CS350 Safehome Project
Software Requirement Specification (SRS)

Project Team #3 Members:

20240397	**Hichan Shin**
20240782	**Youngdo Han**
20240905	**Bumgyu Suh**
20240951	**Mohamed Elnakeeb**

Korea Advanced Institute of Science and Technology

Table of Contents

I. Overview

1. Introduction

SafeHome is an innovative home automation solution that focuses on giving its users robust control over their homes' security/surveillance systems.

The vision for SafeHome is to provide a comprehensive product line that extends beyond just security. While the initial version will focus primarily on home security—an area with immediate public interest—the system is designed for future growth. In subsequent releases, SafeHome will expand to include control over various home systems, such as lighting, heating, air conditioning, and entertainment devices, making it a fully integrated smart home platform.

SafeHome's wireless technology enables users to manage their homes remotely, offering enhanced accessibility and convenience. The first generation will cater specifically to security needs, but future versions will evolve to provide more automation and management features, positioning SafeHome as a universal solution for home automation.

2. Goal

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

Functional goal is to provide the followings:

1) Security functions
2) Surveillance functions
3) User System functions

Non-functional goal is as follows:

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

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

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

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

3. Major Functionalities

1) Surveillance Management

The surveillance functions in the SafeHome product let residents monitor their property through a unified, easy-to-use interface. Users can enter the Surveillance area from either the floor-plan view, where cameras appear as markers on the map, or the thumbnail grid, which presents recent snapshots for quick scanning. From either entry point, a user can open a specific camera view; the live stream is presented at a baseline of approximately 1 FPS to ensure consistent performance across typical home networks and devices.

Where hardware supports it, users can adjust the scene with PTZ controls (pan, tilt, and zoom) directly from the interface, making it simple to center on doors, windows, or other points of interest. For evidence capture and review, the system provides manual recording controls—users can start and stop a recording on demand, then replay captured footage using standard playback actions such as play/pause and timeline scrubbing.

Access and privacy are enforced at the per-user, per-camera level so that each person only sees the cameras they are authorized to view. Administrators have additional privileges to enable or disable individual cameras and manage how they appear within the interface. When a camera is unavailable, disabled, or the viewer lacks permission, SafeHome displays a clear placeholder state and message so users immediately understand why the live stream is not shown.

Together, these surveillance capabilities—ranging from quick entry via floor plan or thumbnails to precise PTZ control, recording, and controlled access—provide a reliable, privacy-preserving way to observe and review activity throughout the home.

2) Security Management

The security functions in the SafeHome product allow homeowners to monitor and manage all aspects of home security through the SafeHome Interface. Users can view the operational status of sensors such as door, window, and motion sensors, check their status, and review intrusion logs. Administrators have additional privileges to turn sensors on or off, create new safety zones, update existing ones, and configure how different zones respond under various security modes.

The system supports multiple security modes—such as Home and Away—that determine which sensors and zones are armed. Users with the appropriate permissions can switch between these modes at any time through the interface, enabling flexible protection based on occupancy and lifestyle. Administrators can

also define new security modes or modify existing ones to meet specific household needs.

When a sensor detects an event while the system is armed, SafeHome automatically triggers an alarm, displays an alert message, and notifies the homeowner through phone. Intrusion events are recorded in the system's log, which can be viewed, exported, or cleared by the administrator.

Through these comprehensive functions—ranging from sensor monitoring to zone management and intrusion response—the SafeHome Security Management system provides users with a robust, flexible, and easily accessible home protection solution.

3) User Management

The SafeHome User System is designed around a single administrator who manages all user accounts and access permissions through the SafeHome Interface. The admin can create, delete, and modify user accounts, assign or revoke camera access, and set user-specific passwords. Individual users can log in securely, update their own passwords, and register or edit phone numbers for connection with the security system.

This role-based approach ensures that only authorized users can access functions appropriate to their permissions, while the admin retains full control over user management. All changes are applied in real-time, providing secure, flexible, and efficient control over system access and user privileges.

II. Project Schedule

The project will proceed following the concept of incremental software development model. The security functions, surveillance functions and the user system 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. The first increment is to be done by the end of this year, 2025.

Plan for first increment

1.	Beginning of the project	Oct 20, 2025	
2.	Initial requirement gathering	Oct 24 – Oct 31	(7 days)
3.	SRS Review Meeting	Nov 3, 2025	
4.	Creating design model	Nov 4 - Nov 14	(11 days)
5.	Design Review Meeting	Nov 17	
6.	Implementation & testing	Nov 14 – Nov 22	(8 days)
7.	Testing & bug fixing	Nov 22 – Dec 1	(9 days)
8.	Test Review Meeting	Dec 10	
9.	First deployment	Dec 20, 2025 –	
10.	First presentation	Dec 22, 2025	

III. Prototype GUI

The SafeHome System can be accessed through the physical control panel installed that can be interacted with physically, or online, through the web. Both methods will share the same GUI for convenience and intuitive user experience.

Fig 1. Login menu

Fig 2. Select task

Fig 3. Surveillance dropdown

Fig 4. Configure dropdown

Fig 5. User profile

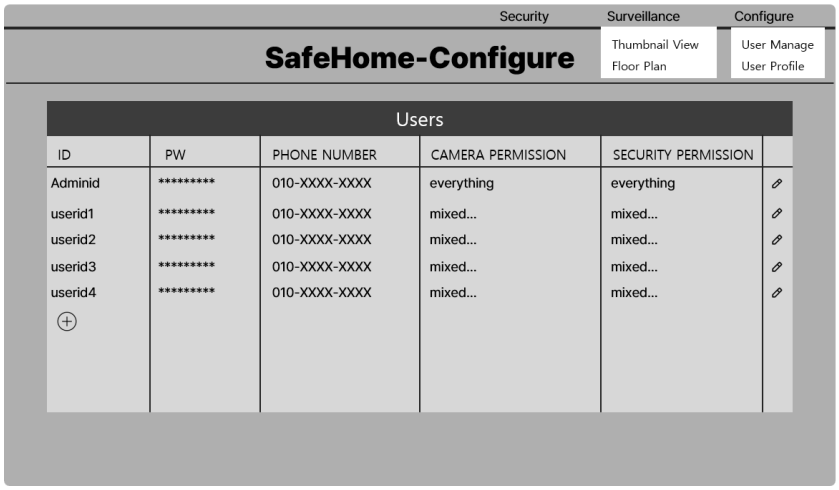


Fig 6. User manage

Fig 7. Add user

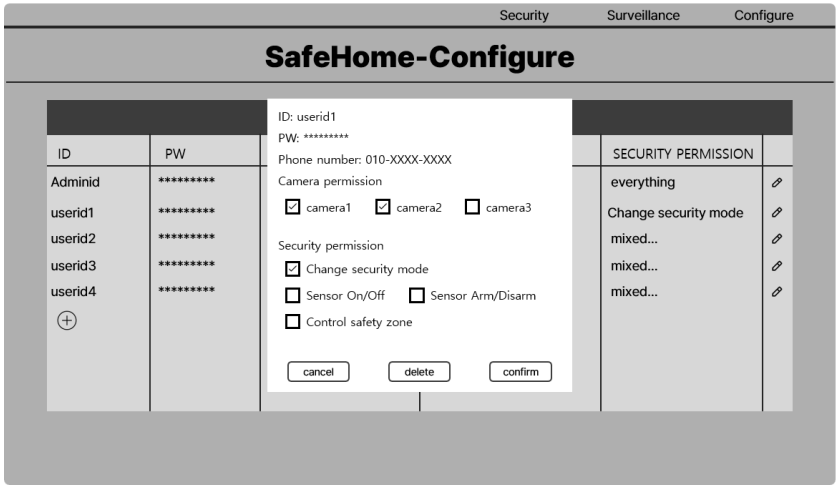


Fig 8. Edit user

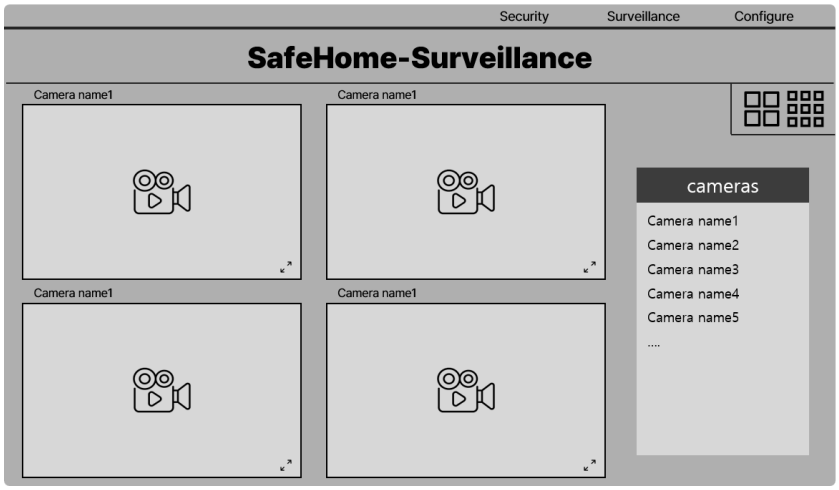


Fig 9. Thumbnail view

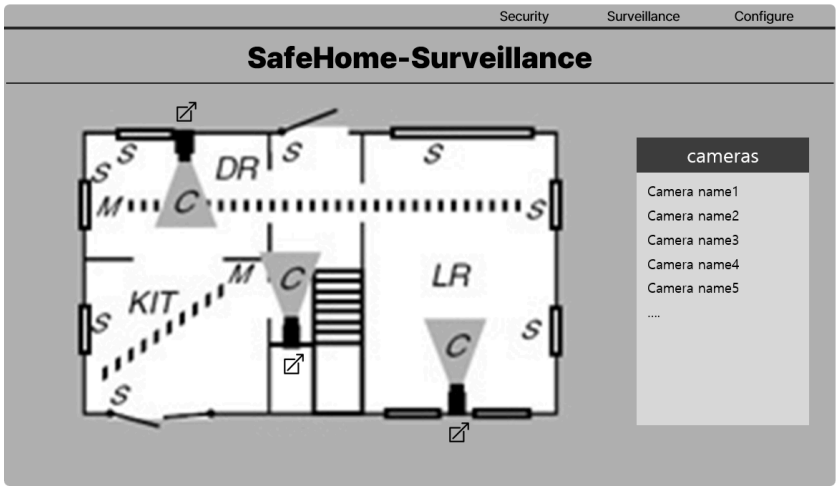


Fig 10. Floor plan

Fig 11. Specific camera

Fig 12. View recording

Fig 13. Disabled camera

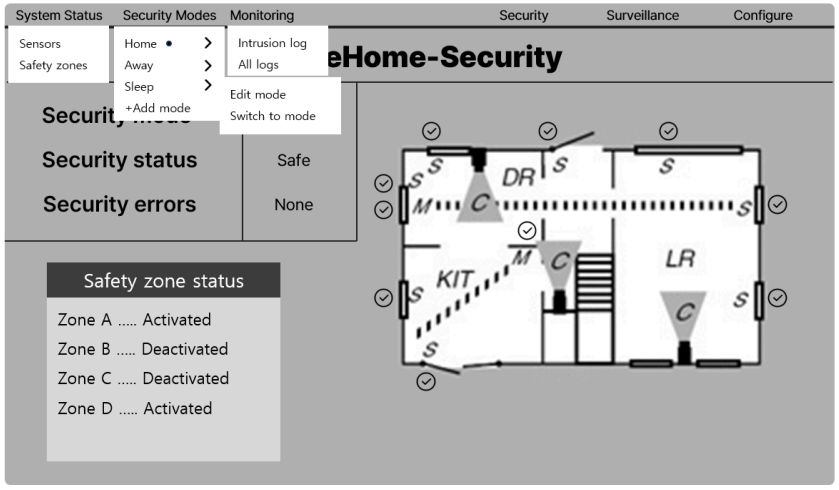


Fig 14. Security dropdown

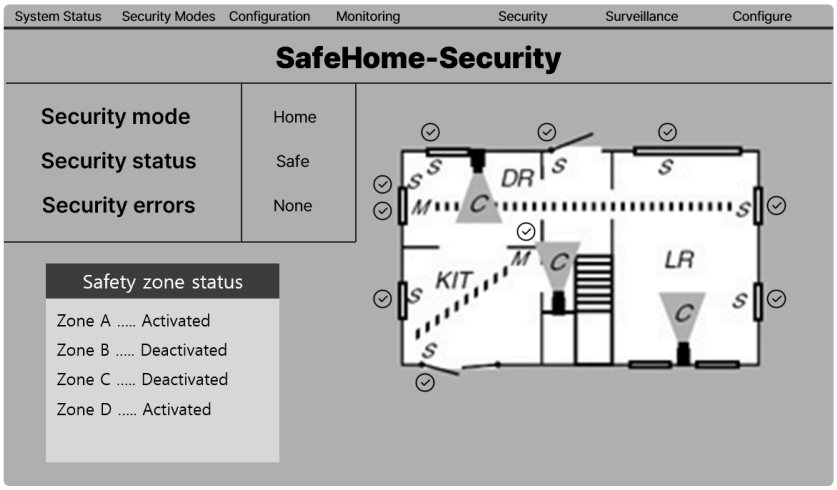


Fig 15. Security page

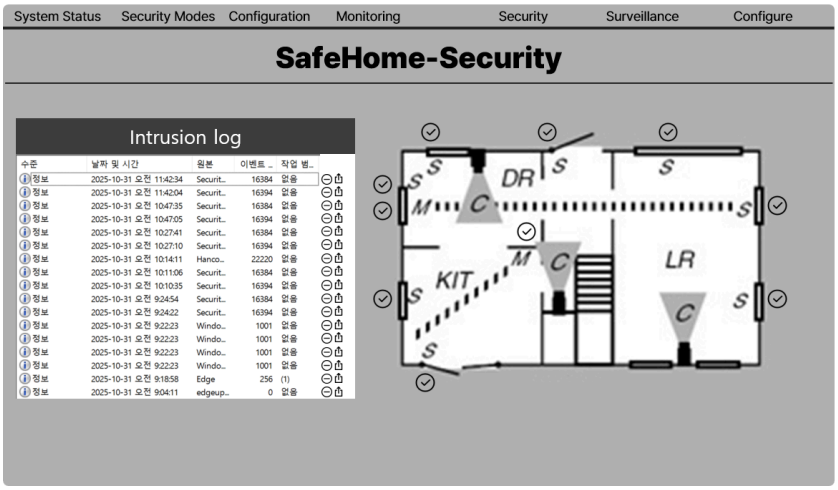


Fig 16. Intrusion log

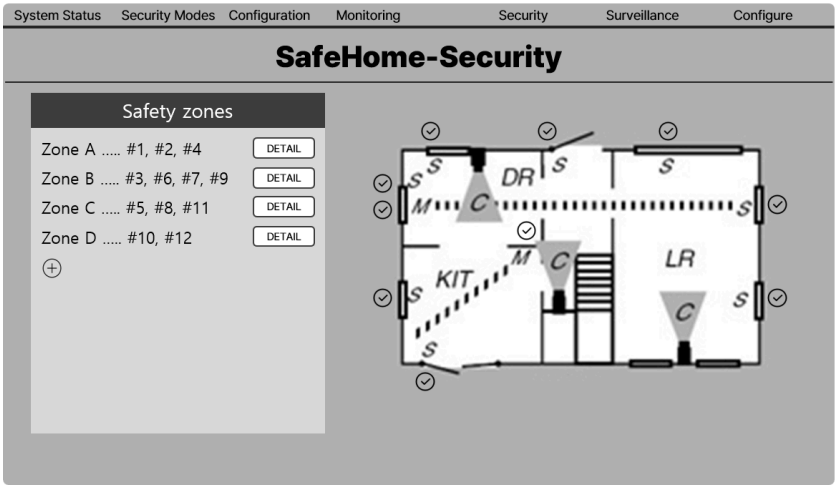


Fig 17. Manage safety zones

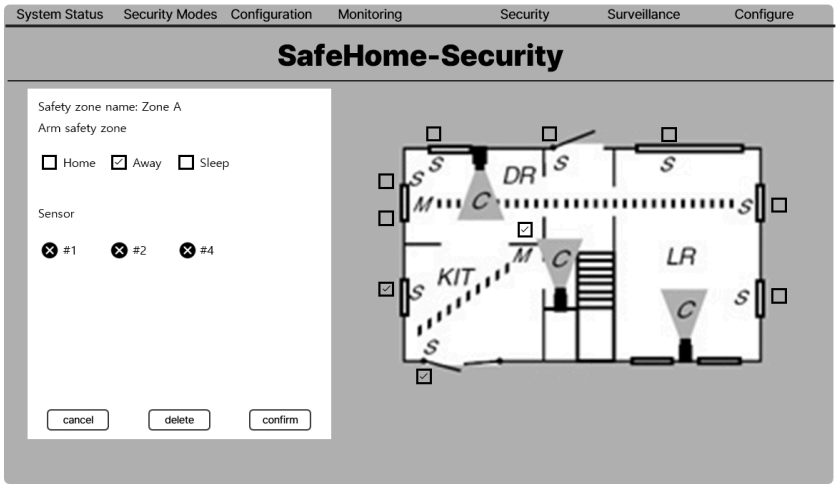


Fig 18. Safety zone detail

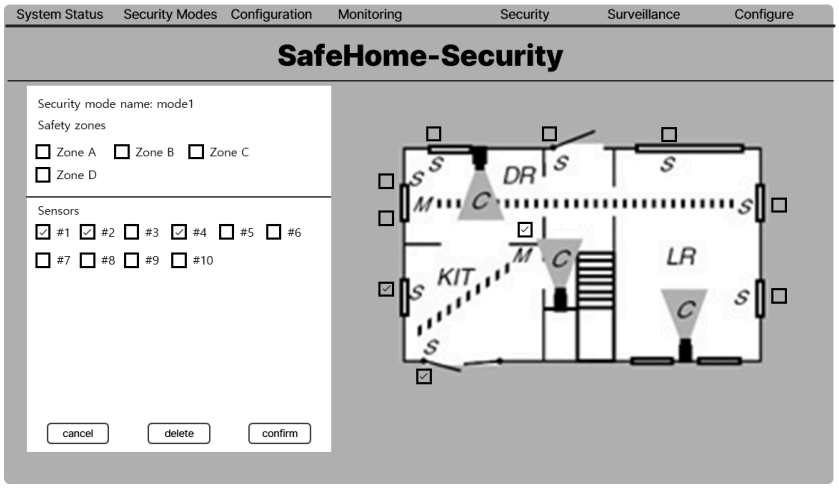


Fig 19. Edit security mode

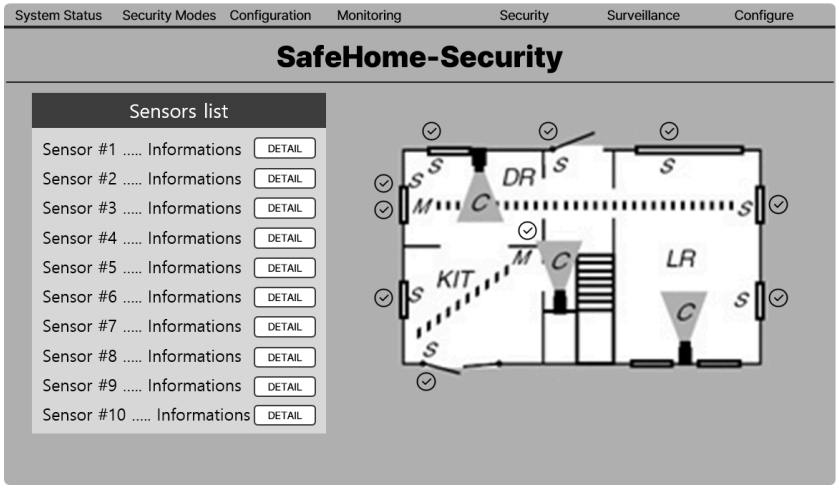


Fig 20. Sensor status

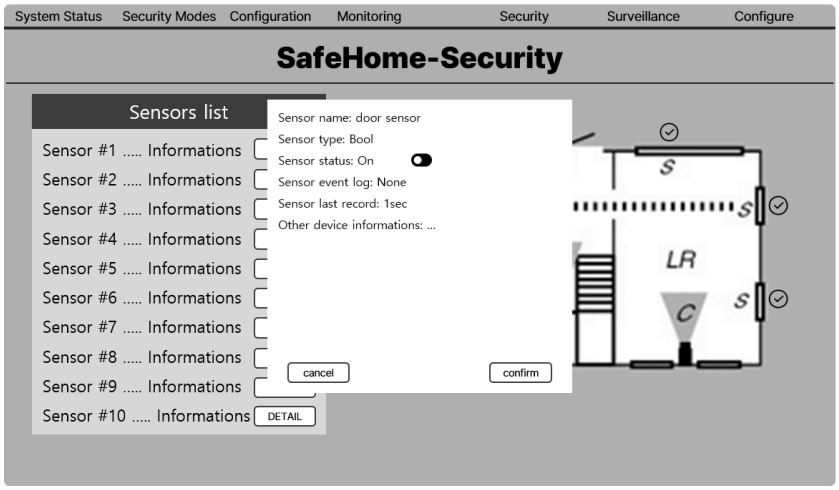


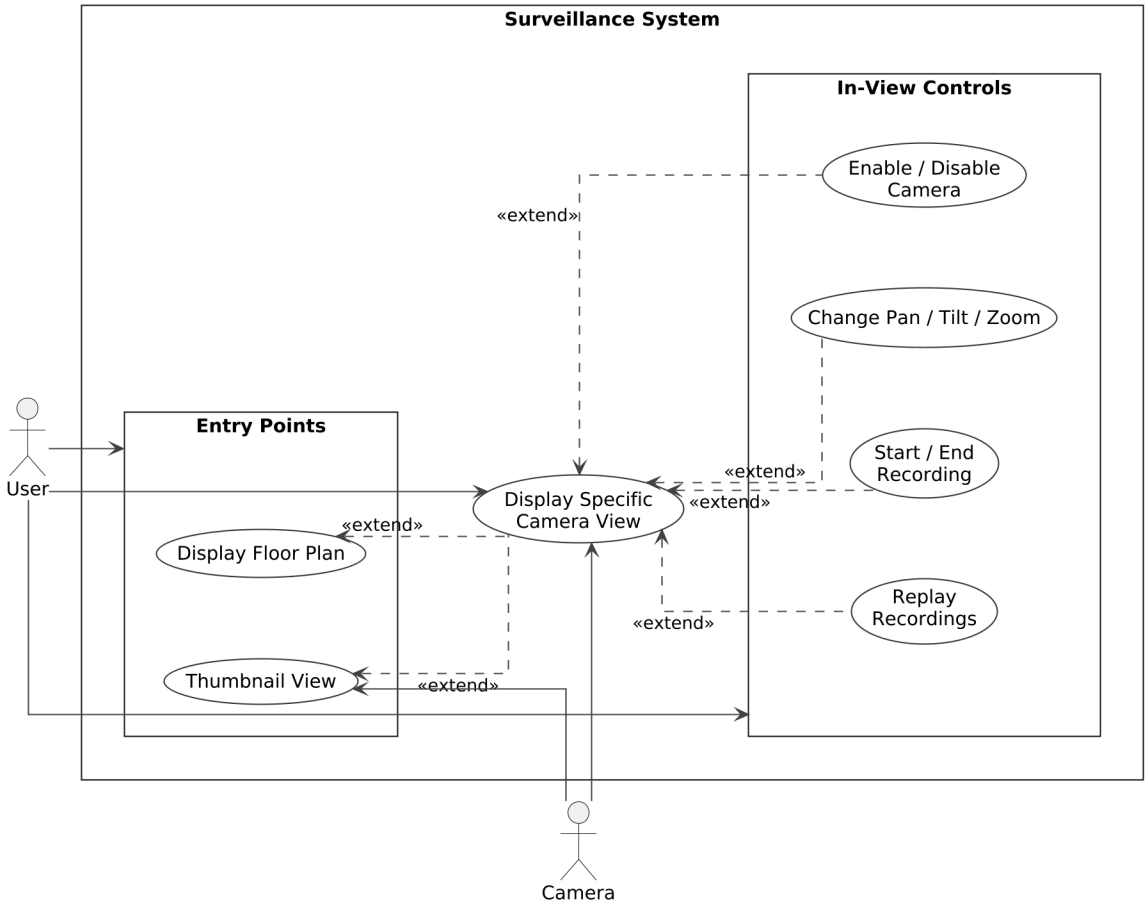
Fig 21. Sensor status detail

IV. Assumptions

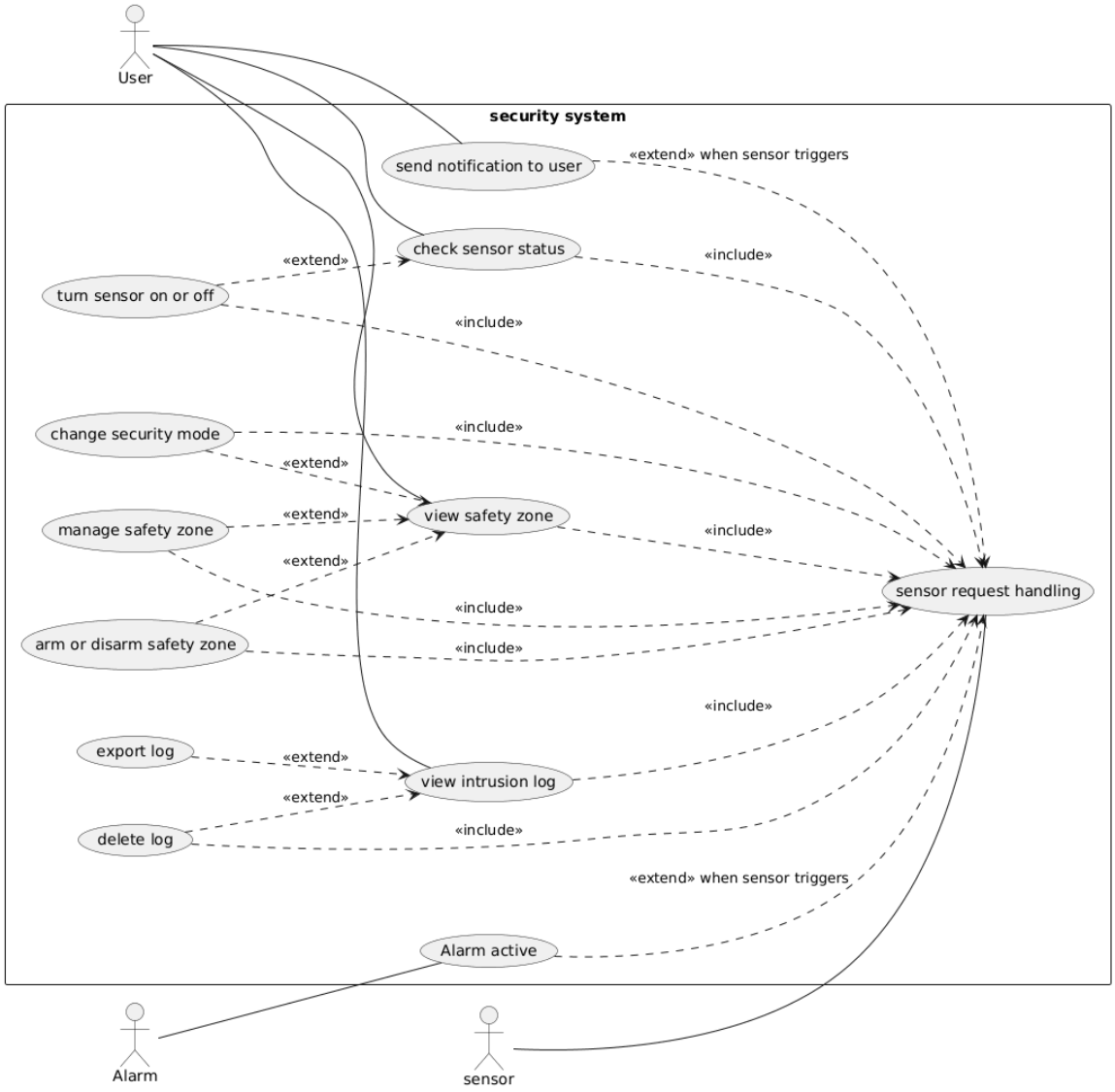
1. Floor plan configuration and hardware deployment is complete and out of the scope of our project.
2. When the SafeHome owner buys the product, the company sets up the floor plan (including the location of the SafeHome devices), so that this is set up already and is not changed through the SafeHome Software. Reconfiguring the floor plan or relocating/adding sensors or cameras are not in the scope of our project.
3. The SafeHome System can be accessed through the physical control panel installed that can be interacted with physically, or online, through the web. Both methods will share the same GUI for convenience and intuitive user experience.
4. The initial admin user already exists and so its ID and PW (password) is known by the appropriate person using SafeHome.
5. Cameras are IP-Based and may or may not support movement(zoom and pan)
6. SafeHome software runs on dedicated hardware installed.
7. Any issues related to the hardware, such as networking, power, or temperature settings, are outside of the scope of our project.

V. Use Case Diagrams

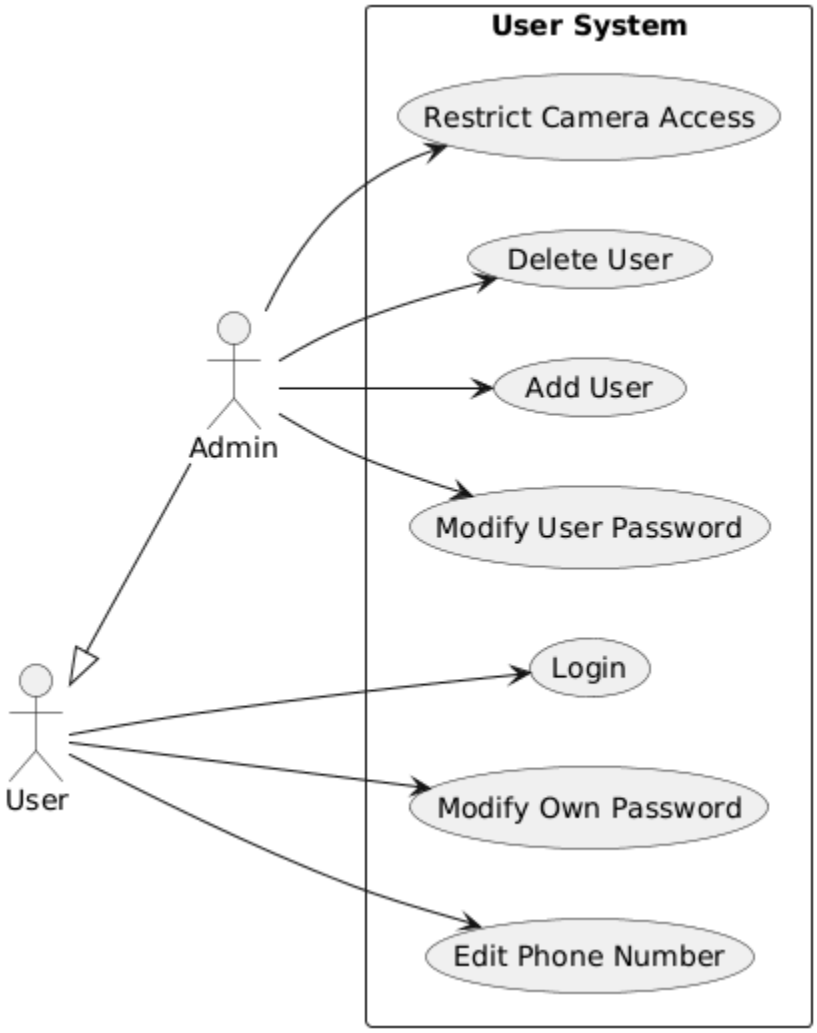
1. Surveillance Functions



2. Security Functions



3. User System



VI. Use Cases

1. Surveillance Use Cases

a. Display Thumbnail view

Primary actor: User
Channels to actor: Safehome Interface
Secondary actor: Cameras
Channels to secondary actors:
1. Camera: Wireless connectivity, Surveillance system interface

Goal In Context: To see all of the camera's views at once
Preconditions: System should be ready, and internet should be set;
The user must be logged in using correct credentials;
Trigger: The user wants to have a view of all cameras simultaneously.
Priority: Medium
Frequency of use: Frequent

Scenario:
1. The user selects "surveillance" from the major function buttons. (Fig. 2)
2. The user selects "Thumbnail view" from the options. (Fig. 3)
3. The system displays all of the active camera's thumbnails. (Fig. 9)
4. Each thumbnail has the name of the camera written at the bottom.
5. Thumbnails are updated every minute.

Exceptions:
4a. Camera unavailable for any reason – System displays a black screen with "Unavailable" written on it.
4b. Camera is disabled – System displays a black screen with "Disabled" written on it.
4c. User does not have permission for this specific camera – System displays a black screen with "No permission" written on it.

Open issues: None

b. Display Specific camera view

Primary actor: User
Channels to actor: Safehome Interface
Secondary actor: Camera
Channels to secondary actors:
1. Camera: Wireless connectivity, Surveillance system interface

Goal In Context: To see a specific camera's view.
Preconditions: System should be ready, and internet should be set;
User must be logged in using correct credentials;

The user should have permission to access this specific camera.

Trigger: The user wants to take a look through a set up camera.
Priority: High
Frequency of use: Frequent

Scenario:
1. The user selects “surveillance” from the major function buttons. (Fig. 2)
2. The user selects “Floor plan” from the options. (Fig. 3)
3. The system displays the floor plan of the house. (Fig. 10)
4. The user selects a camera icon from the floor plan.
5. The system displays the view of the selected camera. (Fig. 11)
6. The system displays video output within the viewing window at one frame per second.

Alternate Scenario:
Alternative to 3~5:
1. The user goes into Thumbnail view - see Use Case 3a: Display thumbnail view.
2. The user presses on the camera he wants to check.

Exceptions:
5a. Camera selected is not working for any reason - system displays error telling owner that the camera is not working.

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 a specific camera is broken?

c. Change pan/tilt/zoom of a specific camera

Primary actor: User
Channels to actor: Safehome Interface
Secondary actor: Camera
Channels to secondary actors:
1. Camera: Wireless connectivity, Surveillance system interface

Goal In Context: To change the camera’s view.
Preconditions: System should be ready, and internet should be set;
The user must be logged in using correct credentials.
The user must have permission to the specific camera.
Trigger: The user wants to look at a different angle from a camera.
Priority: Medium
Frequency of use: Occasional

Scenario:

1. The user goes into a specific camera's view - check usecase: Surveillance(a): Display specific camera view.
2. The system displays the view of the selected camera. (Fig. 11)
3. Within the camera view there is a zoom slider and 4 directional buttons.
4. "Zoom" slider: moving to the right will zoom out the current camera, moving to the left will zoom in.
5. "Angle" buttons: 4 direction buttons the right and left buttons will pan the camera in that direction, the up and down buttons will tilt the camera in that direction.

Exceptions:

3a: The camera does not have a zoom or pan feature(known through drivers) - Buttons are grayed out.

6a: The camera is at maximum of any of the motions - The camera does not respond in any way.

Open Issues:

1. What if the functionality is not available but the buttons still show?
2. Can any of the users with access to the specific camera move it?

d. Begin/End Camera Recording

Primary actor: User
Channels to actor: Safehome Interface
Secondary actor: Camera
Channels to secondary actors:

1. Camera: Wireless connectivity, Surveillance system interface

Goal In Context: To record a certain camera's view.
Preconditions: System should be ready, and internet should be set;
The user must be logged in using correct credentials;
The user has permission to access the camera.
Trigger: The user wants to either start or stop a camera recording.
Priority: Medium
Frequency of use: Occasional

Scenario:

1. The User goes into a specific camera's view - check usecase: Surveillance(b): Display specific camera view.
2. The system displays the view of the selected camera. (Fig. 11)
3. To start a recording they press the "Record" button.
4. A timer appears and the "Record" button is swapped with a "Stop Recording" button.
5. Leaving this camera view will continue recording.
6. When the user wants to end the recording they go back to the same camera view and press "Stop Recording".
7. The timer stops and the button goes back to "Record".
8. The recording is saved in the "Recordings" tab – See use case

Surveillance(e): Replay camera recording.

Exceptions:

5a: The allocated memory is finished – Automatically stop recording and send a notification to the user.

5b: The user forgets the recording for a certain period – Automatically stop recording and send a notification to the user.

5c: The camera stops working while recording is going – Automatically stop recording and send a notification to the user.

Open Issues:

1. How long should the recording go for before getting stopped automatically?
2. Can any of the users with access to the specific camera move it?

e. Replay recording

Primary actor: User
Channels to actor: Safehome Interface
Goal In Context: To see specific camera's view
Secondary actor: Camera
Channels to secondary actors:

1. Camera: Wireless connectivity, Surveillance system interface

Preconditions: System should be ready, and internet should be set;
The user must be logged in using correct credentials;
The user has permission to access the camera.
Trigger: The user wants to find an old recording.
Priority: Medium
Frequency of use: Occasional

Scenario:

1. The user goes into a specific camera's view - check usecase: Surveillance(b): Display specific camera view.
2. The system displays the view of the selected camera. (Fig. 11)
3. Press the "View Recordings" button.
4. A folder is opened with chronologically sorted recordings for this specific camera. (Fig. 12)
5. Pressing a recording will open a video player to view the recording in.

Open Issues:

1. How much storage should be allocated to each user?
2. Deleting recordings?

f. Enable Camera

Primary actor: User
Channels to actor: Safehome Interface
Secondary actor: Camera
Channels to secondary actors:

1. Camera: Wireless connectivity, Surveillance system interface

Preconditions: System should be ready, and internet should be set;
The user must be logged in using correct credentials;
The user has permission to access the camera;
The camera is not enabled.
Trigger: The user wants to enable a certain camera.
Priority: High
Frequency of use: Often

Scenario:

1. The user goes into a specific camera's view - check usecase: Surveillance(b): Display specific camera view.
2. The system displays the view of the selected camera. (Fig. 11)
3. The camera view is a black screen with "Disabled" written in it. (Fig. 13)
4. The user presses the "Enable" button.
5. The camera view shows the live camera footage.
6. The "Enable" button becomes "Disable".

Exceptions:

3a: camera is "Unavailable" – The "Enable" button is not pressable.

Open issues: None

g. Disable Camera

Primary actor: User
Channels to actor: Safehome Interface
Goal In Context: To turn off a disabled camera
Secondary actor: Camera
Channels to secondary actors:

1. Camera: Wireless connectivity, Surveillance system interface

Preconditions: System should be ready, and internet should be set;
The user must be logged in using correct credentials;
The user has permission to access the camera;
The camera is enabled.
Trigger: The user wants to enable a certain camera.
Priority: High
Frequency of use: Often

Scenario:

1. The user goes into a specific camera's view - check usecase: Surveillance(b): Display specific camera view.
2. The system displays the view of the selected camera. (Fig. 11)
3. The camera view is a showing a live camera footage.
4. The user presses the "Disable" button.
5. The camera view switches to a black screen with "Disabled" written in text.
6. The "Disable" button becomes "Enable".

Open issues: None

2. Security Use Cases

a. Check sensor status

Primary actor: User
Channels to actor: Safehome Interface
Secondary actor: Sensors
Channels to secondary actors:
1. Sensors: wireless connectivity

Preconditions: System should be ready, and internet should be set;
The user should have view sensor permission.
Trigger: The user wants to check the status of sensors.
Priority: High
Frequency of use: Frequent.

Scenario:
1. The user logs onto the system.
2. The user selects “security” from major function buttons. (Fig. 2)
3. The user selects “system status” → “sensors” from top of the screen. (Fig. 14)
4. System loads sensor status(power, battery, last seen, on/off). (Fig. 20)
5. The user clicks a sensor to view details. (Fig. 21)
6. The system shows about sensor(device information, event logs).

Exception:
4a. No permission to view sensor status – display “sensor access denied” on the screen.
4b. No information about sensor status – display “no information” on each sensors.

b. Turn a sensor On or Off

Primary actor: Admin
Channels to actor: Safehome Interface
Secondary actor: Sensors
Channels to secondary actors:
1. Sensors: wireless connectivity

Preconditions: Successfully entered the check sensor status page.
Trigger: Admin wants to turn a sensor On or Off.
Priority: Medium
Frequency of use: Occasional

Scenario:
1. Admin successfully reached the check sensor status page. (Fig. 21)
2. Admin selects a sensor from the sensor list to view in more detail.

3. Click the on/off toggle to turn on/off.
4. Click the confirm button to save.
5. Record this change and notify the admin.

Exception:

4a. On/off request not processed for any reason – If a request cannot be processed within a certain time, a "Device Not Responding" message is displayed.

4b. Sending multiple requests to the same sensor simultaneously – If there are pending requests, a "Too Many Requests" message is displayed. Send the previous status along with the request, and reject the request if the previous status is different.

4c. Sensor belongs to currently armed zone – display "Cannot disable sensor in armed zone. Disarm zone first.".

Open issues:

1. When sending a request to a device, there's always a chance of an exception being thrown due to no response or duplicate requests. How about relegating this to another use case?

c. Create new safety zone

Primary actor: Admin
Channels to actor: Safehome Interface
Secondary actor: Sensors
Channels to secondary actors:

1. Sensors: wireless connectivity

Preconditions: System should be ready, and internet should be set; Admin user logged in.
Trigger: Admin decided to create a new zone
Priority: Medium
Frequency of use: Occasional

Scenario:

1. Admin logs into the system and selects “security” from major function buttons. (Fig. 2)
2. Admin selects “system status” → “safety zone” from top of the screen. (Fig. 14)
3. Clicks plus button. (Fig. 17)
4. Select which security mode will arm the safety zone. (Fig. 18)
5. Selects and assigns sensors to the new zone by clicking the checkbox of each sensor in the floor plan.
6. The system processes the request and notifies the admin if it is successful.

Exception:

3a. Duplicate zone name – system requests new name.

4a. Unavailable sensor – system excludes it and notifies the user.

4b. No sensors selected – display "At least one sensor must be assigned to

create a zone".
5a. Failed to process request for any reason(e.g. duplicate request exists) – Displays "create new safety zone failed" and leaves a log.

Open issues:

1. The sensors forming the safety zones may not be disjoint.
2. Should the number of zones per system be limited?

d. Update an existing safety zone

Primary actor: Admin
Channels to actor: Safehome Interface
Secondary actor: Sensors
Channels to secondary actors:

1. Sensors: wireless connectivity

Preconditions: System should be ready, and internet should be set; Admin user logged in.
Trigger: Admin decided to delete a zone
Priority: Medium
Frequency of use: Rare

Scenario:

1. Admin logs into the system and selects “security” from major function buttons. (Fig. 2)
2. Admin selects “system status” → “safety zone” from top of the screen. (Fig. 14)
3. Click the detail button. (Fig. 17)
4. Admin can edit the safety zone or delete it. (Fig. 18)
5. The system processes the request and notifies the admin if it is successful.

Exception:

3a. Zone currently armed – system denies deletion and displays “Disarm zone before deletion.”.
5a. Failed to process request for any reason(e.g. duplicate request exists) – Displays "delete safety zone failed" and leaves a log.

Open issues: None

e. Arm/disarm safety zones by setting security modes

Primary actor: User
Channels to actor: Safehome Interface
Secondary actor: Sensors
Channels to secondary actors:

1. Sensors: wireless connectivity

Preconditions: System should be ready, and internet should be set; User have Arm/disarm permission
Trigger: User decided to change security modes

Priority: High
Frequency of use: Frequent

Scenario:

1. The user logs into the system and selects “security” from major function buttons. (Fig. 2)
2. The current security mode and available security modes are displayed. (Fig. 15)
3. Click Security Modes in the top of the page and open the dropdown. (Fig. 14)
4. Select which security mode to switch and click switch to mode.
5. mode is changed and notified to the admin.

Exception:

4a. When the user tries to change the safety mode, the corresponding sensor is already detected. – Displays "sensor already detected” message

4b. Failed to process request for any reason(e.g. duplicate request exists) – Displays "delete safety zone failed" and leaves a log

5a. The user clicks the cancel button – exit without saving changes.

Open issues:

1. Is there any difference between Away, Overnight Travel, Extended Travel and Home, Guest Home in Fig 5?

f. Add, edit, delete security modes

Primary actor: Admin
Channels to actor: Safehome Interface
Secondary actor: None
Preconditions: System should be ready, and internet should be set; Admin user logged in.
Trigger: Admin decided to view intrusion log
Priority: Medium
Frequency of use: Occasional

Scenario:

1. Admin logs into the system and selects “security” from major function buttons. (Fig. 2)
2. Click “Security Modes” in the top of the page. (Fig. 14)
3. Click “+Add mode” to add security mode or click mode name > “Edit mode” to edit or delete security mode.
4. Go to the page where user can set safety zone and sensors of security mode. (Fig. 19)
5. After editing, click confirm to save and click delete to delete that mode.
6. The system processes the request and notifies the admin if it is successful.

Exception:

3a. User is not Admin – Don’t display add, edit and just display modes and

switch to mode

Open issues: None

g. View intrusion log

Primary actor: Admin
Channels to actor: Safehome Interface
Secondary actor: None
Preconditions: System should be ready, and internet should be set; Admin user logged in.
Trigger: Admin decided to view intrusion log
Priority: Medium
Frequency of use: Occasional

Scenario:

1. Admin logs into the system and selects "security" from major function buttons. (Fig. 2)
2. Click "Monitoring" → Intrusion at the top of the page. (Fig. 14)
3. The system retrieves and displays log entries. (date, time, location, event type). (Fig. 16)
4. Admin can export or delete logs by clicking export, delete icons.

Exception:

3a. No logs found — system displays "No intrusion events recorded.".

Open issues: None

h. Alarm conditions encountered

Primary Actor: Sensor
Channel to actor: Security System
Secondary actors: Admin
Channels to secondary actors:

1. User: Phone

Precondition: System armed and sensors are functional.
Trigger: Any sensor detects motion, or a door opens when it is armed.
Priority: High
Frequency of use: Event-driven

Scenario:

1. A sensor (door, window, or motion) detects an unauthorized event.
2. The system checks whether the sensor is armed or disarmed.
3. The system triggers the alarm siren if sensor is armed.
4. The system displays an alarm message on the control panel and SafeHome Interface.
5. The system notifies the admin via phone.

3. User System Use Cases

a. Login

Primary actor: User
Channels to actor: Safehome Interface
Preconditions: User has valid credentials; System is operational
Trigger: The user wants to log in through the SafeHome interface.
Priority: High
Frequency of use: Frequent

Scenario:

1. The system requests user credentials.
2. User enters credentials (username/password). (Fig. 1)
3. System validates credentials.
4. If credentials are valid, the user gains access to authorized functions. (Fig. 2)

Exception:

2a. Invalid credentials entered: system requests re-entry. After three failed attempts, the account/system locks temporarily.

Note: This use case is abstract/general. Specific login methods are modeled as specialized use cases.

b. Add user

Primary actor: Admin
Channel to actor: configure menu > user manage section
Goal in context: To add user in the Safehome system
Preconditions: Admin user is logged in
Trigger: The admin decides to add user onto the system
Priority: Low
Frequency of use: Not frequent

Scenario:

1. The admin opens the user manage section in the configure menu. (Fig. 6)
2. The admin clicks the add user button.
3. The system asks for a new user's id and password via dialogue. (Fig. 7)
4. The admin enters a new user's id and password.
5. The system adds the new user.
6. The system updates the user manage section to show the new user. (Fig. 6)

Exception:

4a. Duplicated user id — The system asks for user id again.

Open issues:

1. None

c. Delete user

Primary actor: Admin
Channel to actor: configure menu > user manage section
Preconditions: Admin user is logged in
Trigger: The admin decides to delete specific user from the system
Priority: Low
Frequency of use: Not frequent

Scenario:

1. The admin opens the user manage section in the configure menu. (Fig. 6)
2. The admin selects a user from the user list.
3. The system shows the selected user's setting page. (Fig. 8)
4. The admin clicks delete user button.
5. The system deletes the selected user.
6. The system updates the user list to hide the deleted user. (Fig. 6)

Exceptions: None

Open issues:

1. None

d. Restrict camera access

Primary actor: Admin
Channel to actor: configure menu > user manage section
Preconditions: Admin user is logged in
Trigger: The admin decides to grant or revoke camera access permission from the specific user.
Priority: Low
Frequency of use: Not frequent

Scenario:

1. The admin opens the user manage section in the configure menu. (Fig. 6)
2. The admin selects a user from the user list.
3. The system shows the selected user's setting page. (Fig. 8)
4. The user clicks the camera access button.
5. The system displays a floor plan highlighting the cameras that users are authorized to access. (Fig. 10)
6. The admin clicks the camera to toggle the permission.
7. The admin clicks the confirm button to confirm changes. (Fig. 8)
8. The system updates the changed permissions of the user.

Exception: None

Open issues:

1. None

e. Modify user password

Primary actor: Admin
Channel to actor: configure menu > user manage section
Goal in context: To modify password of certain user
Preconditions: Admin user is logged in
Trigger: The admin decides change password of a specific user
Priority: Low
Frequency of use: Not frequent

Scenario:

1. The admin opens the user manage section in the configure menu. (Fig. 6)
2. The admin selects a user from the user list.
3. The system shows the selected user's setting page. (Fig. 8)
4. The admin clicks the change password button.
5. The system displays a dialog that asks for the new password.
6. The admin enters the new password of the user.
7. The admin clicks the confirm button to apply changes.
8. The system updates the changed password of the user.

Exception: None

Open issues:
1. None

f. Modify own password

Primary actor: User
Channel to actor: configure menu > user profile section
Preconditions: User is logged in
Trigger: The user decides to change his password
Priority: Low
Frequency of use: Not frequent

Scenario:
1. The user opens the user profile section in the configure menu. (Fig. 4)
2. The user clicks the change password button. (Fig. 5)
3. The system displays a dialog that asks for the new password.
4. The user enters the new password.
5. The user clicks the confirm button to apply changes.
6. The system updates the changed password of the user.

Exception: None

Open issues:
1. None

g. Edit phone number

Primary actor: User
Channel to actor: configure menu > user profile section
Goal in context: To register phone number of user himself
Preconditions: User is logged in
Trigger: The user decides to register a phone number
Priority: Low
Frequency of use: Not frequent

Scenario:
1. The user opens the user profile section in the configure menu. (Fig. 4)
2. The user clicks the change phone number button. (Fig. 5)
3. The system displays a dialog that asks for a new phone number.
4. The user enters the new phone number.
5. The user clicks the confirm button to apply changes.
6. The system updates the phone number of the user.

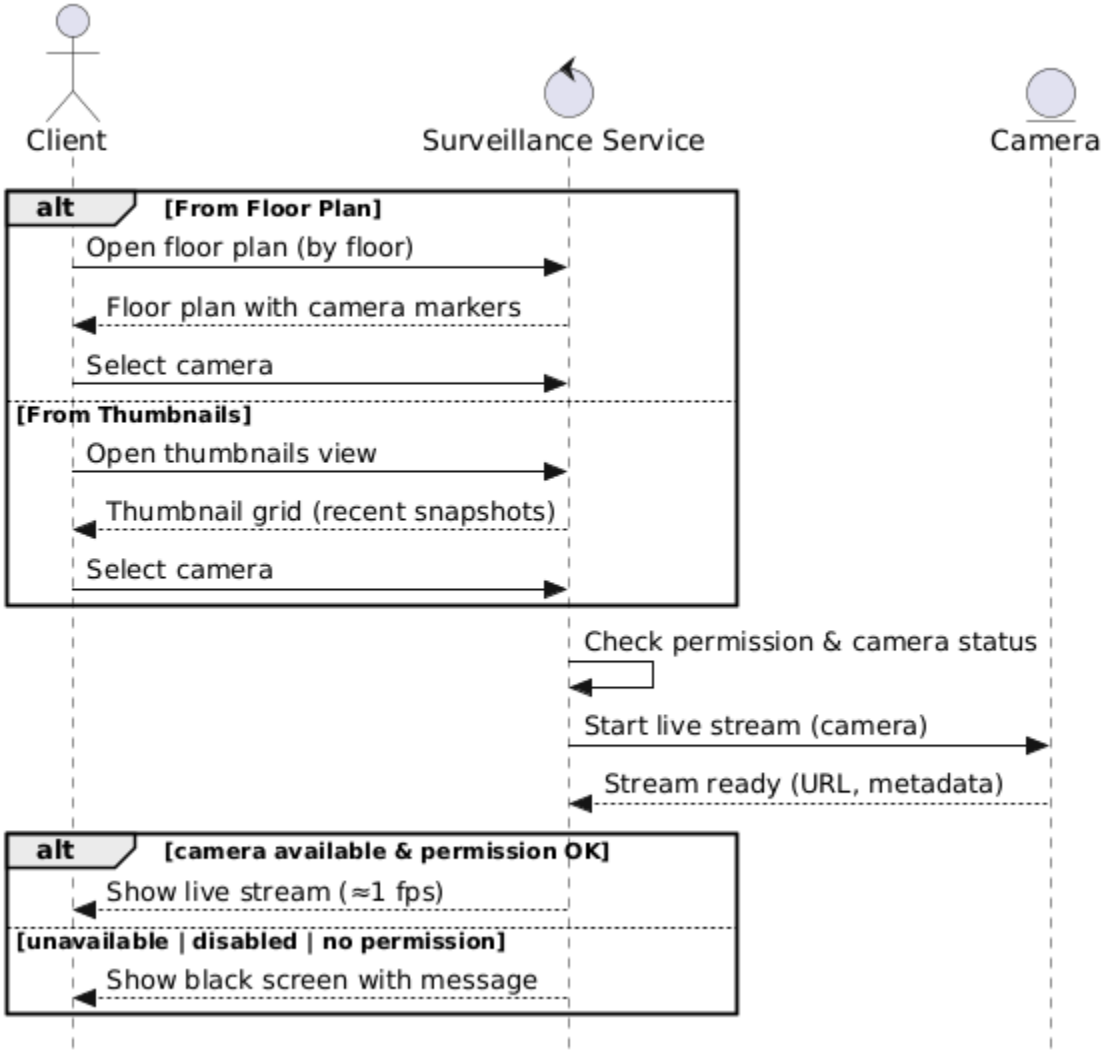
Exception: None

Open issues:
1. None

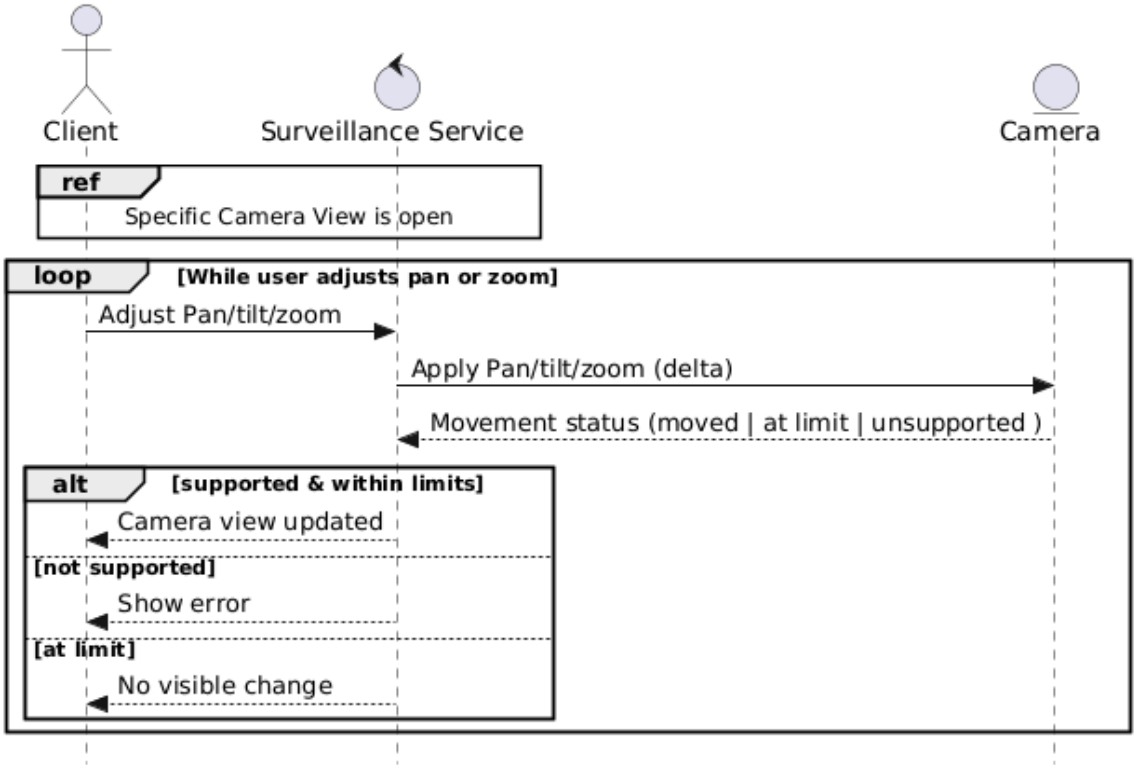
VII. Sequence Diagrams

1. Surveillance Sequence Diagrams

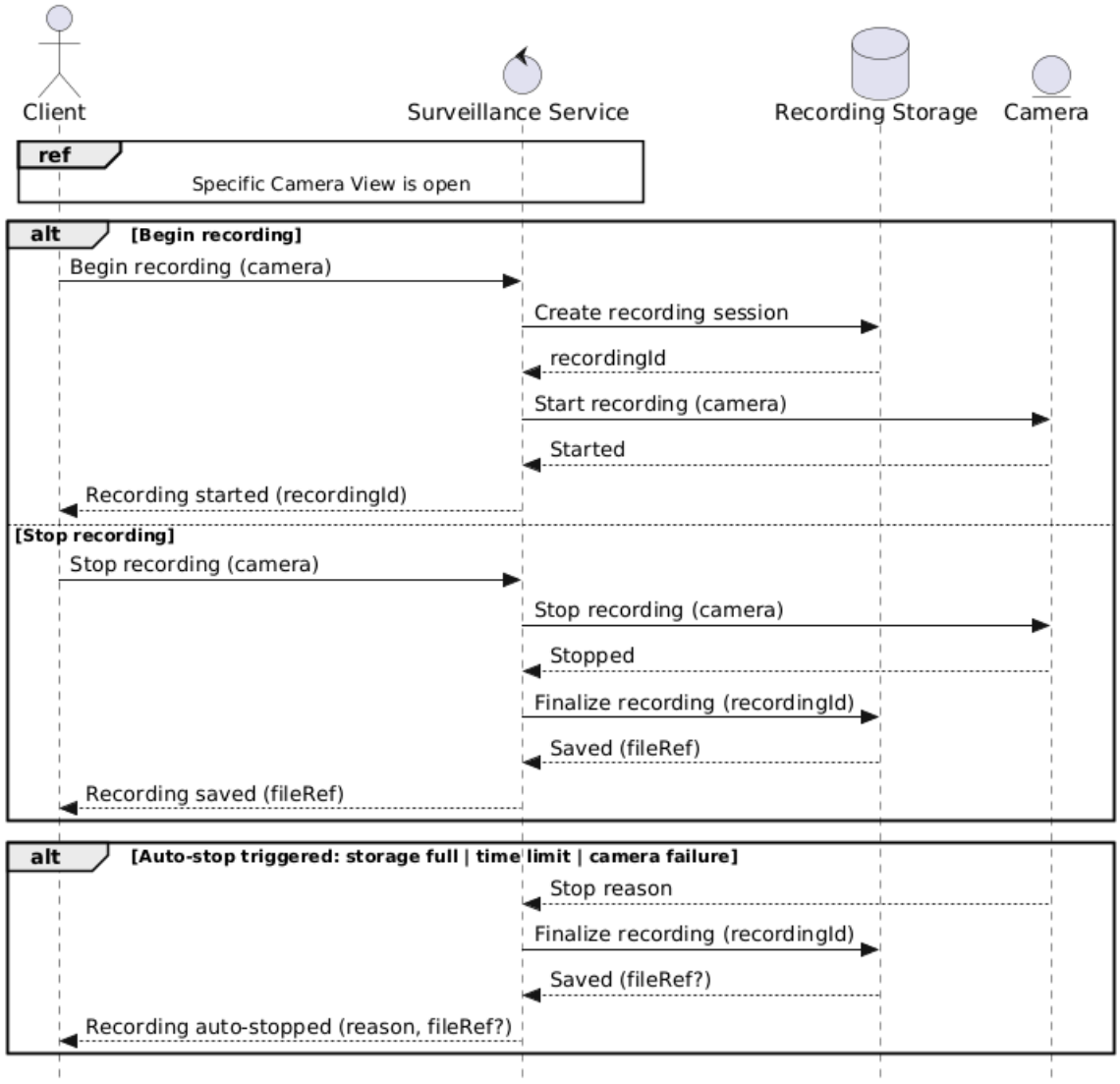
a. Display specific camera view



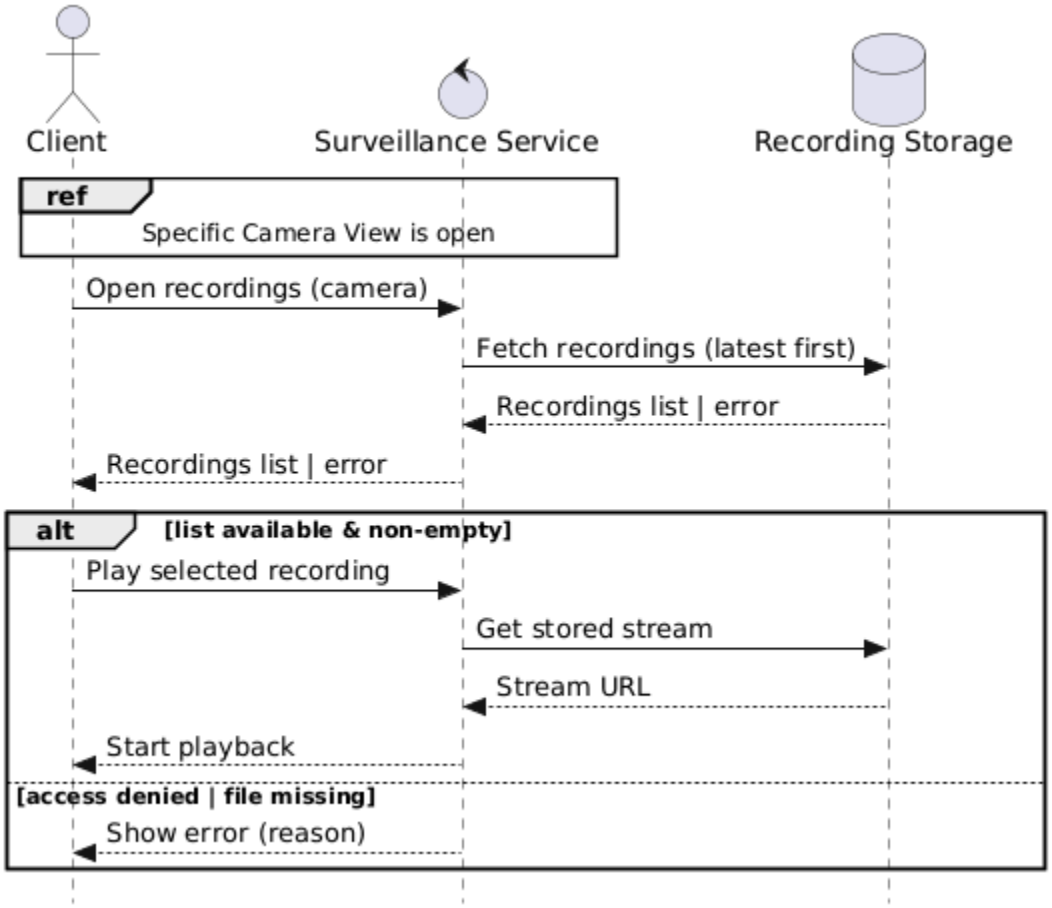
b. Pan/Zoom camera



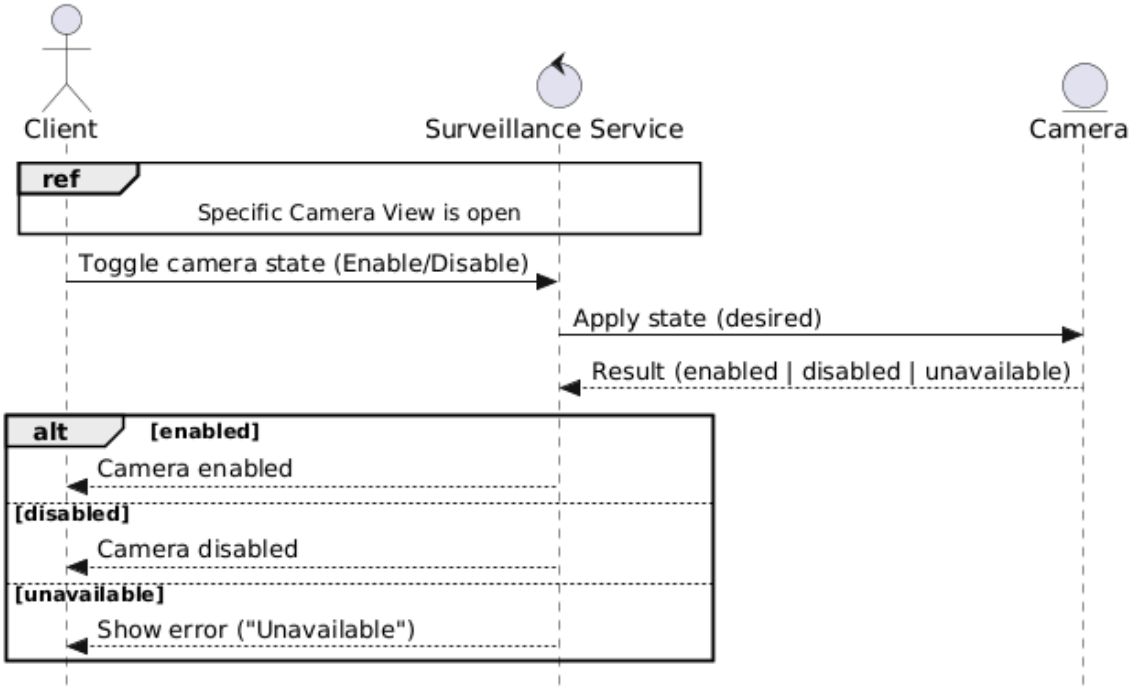
c. Start/Stop recording



d. Replay past recording

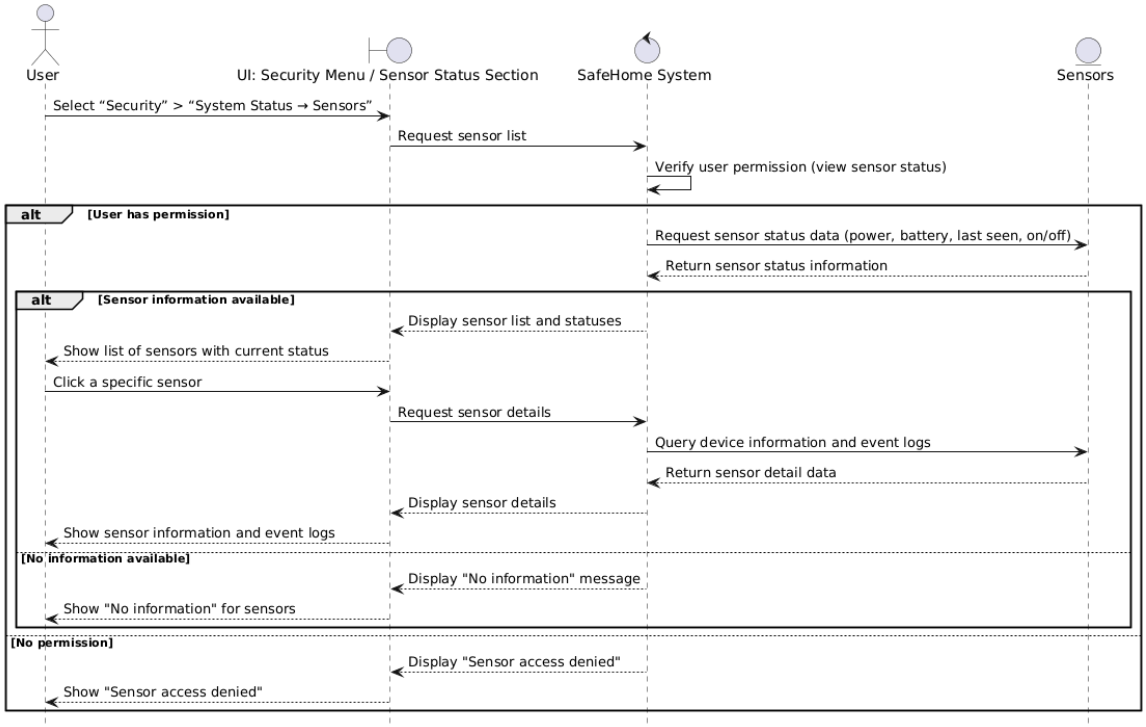


e. Enable/Disable camera

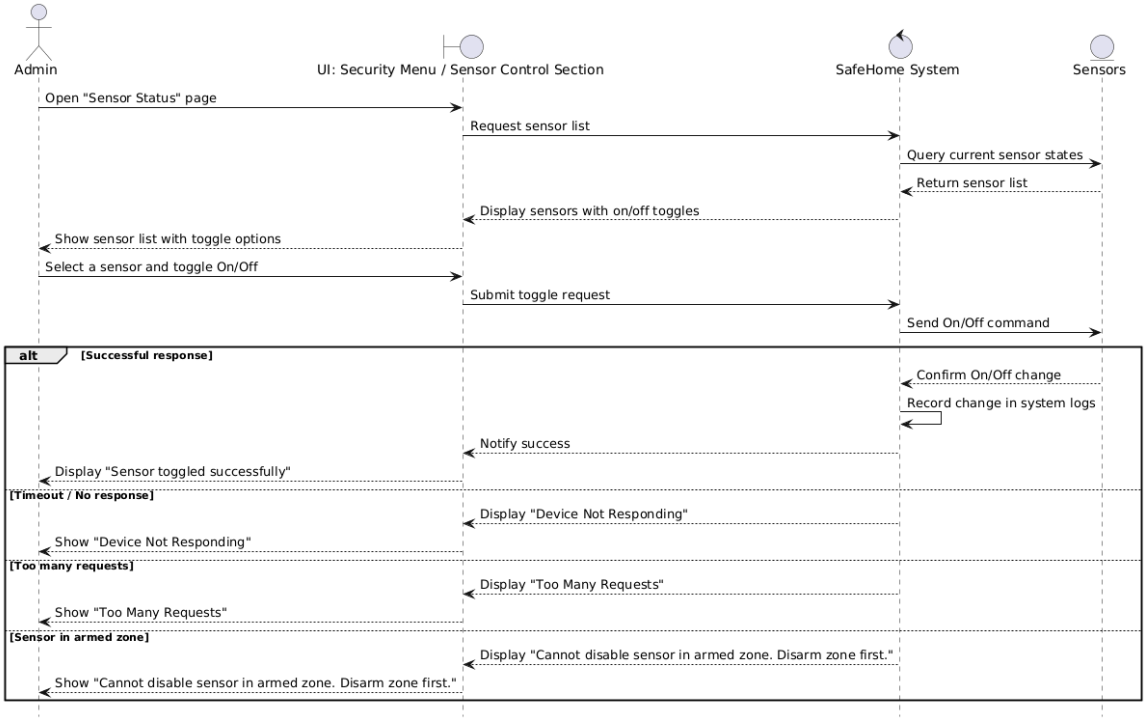


2. Security Sequence Diagrams

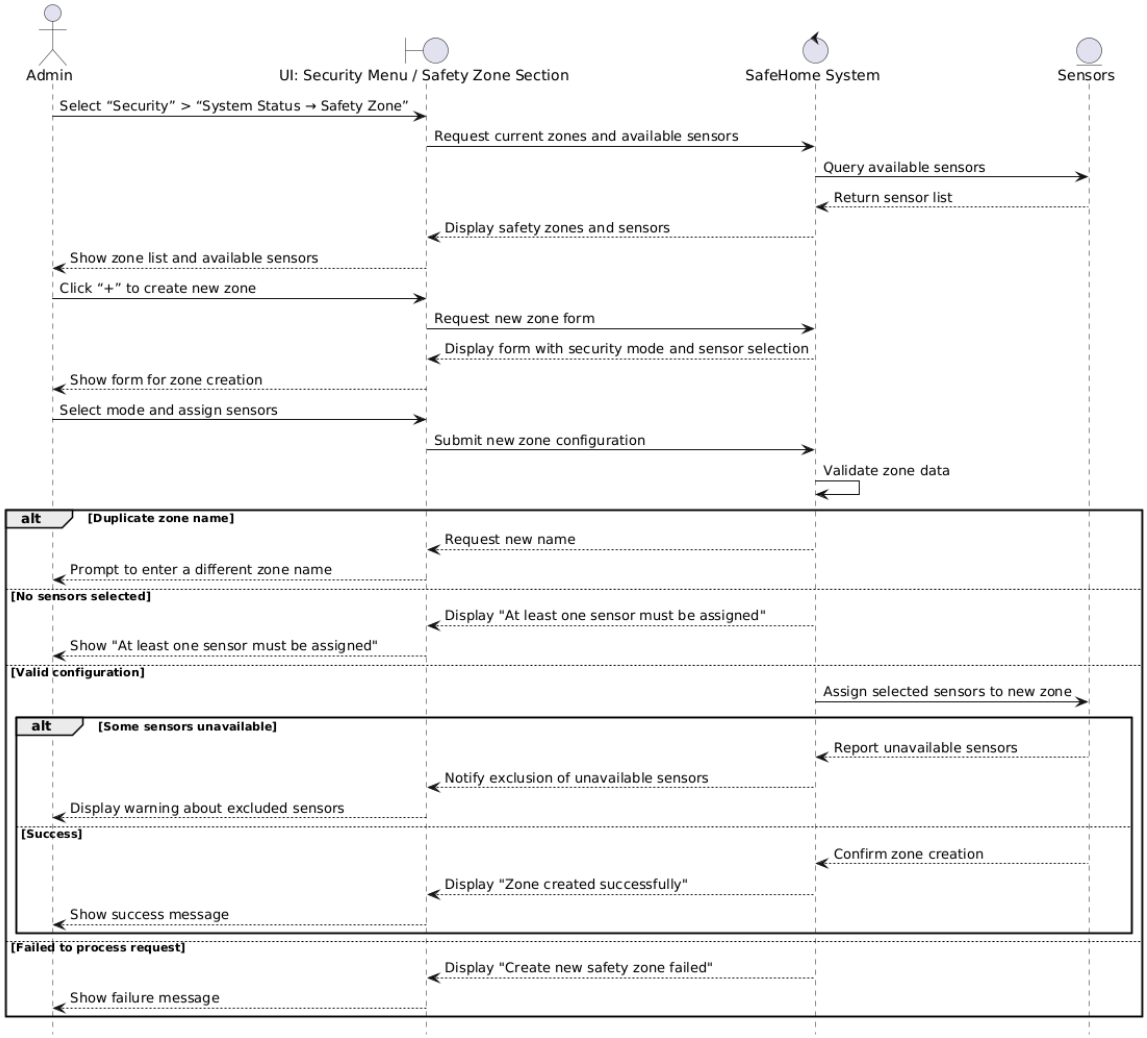
a. Check sensor status



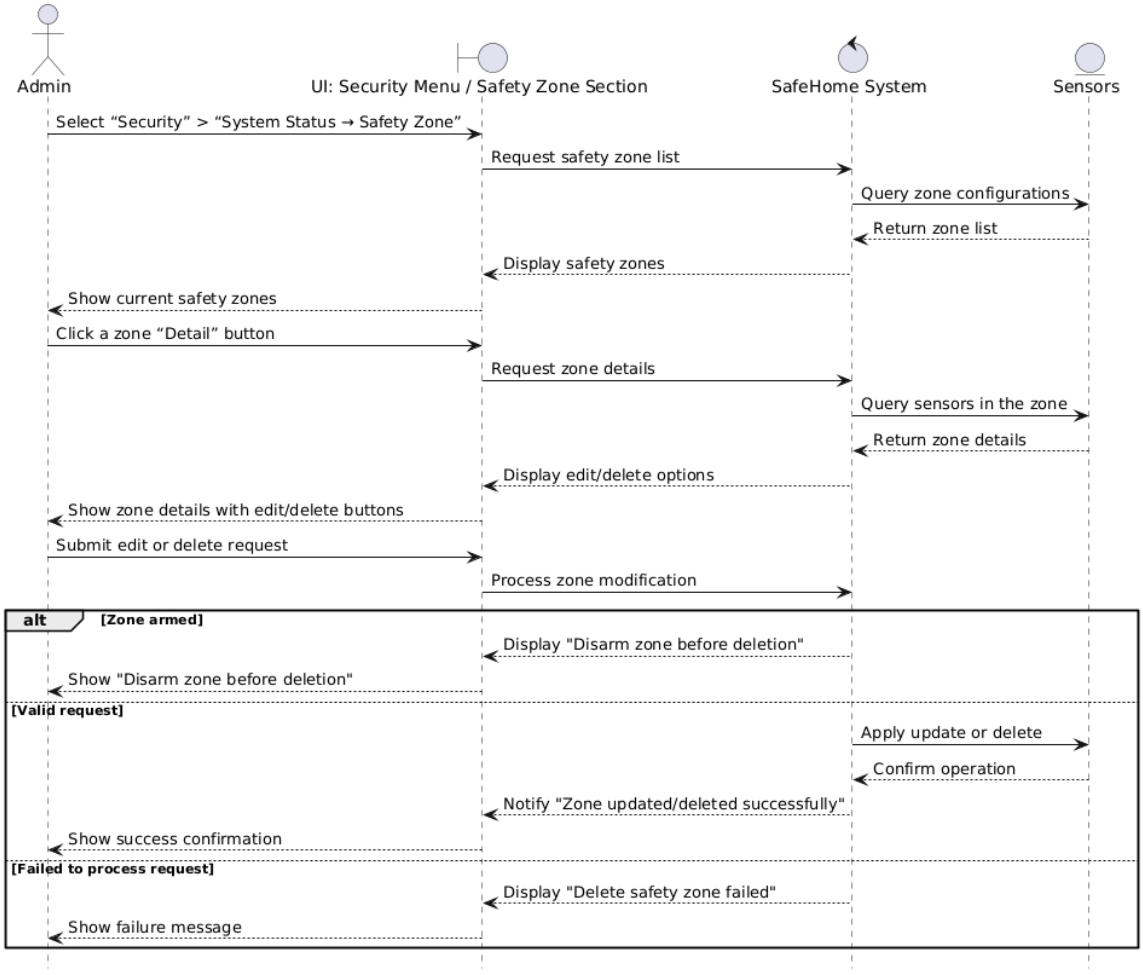
b. Turn a sensor On or Off



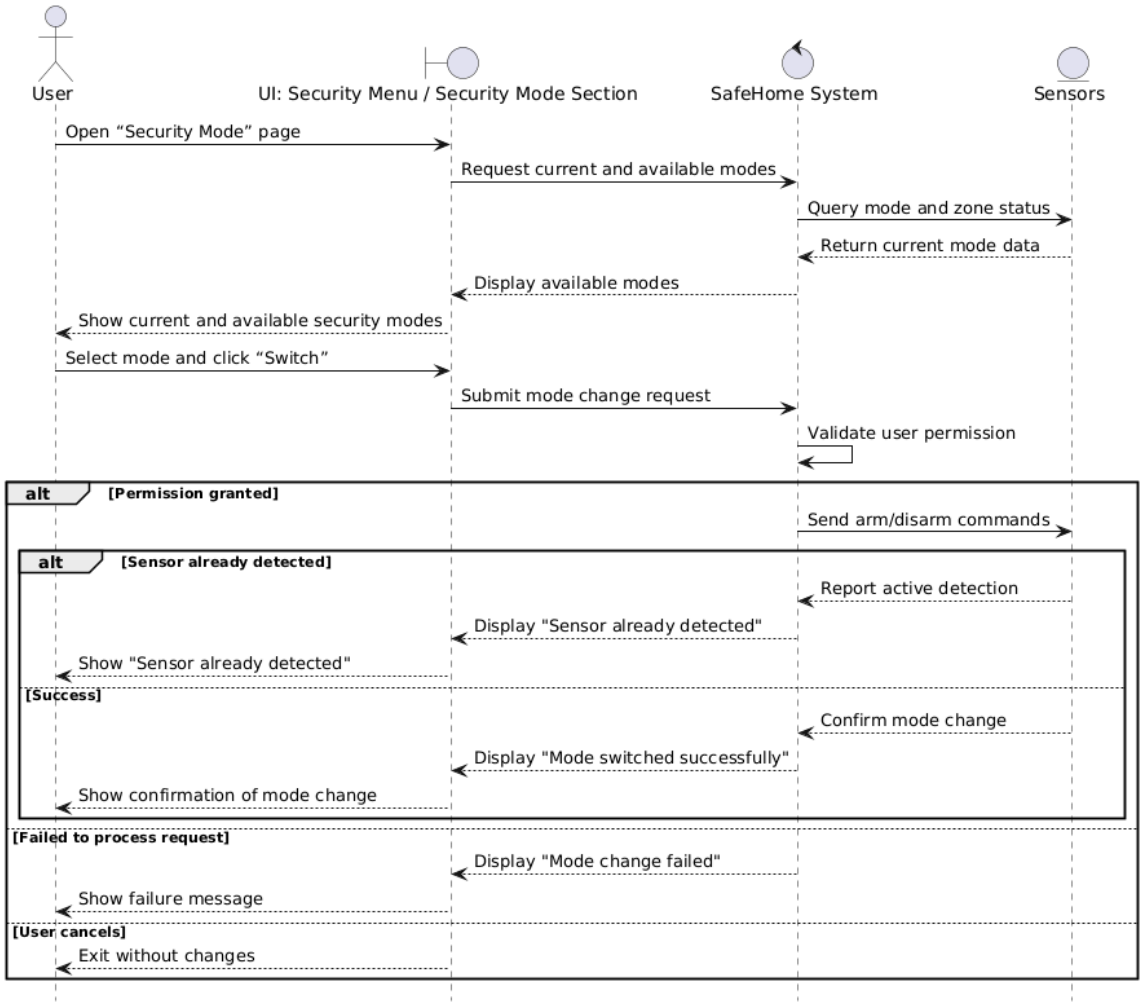
c. Create new safety zone



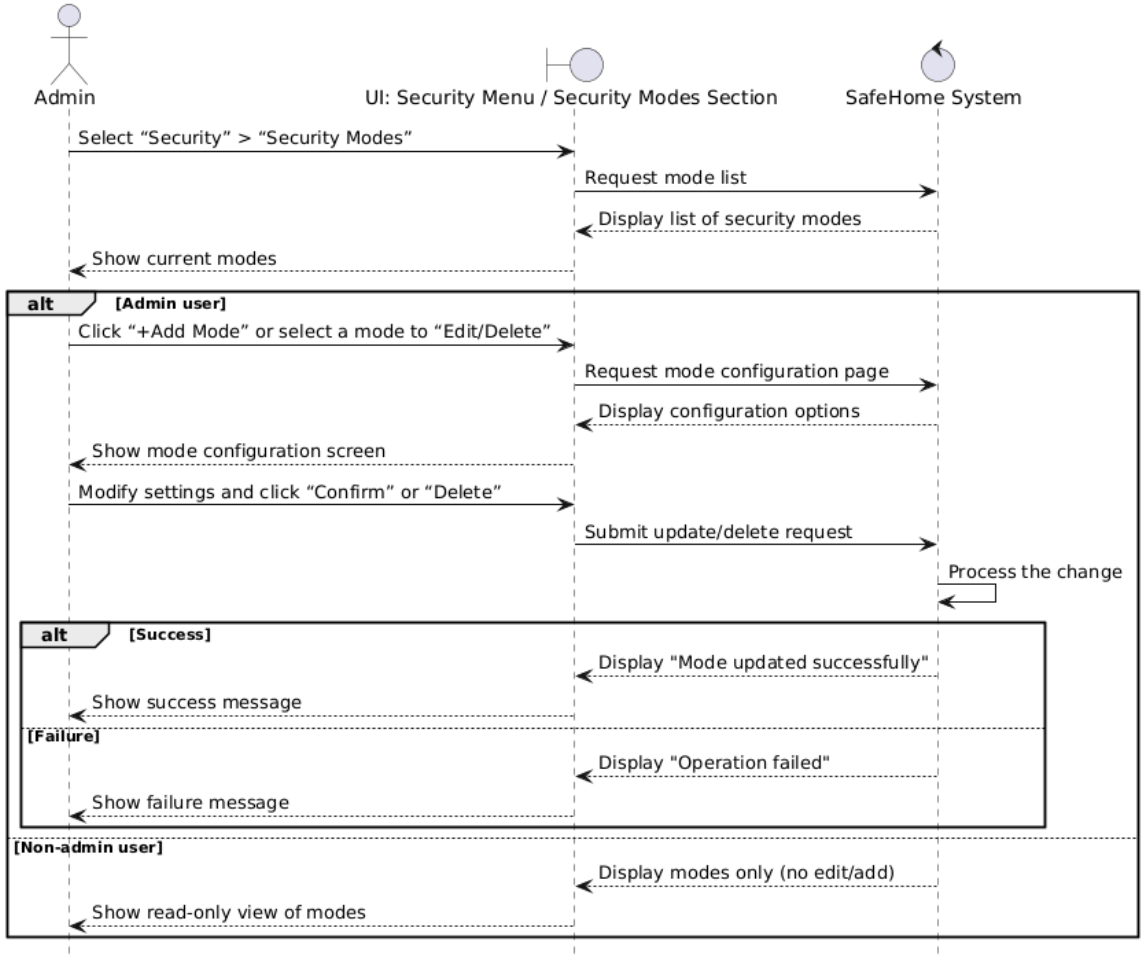
d. Update an existing safety zone



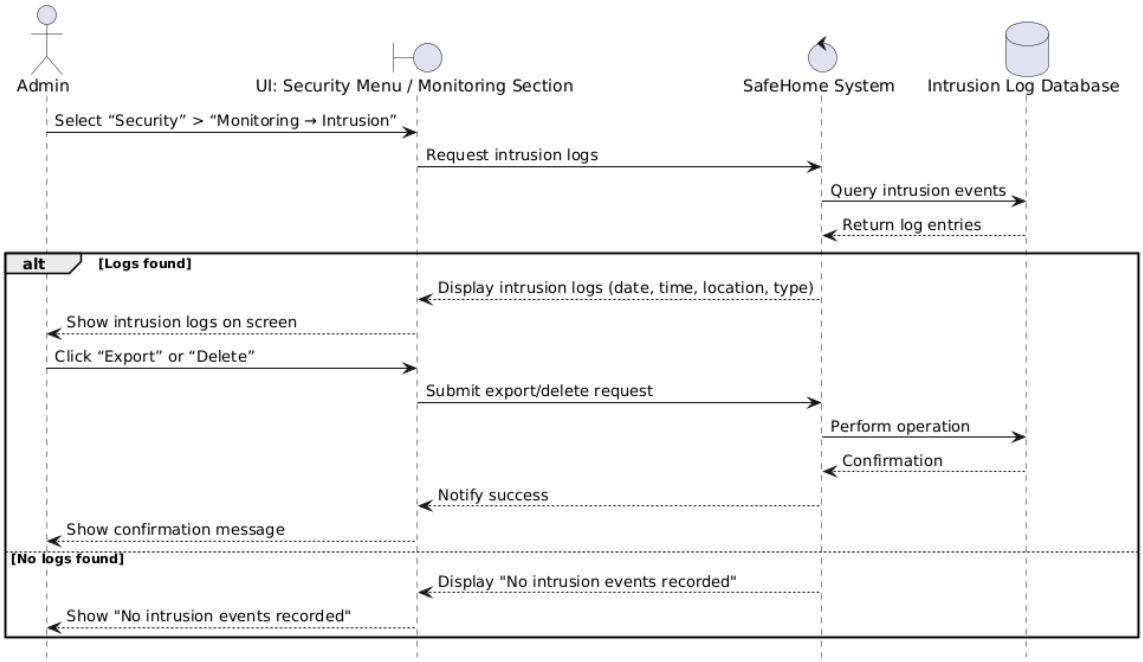
e. Arm/disarm safety zones by setting security modes



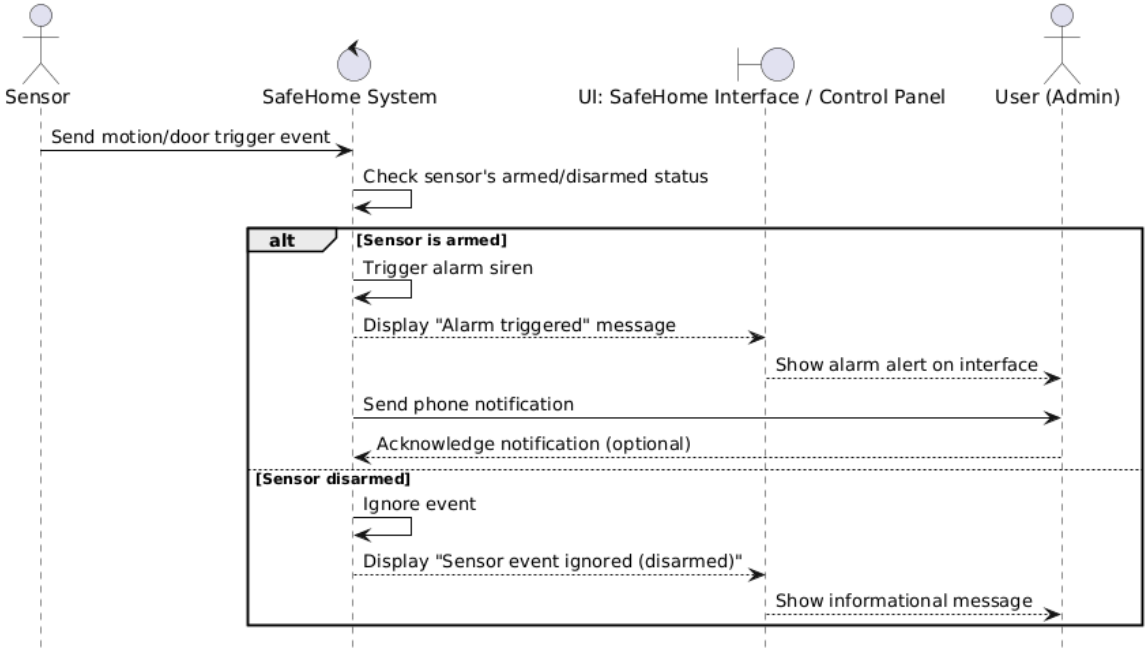
f. Add, edit, delete security modes



g. View intrusion log

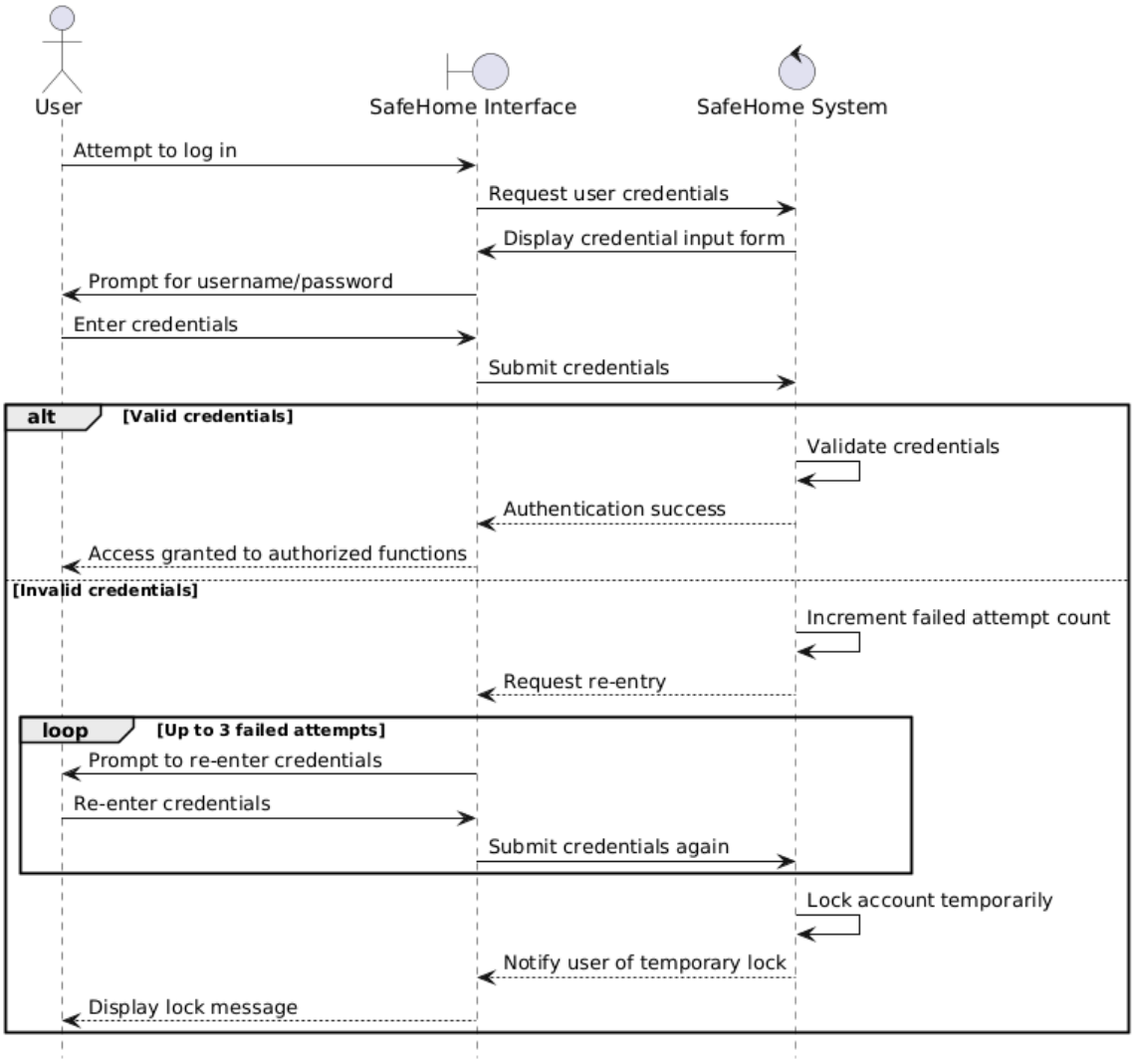


h. Alarm conditions encountered

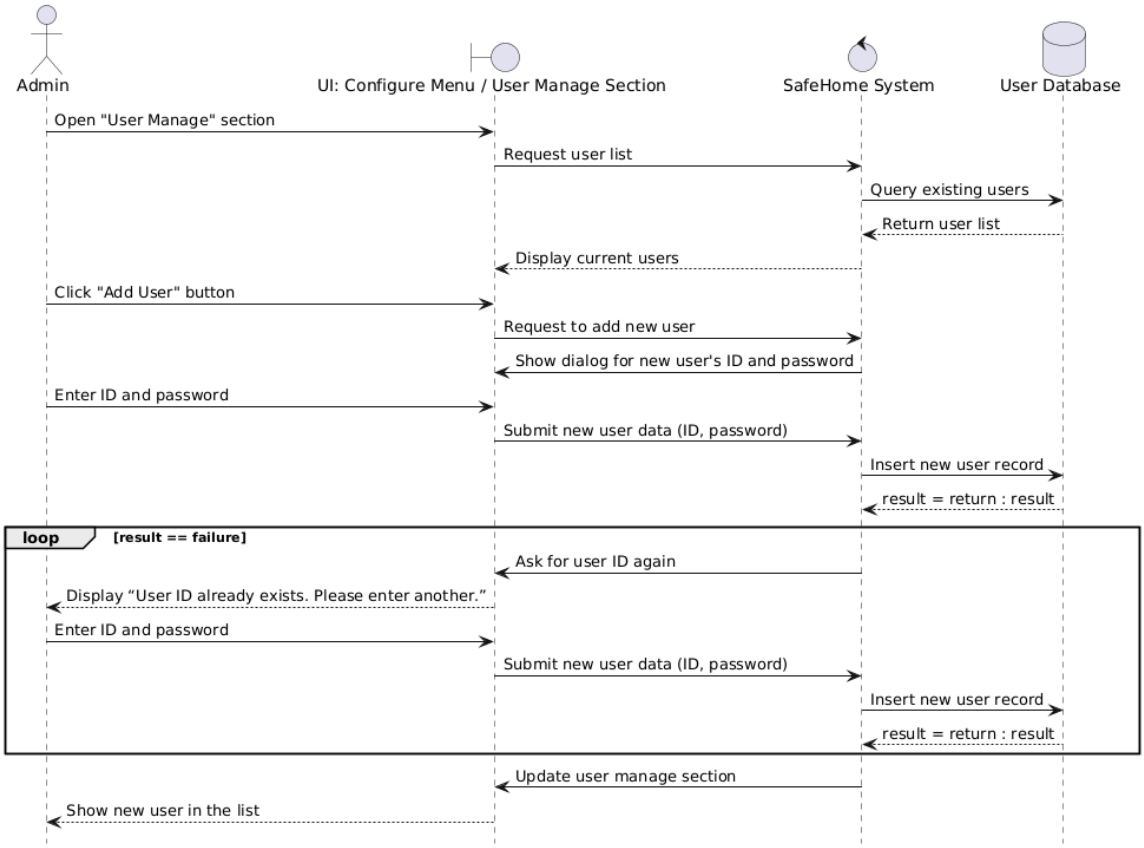


3. User System Sequence Diagrams

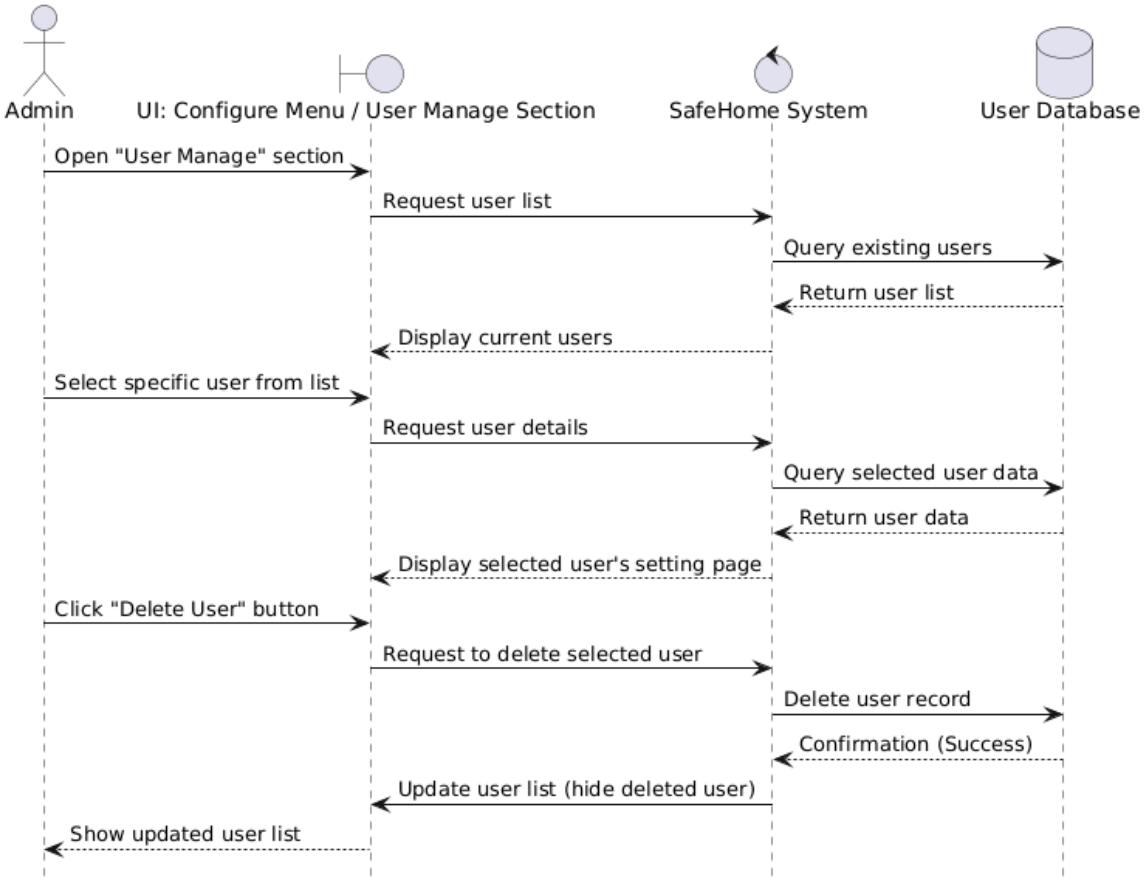
a. Login



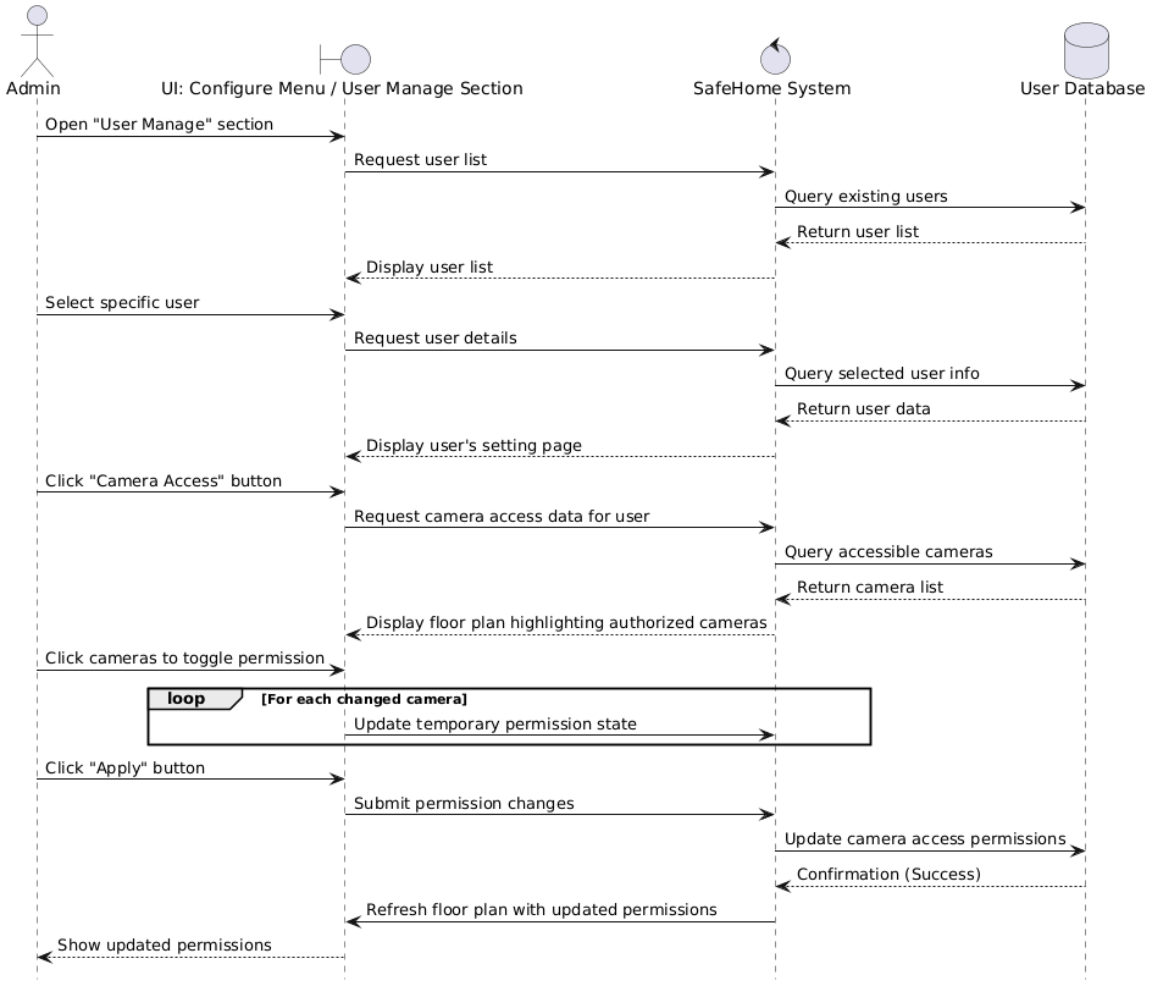
b. Add user


Admin
UI: Configure Menu / User Manage Section
SafeHome System
User Database
Open "User Manage" section
Request user list
Query existing users
Return user list
Display current users
Click "Add User" button
Request to add new user
Show dialog for new user's ID and password
Enter ID and password
Submit new user data (ID, password)
Insert new user record
result = return : result
loop
[result == failure]
Ask for user ID again
Display “User ID already exists. Please enter another.”
Enter ID and password
Submit new user data (ID, password)
Insert new user record
result = return : result
Update user manage section
Show new user in the list

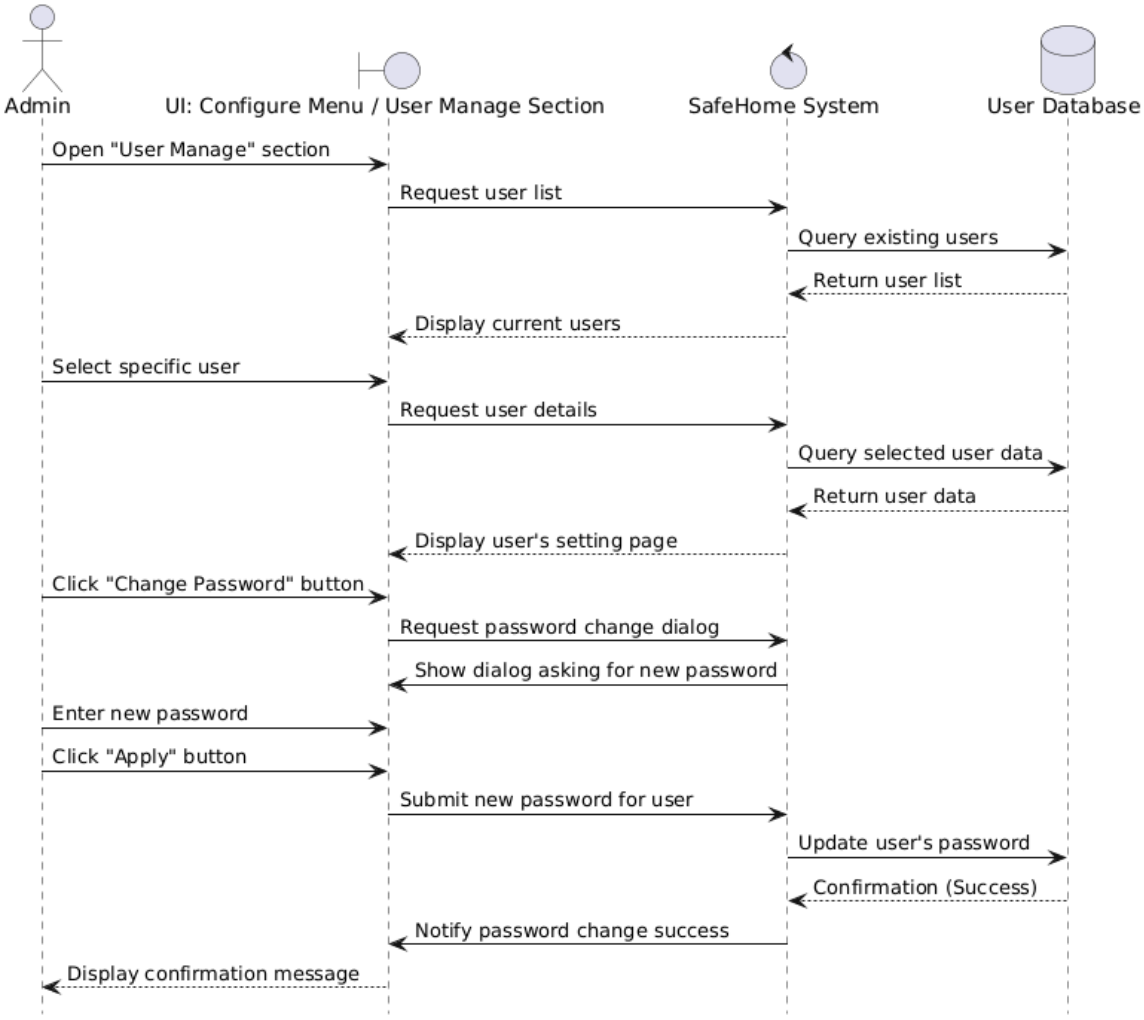
c. Delete user



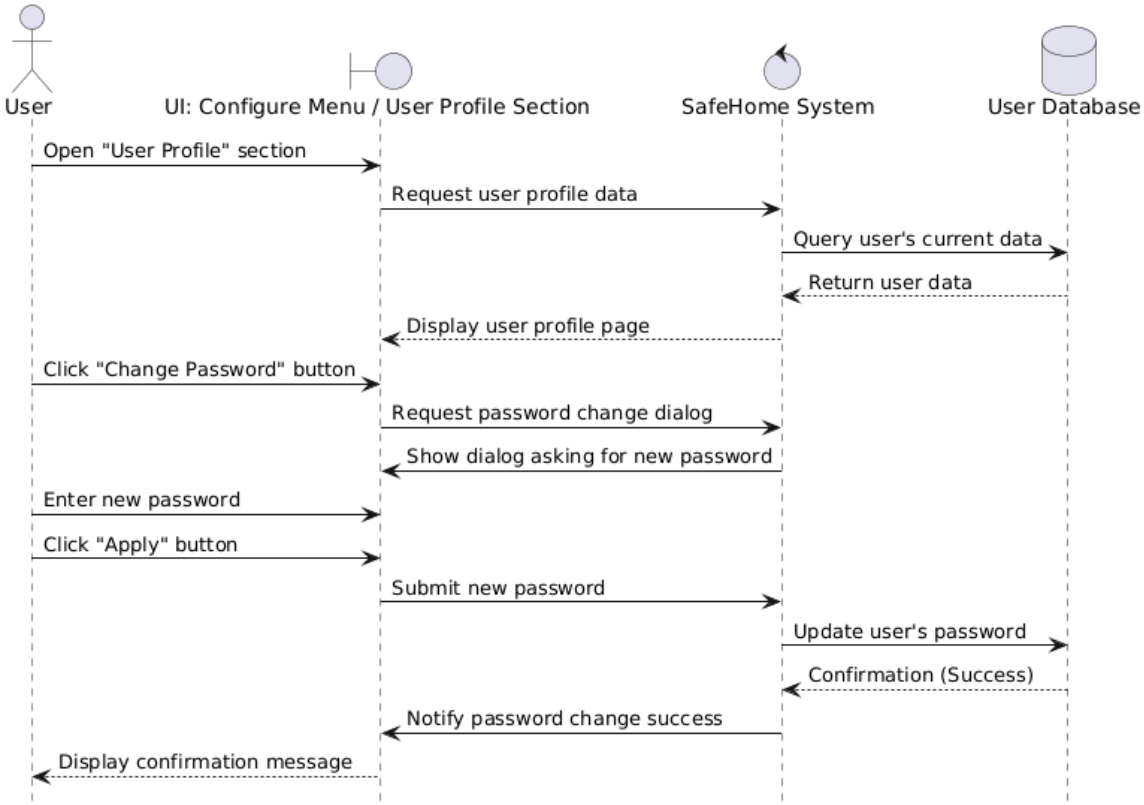
d. Restrict camera access



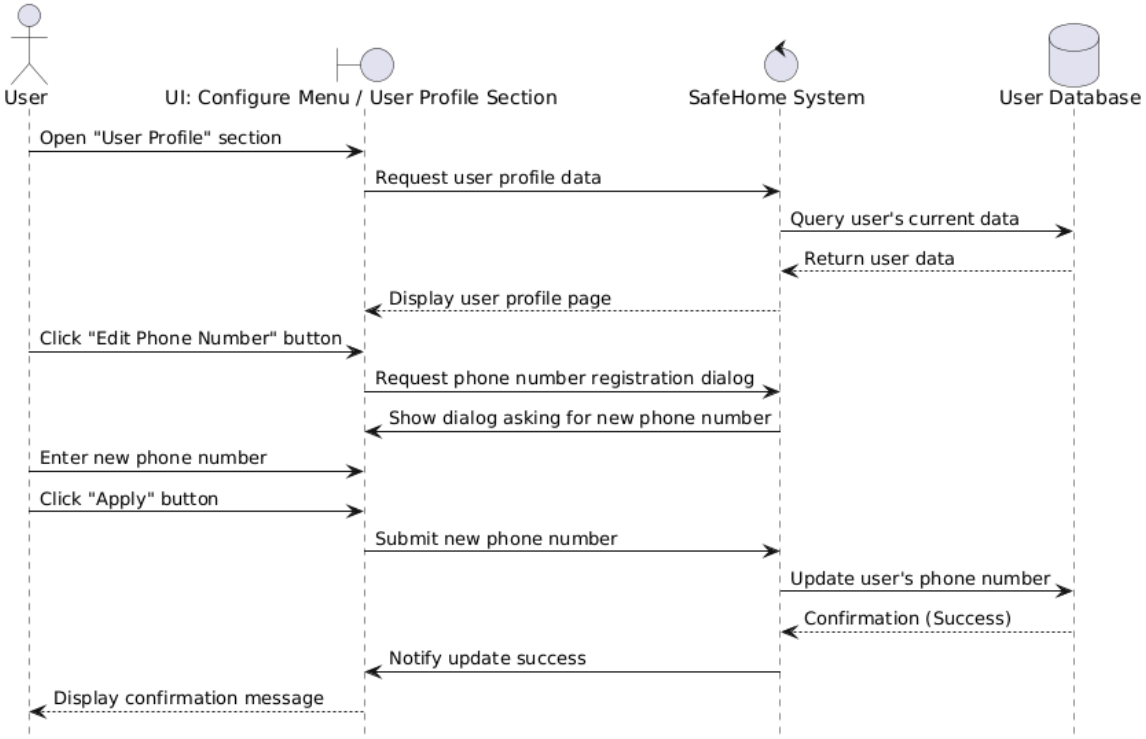
e. Modify user password



f. Modify own password



g. Edit phone number



VIII. Who did what

All the team members were involved in adding to the sections: IV. Assumptions and X. Glossary while working on the rest of the document. Team members were also involved in deciding conventions and better approaches together, which included going over each other's works, then suggesting and/or applying fixes.

Team member A - 20240397 Hichan Shin
1. Made V.2. Security Use Case Diagrams 2. Wrote VI.2. Security Use Cases 3. Wrote III. Prototype GUI
Team member B - 20240782 Youngdo Han
1. Made V.3. User System Use Case Diagrams 2. Wrote VI.4. User System Use Cases 3. Made VII.3 User System Sequence Diagrams
Team member C - 20240905 Bumgyu Suh
1. Wrote II. Project Schedule 2. Wrote IX. Meeting Logs 3. Made VII.2. Security Sequence Diagram
Team member D - 20240951 Mohamed Elnakeeb
1. Made V.1. Surveillance Use Case Diagram 2. Wrote VI.1. Surveillance Use Cases 3. Made VII.1. Surveillance Sequence Diagrams 4. Wrote I. Overview section

IX. Meeting logs

Meeting Logs specify the attendees by the first letter of their first names: Bumgyu (B), Hichan (H), Nakeeb (N), Youngdo (Y)

1. Meeting #1 - Initial SafeHome SRS Discussion

Date: 2025-10-25
Time: 13:00~16:00
Location: N13 2106 + Zoom

a. Meeting Objective

This is the first discussion in the series of meetings focused on the development of the Software Requirements Specification (SRS) for the SafeHome project. The primary goal of this meeting is to establish the framework for collaboration, assign initial tasks, do a general review of what the SRS needs to cover (security, functionality, scope, etc.), and finally define the roles and responsibilities of team members for the SRS creation process.

b. Discussion Notes

1. Collaboration / Tools
    i. Trello will be used to manage tasks via a Kanban-style board.
    ii. Google Docs will be used for documenting the SRS with shared editing.
    iii. Discord remains the primary quick-communication channel.
    iv. Meeting logs are also being actively maintained.
2. Team Workflow
    i. Tasks will be assigned by card on Trello with deadlines and responsible members.
    ii. There will be a “review / done” process so finished parts are checked by another member.
    iii. Glossary will be collaboratively built: each person adds terms related to the section they are working on.
3. Meeting Schedule
    i. Regular working meetings agreed: Monday 4 PM & Thursday 4 PM
    ii. Wednesday meetings are likely NOT possible.
    iii. One more check-in / review meeting is expected Friday morning before submission.
4. SRS Structure Decisions
    i. System will be divided into two functional areas: Surveillance system (cameras) & Security system (sensors + alarms + locks)
    ii. Doorbell/door lock with camera crosses both systems → tentatively placed under surveillance.

iii. A third category for "user & customization features (UX)" was created for functions like floor plans, permissions, etc.

5. Scope Clarifications
   i. SafeHome may be used in other properties besides homes (e.g., stores), so terminology like "homeowner" will be generalized where needed.
   ii. Sensors will be grouped rather than described individually to avoid unnecessary complexity.
   iii. The system should meet minimum requirements, but unnecessary extra features will not be added due to time constraints.
6. Customization & Permissions
   i. Instead of "master + guest password," the group is switching to admin + user access levels.
   ii. Customization includes:
      1. Ability to assign which alarm/notification each sensor triggers.
      2. Custom security modes/schedules (vacation mode, night mode, etc.).
      3. Floor plan visualization will be included under UX.
7. Review & Timeline Management
   i. Final polishing will likely happen on deadline day, but core SRS content should be finished earlier.
   ii. The final deliverable will be checked with a review pass (possibly using ChatGPT).

c. Decisions Made
   1. The floor plan is view-only; users cannot redraw or redesign the layout
   2. Alarm system will be divided into physical alarms (sirens/lights) vs notification-based alarms (alerts/messages)
   3. "Profiles" will be referred to as "Modes", e.g. night mode, vacation mode, etc.
   4. Modes can be custom and saved, allowing users to quickly switch between sensor/alert configurations.
   5. A delay / filtering mechanism will exist for sensors to prevent false-positive triggers (e.g., wait-before-alarm logic)
   6. Camera-specific passwords will NOT be implemented — access control will be handled exclusively through user permissions instead
   7. The "door lock" is treated as a sensor, not a separate smart-lock subsystem (to keep scope manageable)
   8. Two access levels are confirmed: Admin and User (admin can create/remove users & set permissions; user has restricted access).
   9. Use cases for the SRS will be split by category: security, surveillance, and UX/UI use cases
   10. The product schedule will be drafted later in a separate working session and tracked in Trello rather than written during this meeting
   11. Team members should write directly into the shared SRS document when drafting use cases / sections, and log changes in Discord when updates are made

12. Scope will focus on implementable core features, avoiding feature bloat / “nice to haves” unless necessary for minimum functionality.
13. Sensor descriptions will be grouped categorically, not written one-by-one for every possible model/type.
14. Floor plan is considered a UI visualization aid, not a mapping or planning tool.
15. Trello will house task breakdown + ownership + deadlines going forward.
16. Working meetings will be held regularly (Monday 4PM and Thursday 4PM).

d. Task Assignments
    1. H: Sensor
    2. Y: Users + Modes
    3. B: Alarm
    4. N: Surveillance
    5. All: Write different Use Cases
        i. Fill up the format, draw diagram, (add words to glossary, add to assumptions)
        ii. Specify user-config parameters (and their possible defaults)
        iii. Draw use case diagrams

e. Next Meeting
    1. 2025-10-27 MON, 16:00 + potentially 2025-10-30 THURS, 16:00
    2. Agenda:
        i. Control panel vs web vs app
        ii. Have a meeting to make sure the Use Cases are compatible / no contradictions
        iii. Check each other’s graph
        iv. Combine (make the diagrams and text consistent) → Bumgyu

2. Meeting #2 - SafeHome SRS Revision Discussion

Date: 2025-10-27
Time: 16:00~17:00
Location: N10 Group Study Room 6

a. Meeting Objective

This is the second discussion in the series of meetings focused on the development of the Software Requirements Specification (SRS) for the SafeHome project. The primary goal of this meeting is to go over the changing requirements from additional clarification received earlier this day.

b. Discussion Notes
    1. The SRS should not deviate too far from the original template and expectations.

c. Decisions Made
    1. The Use Cases should be reviewed further before continuing onto the Use Case Diagrams and Sequence Diagrams.

d. Task Assignments & Responsibilities & Action Items & Follow-up
    1. H: Revise sensor use cases
    2. Y: enable/disable all/none, add configs for setting the digital alarms/emails
    3. B: finish Use Case Diagram by wednesday, Thursday → start working on sequence diagram
    4. N: add user permission thing to Use Cases
    5. All: continue with use cases
        i. Fill up the format, draw diagram, (add words to glossary, add to assumptions)
        ii. Specify user-config parameters (and their possible defaults)
        iii. Draw use case diagrams
e. Next Meeting
    1. 2025-10-30 THURS, 16:00
    2. Agenda: Progress report

3. Meeting #3 - Diagrams Discussion

Date: 2025-10-30
Time: 18:30~20:00
Location: ACC Study Room

a. Meeting Objective

This is the third discussion in the series of meetings focused on the development of the Software Requirements Specification (SRS) for the SafeHome project. The primary goal of this meeting is to decide on the formatting for the use case and sequence diagrams.

b. Discussion Notes
    1. Stuff left to do:
        i. Project Schedule Graph
        ii. Fix and Add Missing Prototype GUI
        iii. Organize order of Use Cases, and make sure that the references are correct
        iv. Assumptions:
        v. 1. Review your own work, find inconsistencies, and also add to “assumptions” and “glossary” if anything is missing
        vi. Review everyone’s work to find inconsistencies
        vii. Overview Section
        viii. Table of Contents (last)
c. Decisions Made
    1. Login → preconditions (obviously except for the “login” use case)
        i. Do we include permission to do something (with camera, with sensor etc) in preconditions?
    2. Not having user permission → “exception” section of use case text
    3. Use Case Diagram:
        i. Do not include “guest/admin” unless they are not associated to any use case directly
        ii. No LOGIN

4. Sequence diagram:
    i. Skip login
    ii. Combine exceptions to a single “alt” as much as possible
    iii. Remember to have responses in sequence diagram

d. Task Assignments & Responsibilities & Action Items & Follow-up
    1. B: Project Schedule Graph, finish the Meeting Logs (2nd and 3rd meetings), remake Hichan’s sequence diagrams
    2. H: GUI
    3. Y: Sequence Diagrams, Assumption&Glossary (check it last)
    4. N: Sequence Diagrams, Overview
    5. Everyone: review use cases, assumptions, glossary

e. Next Meeting
    1. 2025-10-31 FRI, 14:00
    2. Agenda: Finalization

4. Meeting #4 - Finalization

Date: 2025-10-31
Time: 14:00~15:00
Location: Group Study Room 1

a. Meeting Objective

This is the third discussion in the series of meetings focused on the development of the Software Requirements Specification (SRS) for the SafeHome project. The primary goal of this meeting is to decide on the formatting for the use case and sequence diagrams.

b. Discussion Notes
    1. Stuff left to do:
        i. Who Did What section
        ii. Fix Sequence Diagram format
        iii. Fix Common Use Cases formatting (match the rest)

c. Decisions Made
    1. Sequence diagrams
        i. Put exceptions after the normal route
        ii. Put titles outside the image
        iii. Follow the “alt” box format
        iv. Get rid of blue underline font

d. Task Assignments & Responsibilities & Action Items & Follow-up
    1. B: finish the Meeting Logs (4th Log, review others), remake Hichan’s sequence diagrams
    2. H: GUI → Configuration, remake Security Use Case Diagram in plantUML
    3. Y: Fix sequence diagrams, Assumption&Glossary (check it last)
    4. N: Overview, fix sequence diagrams, unify Use Cases Format
    5. Everyone: who did what section, assumptions, glossary, “homeowner” → user/admin

X. Glossary

1. SafeHome: the software running in the SafeHome hardware product installed in the Homeowner's home
2. User: an account that anyway
3. Admin: the user that has unlimited access to other users and devices
4. Surveillance: Functions related to cameras
5. Security: Functions related to alarms/sensors
6. Device: a peripheral that can be connected to the central SafeHome hardware, and therefore be controlled by SafeHome. All devices should be able to be Enabled, Disabled, and Tested (that it is working properly with no errors). Examples:
    1. Camera: video camera installed in various rooms at home
    2. Alarm: makes a loud noise/flashing lights when triggered
    3. Sensors: receive some kind of signal, like a motion detection sensor, and reacts accordingly
7. SafeHome Interface: the GUI used by the user to interact with SafeHome, whether through the web or through the control panel.
8. Camera Thumbnail: a screenshot of the camera's view taken in the last minute, which is displayed in the "Thumbnail view"
9. Camera view: Whenever a specific camera is selected it shows a "View" with the camera footage and several buttons at the bottom
10. Floor plan: A graphical representation of the floor plan that the SafeHome is in, it shows room layout and devices
11. Safety zone: A disjoint set of sensors that is activated and deactivated together.
12. Security mode: A set of safety zones that will be enabled in this mode. Three named modes {Home, Away, Sleep} exist and can be configured by the user. More can be added.