarmed or all disarmed.
Floor Plan	Visual layout of the home, used for zone mapping, camera placement, and device configuration.	Uploaded or drawn by the user.
Surveillance	Monitoring subsystem for viewing, recording, and replaying camera feeds.	Operates under System control.
Thumbnail Shot	Static preview image of a camera feed on the selection page.	Refreshed periodically.
Home Management Menu	Interface for creating and managing modes, schedules, and device settings.	Accessible via web browser.
Mode Application	Activation process of a Home Management Mode.	Applied globally or partially.
Device Mode / Zone Mode / Base Mode Hierarchy	Priority rule for applying overlapping configurations.	Order: device > zone > base.
Offline Device	Registered device that is currently unreachable.	Generates warning messages.
Unregistered Device	Device not yet added to the system registry.	Cannot be controlled.
Conflict Resolution Rule	Logic determining which configuration prevails during overlaps.	Based on hierarchy order.
Authentication	Validation of credentials before access.	Used for login, deletion, and mode control.
Validation	Logical check of data consistency or correctness.	Applied to all configuration actions.
Schedule Setting	Time-based automation (activate/deactivate modes or devices).	Example: lights on at 10 PM.

Term	Definition	Notes
Configuration Summary	Overview shown before confirming settings.	Used in create/update workflows.
Configuration Conflict	Inconsistent device or zone settings.	System resolves or alerts.
Confirmation Message	Notification of successful operation.	Standardized format.
Exception Handling	Defined behavior for abnormal or failure conditions.	Includes warnings, retries, or fallback.
Open Issue	Design question requiring further decision.	Listed at end of each use case.
System Lock	Temporary access restriction after repeated failed logins.	Default: 5 minutes.
Communication Failure	Error where commands can’t be delivered between modules.	Triggers retry or warning.
Data Storage / Database	Repository for configuration, mode, and recording data.	May be cloud-based.
Log / Mode Setting Log	Record of mode application history (actor, time, scope, result).	Used for auditing.
Audit / Auditing	Reviewing system logs for transparency.	Supports security monitoring.
User Interface (UI)	Display through which the user interacts with the system.	Includes web and panel UI.
System Restart	Automatic reboot after critical updates.	Used after password change.
Mode Number	Numeric identifier for predefined modes.	Used in Control Panel input.
Zone Number	Numeric identifier for specific zones.	Optional Control Panel input.
Actor	Entity performing an action (User, Guest, System, etc.).	Defined per scenario.
Increment	Development phase in which a feature becomes available.	First / Second increment.
Priority	Relative importance of a function.	High / Medium / Low.

Appendix B. Abbreviations

Abbreviation	Full Term	Description
ARM	Arm Mode	Security state in which all sensors are active.
DISARM	Disarm Mode	Security state in which sensors are inactive.
GUI	Graphical User Interface	Visual interface for user interaction.
HVAC	Heating, Ventilation, and Air Conditioning	System managing indoor temperature and airflow.
PW	Password	Code used for authentication.
UI	User Interface	Any interactive display or control screen.
LED	Light Emitting Diode	Indicator light used on the Control Panel.
ID	Identification	Unique user or device identifier.
LAN	Local Area Network	Internal home network connecting all devices.