CS350 Safehome Project
Software Requirement Specification (SRS)

Project Team #2 Members:

20220686	최민준
20200315	성대규
20230704	조성호
20230091	김민경

Table of Contents

I. Overview

1. Introduction

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

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

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

2. Goal

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

Functional goal is to provide the followings:

- Security functions
- Surveillance functions

Non-functional goal is as follows:

- To fulfill customer satisfaction
- To provide highest level of assurance and guarantee
- Timely release of product
- To make profit

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

- *Completeness* - The Safehome system we develop has all the function specified in the function requirements below.
- *Reliability* - The Safehome system we develops provide reliable services for all the function even in an emergency or an unexpected situation.
- *Simplicity* - We follow the basic principle, "Keep It Simple," in the entire process framework: communication, planning, modeling, construction and So the entire development process is not very complex and the time to process the work is managed within the planned schedule.
- *Customized service* - The Safehome system should be configured for a specific homeowners' environment considering the house, life pattern, and personal requirements.
- *User-friendliness* - The Safehome system has user-friendly interface that homeowners can access anywhere, anytime with ease.

3. Major Functionalities

1) Security Management

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

master password, and configuring system settings such as delay time, master password, guest password, phone number.

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

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

2) Surveillance Management

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

3) Future extentions

Future increments of the SafeHome product will extend beyond security and surveillance to provide comprehensive home automation capabilities. The system will support remote control over telephone interfaces, allowing users to manage key functions even while away from home. Additional features will include integration with answering machines, smart lighting control, heating and air conditioning management, and operation of home entertainment devices. These enhancements will enable users to monitor, configure, and control their home environment conveniently through both local and remote access, ultimately transforming SafeHome into a complete intelligent home management system.

II. Project Schedule

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

ID	Named process	Begins	Ends
1	Beginning of the project	Oct 20, 2025	
2	Initial requirement gathering	Oct 21, 2025	Oct 31, 2025
3	Planning and creating analysis model	Oct 21, 2025	Oct 31, 2025
4	Creating design model	Nov 1, 2025	Nov 14, 2025
5	Construction & testing	Nov 15, 2025	Dec 1, 2025
6	Testing & bug fixing	Dec 2, 2025	Dec 20, 2025
7	First deployment	Dec 21, 2025	

III. Prototype GUI

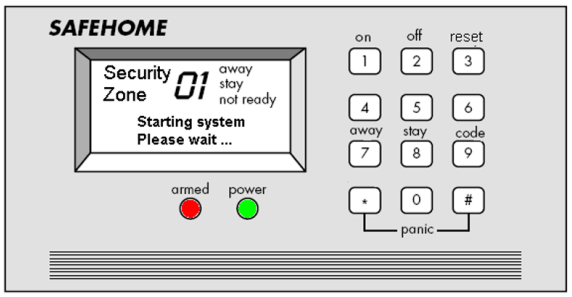


Fig 1. Control Panel

Fig 2. Login Screen

Fig 3. Main Functions

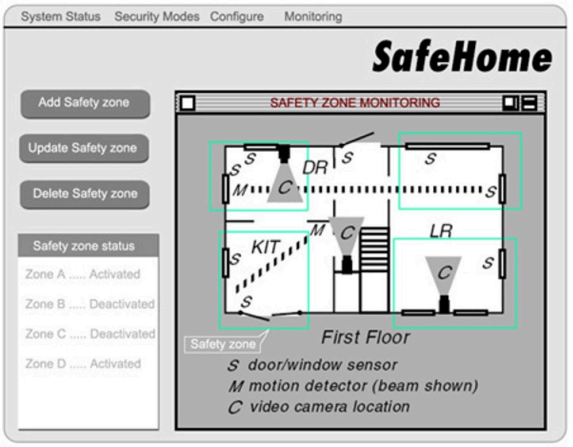


Fig 4. Security Function - Safety zone

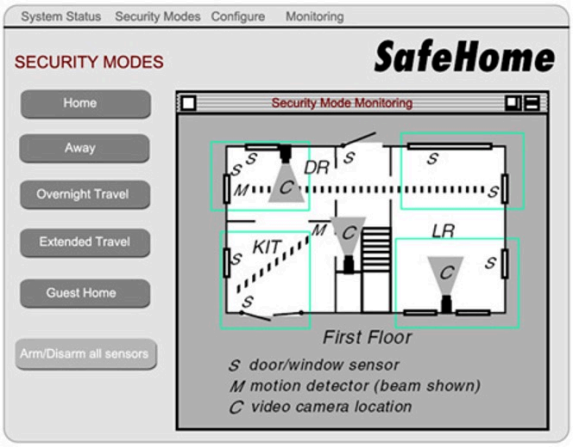


Fig 5. Security Function - Security Mode

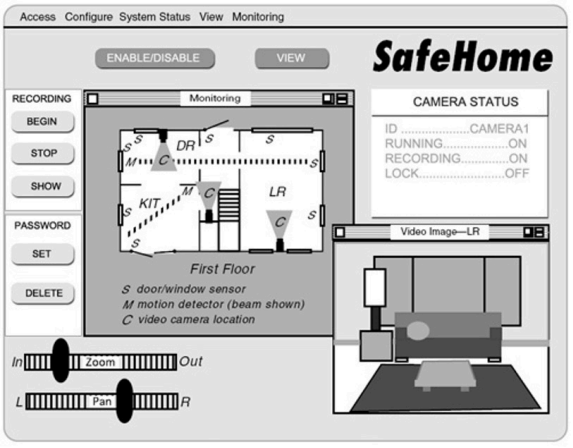


Fig 6. Surveillance Function

IV. Assumptions

📌 Note. Slide <x> refers to the slide # in Safehome_dialog.pptx. Meeting <d> refers to meeting <d>.

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

b. The Web page would have to be secure, encrypted, to guarantee that user's insformation is safe. (slide 20)
c. Web page login requires a 8-character password. (slide 20)
d. "Log onto web page" on slide 20 is described in the use case "Log onto the system through web browser"
e. Reconfiguring floor plan or relocating the sensors/cameras in slide 21 is to be implemented in the next increment.
f. "Arm/disarm each sensor" on slide 21 is not implemented because we only consider arm/disarm sensors of each safety zone.
g. "Thumbnail views" on slide 31 is specified in the use case "View thumbnail shots"
h. Overnight travel and extended travel mode on slide 39 are to be implemented in the next increment.
i. "encounters an error condition" on slide 45 is not defined as an use case but is described in exceptions of each use cases
j. "Doggie angst" sensor on slide 58 is considered to be implemented in the next increment
k. "system administrator" in our use case scenarios is not a person who is in charge of managing the system. It is the system itself acting as a facilitator for the use of system functionalities. (slide 69)
l. We added function to view intrusion log on the web page. It is described in use case "View intrusion log"
m. "login" includes master login and guest login, which differ in abilities.
n. Sensors recognize normal and abnormal usage.
o. All sensors, the control panel, and the system administrator are connected to the internet without delay.
p. A house that uses "Safehome" has one control panel, installed next to the entrance.
q. The system processes requests in a sequential manner, without concurrency. (meeting 1)
r. The website does not allow simultaneous logins from multiple devices using the same account. (meeting 1)

s. All user IDs for the website are unique, cannot be changed. (meeting 2)

t. The control panel has a battery and can turn the led on at any state. (meeting 2)

u. If no action is taken while logged into the panel, it will automatically log out after 30 seconds. (meeting 2)

v. If no action is taken while logged into the web interface, it will automatically log out according to the configured setting with default setting of 5 minutes (meeting 2)

w. Input sequence configuration of the control panel is out of project scope. (meeting 2)

x. The database is consistent, always synchronized with user input. (meeting 2)

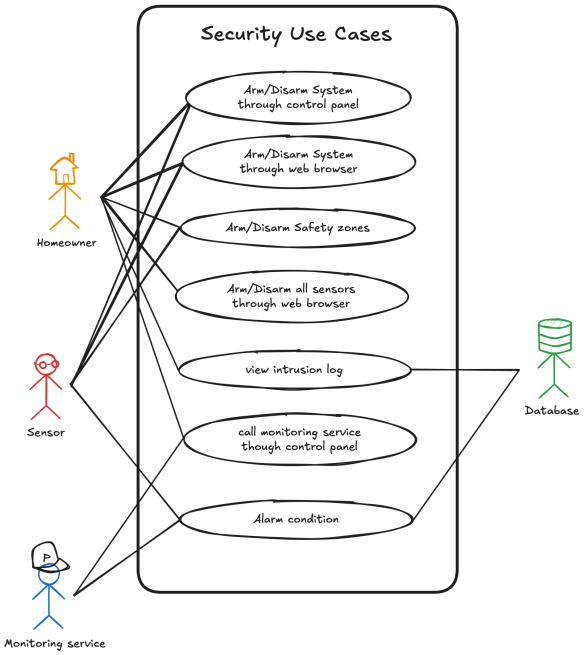
y. Control panel login requires a 4-digit password. (decided based on slide 90, discussed in meeting 2)

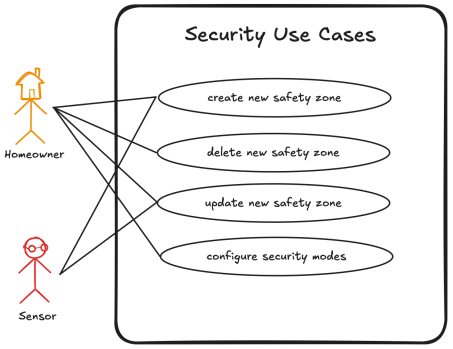
z. Information of sensors are saved as coordinates on the floor plan when floor plan is registered. Setting the coordinates are out of project scope. (meeting 3)

V. Use Case Diagrams

1. Common Functions

2. Security Functions





3. Surveillance Functions

VI. Use Cases

1. Common Use Cases

a. Log onto the system through control panel

Use case: Log onto the system through control panel

Primary actor: Homeowner, Guest

Goal in context: To log onto the Safehome system through control panel

Preconditions:

1. System has been configured.
2. Appropriate password must be obtained.
3. Control panel turns on - See use case: “Turn the system on”

Trigger: The homeowner/guest decides to log onto the system.

Scenario:

1. The homeowner/guest uses the control panel.

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

Exception:

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

3b. Password incorrect or not recognized. - The system asks for password again, and if the homeowner/guest enters incorrect or unrecognizable password three times in a row the system locks itself for predefined time.

Priority: High(essential) priority.

When available: First increment.

Frequency of use: Frequent

Channel to actor: Control panel

Secondary actors: System administrator

Channel to secondary actors:

1. System administrator: PC-based system

Open issues:

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

b. Log onto the system through web browser

Use case: Log onto the system through web browser

Primary actor: Homeowner

Goal in context: To log onto the Safehome system through web browser

Preconditions:

1. System has been configured.
2. Appropriate ID and password must be obtained.

Trigger: The homeowner decides to log onto the system.

Scenario:

1. The homeowner uses the web browser.
2. The homeowner enters master ID and password. (Password with 8 characters including letters)
3. The system validates ID and password.
4. The system displays accessible functions on the web browser.

Exception:

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

3b. Either ID or Password incorrect or not recognized - The system asks for ID and password again, and if the homeowner enters incorrect or unrecognizable ID & password three times in a row the system locks itself for predefined time.

Priority: High(essential) priority.

When available: First increment.

Frequency of use: Frequent.

Channel to actor: Web application.

Secondary actors: System administrator

Channel to secondary actors:

1. System administrator: PC-based system

Open issues:

1. What mechanisms protect unauthorized use from hacker of the internet?

c. Configure system setting

Use case: Configure system setting

Primary actor: Homeowner

Goal in context: Set configure system to satisfies user’s needs.

Preconditions:

Trigger: The homeowner decides to set configure system

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner selects “configure” button.
3. The system displays “configure system setting” through web.
4. The homeowner changes setting as desired. (e.g. changing Password, Language Settings, Bug report, Q&A, Setting Alarm Delay Time)
5. The system asks the homeowner to confirm whether to save the changes.
6. The homeowner confirms to save the changes.
7. The system changes settings in the database as the homeowner changed.

Exception:

1-6a. An alarm condition is encountered – See use case: “alarm condition encountered”

5b. The homeowner declined to save the changes. - The system asks confirmation, and if the homeowner selects ‘yes’ button, return to main screen without saving changes. If the homeowner selects ‘no’ button, return to configure system setting screen.

Priority: Medium priority.

When available: First increment.

Frequency of use: Rare.

Channel to actor: Web application.

Secondary actors: System administrator, Database

Channel to secondary actors:

1. System administrator: PC-based system
2. Database: HTTP/HTTPS Request (API call)

Open issues:

1. What are the default settings set before user configuration?

d. Turn the system on

Use case: Turn the system on

Primary actor: Homeowner

Goal in context: Turn the system on

Preconditions:

1. System is turned off.

Trigger: The homeowner decides to set configure system

Scenario:

1. The homeowner presses ‘On’ button.
2. The power LED turns green and blinks until the sensor test is complete.
3. The system turns on, and make all functions available including alarm system and log system.
4. The system turns on the sensors.
5. The system turns on the cameras.
6. All devices are reset to the disarmed state.
7. The system performs the testing process for each sensor.
8. The system gets whether each sensor having problem or not.
9. The homeowner logs onto the system – see use case : “Log onto the system through control panel”
10. The system displays the status of the sensors, indicating whether all sensors are normal and which sensors have issues.
11. The power LED stops blinking and remains lit in green.

Exception:

2-4a. An alarm condition is encountered – See use case: “alarm condition encountered”

Priority: High(essential) priority.

When available: First increment.

Frequency of use: Occasional.

Channel to actor: Control panel

Secondary actors: System administrator, Sensors (doors, windows, motion detectors), Camera

Channel to secondary actors:

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

Open issues:

1. What happens if sensor connection error occurs for some sensors?
2. How can sensor security be assured at connection?

e. Turn the system off

Use case: Turn the system off

Primary actor: Homeowner

Goal in context: Turn the system off

Preconditions:

1. The system is turned on

Trigger: The homeowner decides to turn the system off

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through control panel”
2. The homeowner presses “Off” button.
3. The system turns off, and makes all functions unavailable.
4. The system turns off the sensors.
5. The system turns off the cameras.
6. The power LED turns red.

Priority: High(essential) priority,

When available: First increment.

Frequency of use: Occasional.

Channel to actor: Control panel

Secondary actors: System administrator, Sensors (doors, windows, motion detectors), Camera

Channel to secondary actors:

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

Open issues:

1. How can we check no error occurs while turning off the system?

f. Reset the system

Use case: Reset the system

Primary actor: Homeowner

Goal in context: reset configure system to default

Preconditions:

1. The system is turned on

Trigger: The homeowner decides to reset the system

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through control panel”
2. The homeowner presses “reset” button.
3. The system asks the homeowner to confirm resetting the system.
4. The homeowner confirms to reset the changes.
5. The system changes settings to default except password.

Exception:

1-5a. An alarm condition is encountered – See use case: “alarm condition encountered”

4b. The homeowner declined to reset the system. - The system return to configure system setting

Priority: Medium priority.

When available: First increment.

Frequency of use: Rare.

Channel to actor: Control panel

Secondary actors: System administrator

Channel to secondary actors:

1. System administrator: PC-based system

Open issues:

1. What happens after reset is done?
2. How can we prevent malicious reset processes?

g. Change master password through control panel

Use case: Change master password through control panel

Primary actor: Homeowner

Goal in context: Change master password

Preconditions:

1. Current appropriate password must be obtained.

Trigger: The homeowner decides to change master password

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through control panel”
2. The homeowner activates ‘change master password’ input sequence.
3. The system displays one field for entering the current password and two fields for entering the new password.
4. The homeowner types current appropriate password, and types new password for both two fields.
5. The system checks whether typed current password is appropriate.
6. The system checks whether typed new passwords are same.
7. The system changes the master password.

Exception:

1-6a. An alarm condition is encountered – See use case: “alarm condition encountered”

4b. Typed current password is not appropriate. - The system asks for type current password again, and if the homeowner enters incorrect or unrecognizable password three times in a row the system locks itself for predefined time.

5b. Typed new passwords are not same. - The system asks for type new password of last field again.

Priority: Medium priority.

When available: First increment.

Frequency of use: Rare.

Channel to actor: Control panel

Secondary actors: System administrator

Channel to secondary actors:

1. System administrator: PC-based system

Open issues:

1. How can we prevent malicious reset processes?

2. Security Use Cases

a. Arm/disarm system through control panel

Use case: Arm/disarm system through control panel

Primary actor: Homeowner

Goal in context: Arm/disarm the system

Preconditions:

1. The system is running.
2. Logged in to system with homeowner account.

Trigger: The homeowner decides to arm/disarm the system

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner presses “home” button or “away” button.
3. The system activates/deactivates sensors according to home/away condition.
4. The homeowner observes red light indicating armed or no light indicting disarmed on the “armed” LED.

Exception:

1-4a. An alarm condition is encountered. - See use case: “An alarm condition encountered”

2b. The homeowner pressed “away” button but some of the doors and windows are not closed. - Control panel displays “Doors and windows are not closed” and makes beep sound

Priority: High priority

When available: First increment.

Frequency of use: Frequent.

Channel to actor: Control panel

Secondary actors: System administrator, Sensors (doors, windows, motion detectors)

Channel to secondary actors:

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

Open issues:

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

b. Arm/disarm system through web browser

Use case: Arm/disarm system through web browser

Primary actor: Homeowner

Goal in context: Arm/disarm the system

Preconditions:

1. The system is running.
2. Logged onto the system through web browser with homeowner account.

Trigger: The homeowner decides to arm/disarm the system

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner selects “Security”.
3. The system displays security page on web.
4. The homeowner selects “Security modes”
5. The system displays security modes page on web.
6. The homeowner selects “home” button or “away” button (or user-defined security modes).
7. The system activates/deactivates sensors according to home/away condition.
8. Homeowner observes message “The system is home mode” or “The system is away mode” on the web browser.

Exception:

1-8a. An alarm condition is encountered. - See use case: “An alarm condition encountered”

6b. It is already in the selected mode - The button for current state is disabled.

7b. The homeowner pressed disarm button but some of the doors and windows are not closed. - Web browser displays “Doors and windows are not closed” and mode does not change.

7c. Sensor testing fails when arming. - Display message “A sensor is malfunctioning” and state does not change.

Priority: High priority.

When available: First increment.

Frequency of use: Frequent.

Channel to actor: Web application.

Secondary actors: System administrator, Sensors (doors, windows, motion detectors)

Channel to secondary actors:

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

Open issues:

1. What mechanisms protect unauthorized use of this capability by employees of the company?
2. Is security sufficient? Other people must not be able to change the system state

c. Arm/disarm safety zone selectively

Use case: Arm/disarm safety zone selectively

Primary actor: Homeowner

Goal in context: Arm/disarm only certain parts of the house.

Preconditions:

1. The system is running.
2. Logged onto the system through web browser with homeowner account.
3. Safety zones are configured.

Trigger: The homeowner decides to arm/disarm safety zones selectively.

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner selects “Security”.
3. The system displays security page on web.
4. The homeowner selects “Configure”.
5. The system displays list of safe zones and their status on web.

6. The homeowner selects buttons for each safe zone to toggle its state of armed/disarmed.
7. The system displays “changing...” on web next to the selected safe zone.
8. The system activates/deactivates sensors belongs to each safe zone.
9. Homeowner observes change in the states of safe zones on web browser.

Exception:

1-9a. An alarm condition is encountered. - See use case: “An alarm condition encountered”

3b. The floor plan is not configured - Web browser displays empty screen with “Floor plan is not configured”.

5b. There is no configured safe zone -Web browser displays “No safe zone” in the list of safe zones box.

8b. The homeowner deactivates a safe zone but some of windows and doors in that safe zone are not closed - Web browser displays “Doors and windows are not closed”

8c. Sensor testing fails when arming. - Display message “A sensor is malfunctioning” and state does not change.

Priority: Medium priority

When available: First increment.

Frequency of use: Frequent.

Channel to actor: Web application, Internet connection to SafeHome website

Secondary actors: System administrator, Sensors (doors, windows, motion detectors)

Channel to secondary actors:

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

Open issues:

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

2. Is security sufficient? Other people must not be able to change the system state.

d. Arm/disarm all sensors through web browser

Use case: Arm/disarm all sensors through web browser

Primary actor: Homeowner

Goal in context: Arm/disarm all sensors

Preconditions:

1. The system is running.
2. Logged onto the system through web browser with homeowner account.

Trigger: The homeowner decides to arm/disarm all sensors

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner selects “Security”.
3. The system displays security page on web.
4. The homeowner selects “Security modes”.
5. The system displays security modes page on web.
6. The homeowner selects “arm/disarm all sensors” button.
7. The system activates/deactivates all sensors.
8. Homeowner observes message “All sensors are armed/disarmed” on the web browser.

Exception:

1-8a. An alarm condition is encountered. - See use case: “An alarm condition encountered”

6b. The sensors are already all activated/deactivated - The button is disabled accordingly

7b. The homeowner pressed disarm button but some of the doors and windows are not closed. - Web browser displays “Doors and windows are not closed” and mode does not change.

7c. Sensor testing fails when arming. - Display message “A sensor is malfunctioning” and state does not change.

Priority: Medium priority.

When available: First increment.

Frequency of use: Occasional.

Channel to actor: Web application.

Secondary actors: System administrator, Sensors (doors, windows, motion detectors)

Channel to secondary actors:

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

Open issues:

1. What mechanisms protect unauthorized use of this capability by employees of the company?
2. Is security sufficient? Other people must not be able to change the system state

e. Alarm condition encountered

Use case: Alarm condition encountered

Primary actor: System administrator

Goal in context: Make safety warning to homeowner and notify monitoring service to make further investigation.

Preconditions:

1. The system is running.
2. One or more armed sensors detects security hazard. More specifically, when an armed door/window sensor detects door/window opening, or when an armed motion sensor detects motion.

Trigger: Armed sensor detects security hazard.

Scenario:

1. One or more armed sensor alerts alarm condition has been encountered.

2. The system starts countdown for alarm and the speaker makes a noise audible in ? meters. (level 1 alert)
3. The system displays “Security warning” on the web.
4. The “Armed” LED starts blinking red light.
5. The user inputs password to turn the alarm off.
6. The user presses “Stop alarm”, then alarm is disabled.
7. If alarm is not turned off in user-set time (default: 5 minutes), the system increases the alarm level to 2 and speaker makes a noise audible in 20 meters.
8. The system calls the monitoring service.

Exception:

5a. The password is incorrect or not recognized - If input tries are less than three then prompts for reentry. Otherwise lock system for predefined time.
5b. The password is incorrect or not recognized and no input tries are remain - The system prevent the homeowner from accessing the control panel.

5c. Delay time is not configured - Regard it as 2 minutes.

Priority: High priority.

When available: First increment.

Frequency of use: Rare.

Channel to actor: Wireless connection

Secondary actors: Homeowner, Sensors (doors, windows, motion detectors), Speakers, Database

Channel to secondary actors:

1. Sensors: wireless connectivity
2. Speakers: hard-wired to control panel / wireless connection
3. Database: HTTP/HTTPS requests (API call)

Open issues:

1. If alarming condition is reached too frequently, monitoring service may fail to handle all of the monitoring service calls.

2. There should be enough time for users to nullify alarm condition. Because when countdown ends, the system will make very loud noise and call monitoring service.

f. Create new safety zone

Use case: Create new safety zone

Primary actor: Homeowner

Goal in context: To create a new safety zone for specific areas in the home

Preconditions:

1. System is running.
2. The floor plan is configured.
3. Logged in to system with homeowner account through web browser.
4. Sensors are registered to the system by their coordinates.

Trigger: The homeowner decides to create a new safety zone.

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner selects "Security" from the main menu.
3. The system displays security page on web.
4. The system displays a floor plan (1F) and the list of available floors.
5. The homeowner selects desired floor level.
6. The system displays floor plan of the selected level on web.
7. The homeowner selects “Add Safety Zone” from the menu.
8. The system prompts for safety zone name.
9. The homeowner inputs name.
10. The system prompts for safety zone area.
11. The homeowner selects level and draws a square on desired area.
12. The system displays list of sensors included in the zone, based on user input.

13. The system verifies the sensor connections and validates configuration.
14. The homeowner confirms creation.
15. The system saves the new safety zone in the database and displays created safety zone.
16. The system sets the new safety zone disarmed.
17. The system displays “Successfully created Safety Zone {name}”

Exception:

1-17a. An alarm condition is encountered. - See use case: “An alarm condition encountered”

8b. Duplicate safety zone name - The system requests a unique name.

12b. Selected sensor is already included in another safety zone - The system displays a warning and requests to change update details.

13b. Testing of sensor fails - Display “Sensor {} is malfunctioning” and abort the creation of Safety Zone.

15b. Failed to save Safety Zone in database (ran out of storage space) - Display “Failed to save Safety Zone” and abort the creation of Safety Zone.

Priority: Medium priority.

When available: First increment.

Frequency of use: Rare.

Channel to actor: Web Application.

Secondary actors: System administrator, Sensors (doors, windows, motion detectors)

Channel to secondary actors:

1. System administrator: PC-based system
2. Sensors: wireless connectivity
3. Database: HTTP/HTTPS requests (API call)

Open issues:

1. What if the homeowner wants to have Safety Zone not in the shape of rectangle?
2. How large the database should be?

g. Delete safety zone

Use case: Delete safety zone

Primary actor: Homeowner

Goal in context: Remove an existing safety zone.

Preconditions:

1. System is running.
2. The floor plan is configured.
3. Logged in to system with homeowner account through web browser.
4. At least one safety zone exists.

Trigger: The homeowner decides to delete an existing safety zone.

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner selects "Security" from the main menu.
3. The system displays security page on web.
4. The system displays a floor plan (1F) and the list of available floors.
5. The homeowner selects desired floor level.
6. The system displays floor plan of the selected level on web.
7. The homeowner selects “Delete Safety Zone” from the menu.
8. The homeowner selects a safety zone to delete.
9. The system displays information of selected safety zone (name, floor number, included sensors) and asks for confirmation.
10. The homeowner confirms deletion.
11. The system deletes the safety zone and displays “Successfully deleted Safety Zone {name}”

Exception:

1-11a. An alarm condition is encountered. - See use case: “An alarm condition encountered”

7b. There is no Safety Zone - The button is disabled accordingly.

8b. The homeowner did not selected on the Safety Zone area - Cancel the deletion of Safety Zone.

Priority: Medium priority.

When available: First increment.

Frequency of use: Rare.

Channel to actor: Web application.

Secondary actors: System administrator

Channel to secondary actors:

1. System administrator: PC-based system
2. Database: HTTP/HTTPS requests (API Call)

Open issues:

1. What happens if no safety zone is left after deleting?

h. Update an existing safety zone

Use case: Update an existing safety zone

Primary actor: Homeowner

Goal in context: Update details of an existing safety zone such as adding/removing sensors, renaming zone.

Preconditions:

1. System is running.
2. The floor plan is configured.
3. Logged in to system with homeowner account through web browser.
4. At least one safety zone exists.

Trigger: The homeowner decides to modify existing details of a safety zone.

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner selects "Security" from the main menu.

3. The system displays security page on web.
4. The system displays a floor plan (1F) and the list of available floors.
5. The homeowner selects desired floor level.
6. The system displays floor plan of the selected level on web.
7. The homeowner selects “Update Safety Zone” from the menu.
8. The homeowner selects the safety zone to update.
9. The system displays current configuration of the safety zone.
10. The homeowner updates one or more details.
11. The system tests the updated sensor connections and validates configuration.
12. The system displays updated information of selected safety zone and asks for confirmation.
13. The homeowner confirms changes.
14. The system saves the updated configuration to the database
15. The system displays “Successfully changed Safety Zone {name}”

Exception:

1-15a. An alarm condition is encountered. - See use case: “An alarm condition encountered”

5b. Desired level of homeowner is 1F(default) - No level selection required.

10b. Invalid or conflicting update on sensors - The system rejects update.

10c. Selected sensor is already included in another safety zone - The system displays a warning and requests to change update details.

14b. Failed to save Safety Zone in database (ran out of storage space) - Display “Failed to save Safety Zone” and abort the creation of Safety Zone.

Priority: Low priority.

Frequency of use: Rare.

Channel to actor: Web application.

Secondary actors: System administrator, Sensors (doors, windows, motion detectors)

Channel to secondary actors:

1. System administrator: PC-based system
2. Sensors: wireless connectivity
3. Database: HTTP/HTTPS requests (API call)

Open issues:

1. What if homeowner wants to have overlapping Safety Zones?

i. Configure Safehome modes

Use case: Configure Safehome modes

Primary actor: Homeowner

Goal in context: Configure basic states of Samehome system, enable making user-customed states.

Preconditions:

1. The homeowner is logged into the Safehome system.

Trigger: The homeowner wants to set/change Safehome modes

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner selects "Security" from the main menu.
3. The system displays security page on web.
4. The homeowner selects "Configure" from the menu.
5. The system displays a list of configurable Safehome modes on web. (e.g. home, away, 3 user-defined states)
6. The homeowner selects a mode to be set/configured.
7. The homeowner updates one or more details (e.g. name of mode, safety zones to be armed)
8. The system validates configuration and saves the updated configuration to the database.
9. The system displays “Successfully updated Safehome mode {name}”

Exception:

1-9a. An alarm condition is encountered. - See use case: “An alarm condition encountered”

7b. Duplicate mode name - The system requests a unique name.

Priority: Medium priority.

When available: First increment.

Frequency of use: Rare.

Channel to actor: Web application.

Secondary actors: System administrator, Database

Channel to secondary actors:

1. System administrator: PC-based system
2. Database: HTTP/HTTPS requests (API call)

Open issues:

1. What happens if the homeowner changes the configuration of currently active SafeHome mode?

j. View intrusion log

Use case: View intrusion log

Primary actor: Homeowner

Goal in context: Show the homeowner records of past intrusion events detected by the Safehome system

Preconditions:

1. The homeowner is logged into the Safehome system.
2. Intrusion logs have been saved to the system.

Trigger: The homeowner decides to view intrusion logs.

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner selects "Security" from the main menu.
3. The system displays security page on web.

4. The homeowner selects "Monitoring" from the menu.
5. The system retrieves stored intrusion records from the log database.
6. The system displays a list of recorded intrusion events with date, time, and zone information on web.
7. The homeowner selects an individual event.
8. The system displays full details of the selected event, such as number of the triggered sensor and alarm status.

Exception:

1-8a. An alarm condition is encountered. - See use case: “An alarm condition encountered”
4a. No detected intrusion logs found in database - The system displays “No intrusion records found.”

Priority: Low priority.
When available: First increment.
Frequency of use: Rare.

Channel to actor: Web application.

Secondary actors: System administrator, Database

Channel to secondary actors:

1. System administrator: PC-based system
2. Database: HTTP/HTTPS requests (API call)

Open issues:

1. In what order we want to display the logs? Sort-by-date or higher alarm level first?

k. Call monitoring service through control panel 32

Use case: Call monitoring service through control panel

Primary actor: Homeowner / Guest

Goal in context: Call monitoring service.

Preconditions:

1. The system is running.

Trigger: A person tries to reach help through SafeHome system.

Scenario:

1. A person presses the “*” and “#” buttons at the same time representing panic signal.
2. Control Panel sends call to monitoring service.
3. Control Panel makes loud noise which is audible in 30 meters. (alarm level 2)
4. The system leaves the log about alarm condition.

Exception:

Priority: High priority.
When available: First increment.
Frequency of use: Rare.

Channel to actor: Control panel

Secondary actors: System administrator, Monitoring Service

Channel to secondary actors:

1. System administrator: PC-based system
2. Monitoring Service: Internet

Open issues:

1. What are the possibilities of mistaken input?

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:

1. Systems should be ready, and internet should be set.
2. Appropriate user ID and passwords must be obtained.

Trigger: Homeowner decides to take a look of 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 homeowner selects “pick a camera”
4. The system displays the floor plan of the house.
5. The homeowner selects a camera icon from the floor plan
6. The system asks a password if the selected camera has a password.
7. The homeowner enters the password.
8. The system requests database for the password.
9. The database sends password.
10. The system validates the password.
11. The system displays the state of the selected camera.
12. The homeowner selects the "view" button.
13. The system requests video frame to Camera.
14. The camera sends video frame.
15. The system displays video output within the viewing window at one frame per second.

Exceptions:

1-15a. An alarm condition is encountered. - See use case: “An alarm condition encountered”

3b. Homeowner selects "all cameras" - See use-case: "view thumbnail snapshots”
6b. The camera does not have a password - Go to procedure 9.
8b. The password is incorrect or not recognized - If input tries are less than three then prompts for reentry. Otherwise lock system for predefined time.
8c. The password is incorrect or not recognized and no input tries are remain - The system prevent the homeowner from accessing the camera .
10b. If the camera is disabled, “view” button is disabled – See use case : “Enable camera”

Priority: Medium priority.

When available: First increment

Frequency of use: Occasional.

Channel to actor: Web application.

Secondary actor: System administrator, Camera

Channels to secondary actors:

1. System administrator: PC-based system
2. 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 control visual aspect (panning, zooming) of camera's view.

Preconditions:

1. Systems should be ready, and internet should be set.
2. Appropriate user ID and passwords must be obtained.

Trigger: Homeowner decides to control a view of camera.

Scenario:

1. The homeowner logs onto the system – see use case : "Log onto the system through web browser"
2. The homeowner display camera view – See use case : "Display specific camera view"

3. The homeowner moves ‘Zoom’ button horizontally to zoom in or zoom out the camera.
4. The system sends zoom request to camera.
5. The camera zooms device according to the request.
6. The homeowner moves ‘Pan’ button horizontally to pan left or pan right the camera.
7. The system sends pan request to camera.
8. The camera pans device according to the request.

Exceptions:

1-8a. An alarm condition is encountered - See use case: "alarm condition encountered."

Priority: Low priority.

When available: First increment

Frequency of use: Occasional.

Channel to actor: Web application.

Secondary actor: System administrator, Camera

Channels to secondary actors:

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

Open Issues:

1. Will system response via the Internet be acceptable given the bandwidth required for camera views?
2. What if the homeowner forgets the specific password for the camera?
3. What if a specific camera is broken?
4. What if the panning is disable due to obstacles near by the camera?

c. Begin camera recording

Use Case: Begin camera recording

Primary actor: Homeowner

Goal In Context: To record the camera.

Preconditions:

1. Systems should be ready, and internet should be set.
2. Appropriate user ID and passwords must be obtained.
3. Sufficient space of recorded video storage (database) is available for more than specific size (one-day full recording size of all home cameras).

Trigger: Homeowner decides to record 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 homeowner selects “pick a camera”
4. The system displays the floor plan of the house.
5. The homeowner selects a camera icon from the floor plan
6. The system asks a password if the selected camera has a password.
7. The homeowner enters the password.
8. The system validates the password.
9. The system displays the state of the selected camera.
10. The homeowner selects “begin” for start recoding.
11. The system request camera to start recoding.
12. The system sets the recoding status to “on”
13. The camera starts recording.
14. The camera sends recorded frame to database.

Exceptions:

1-14a. An alarm condition is encountered - See use case: "alarm condition encountered."
3b. Homeowner selects "all cameras" - See use-case: "view thumbnail snapshots”
6b. If the camera does not have a password - Go to procedure 9.

8b. The password is incorrect or not recognized - If input tries are less than three then prompts for reentry. Otherwise lock system for predefined time.
8c. The password is incorrect or not recognized and no input tries are remain - The system prevent the homeowner from accessing the camera .

10b. The camera is already recording - “begin” button is disabled. See use case : “Enable camera”

Priority: Medium priority.

When available: First increment

Frequency of use: Frequent.

Channel to actor: Web application.

Secondary actor: System administrator, Camera, Database

Channels to secondary actors:

1. System administrator: PC-based system
2. Camera: wireless connectivity
3. Database: HTTP/HTTPS Request (API call)

Open Issues:

1. Will system response via the Internet be acceptable given the bandwidth required for camera views?
2. What if the recording storage size is not sufficient?
3. What if the homeowner forgets the specific password for the camera?
4. What if a specific camera is broken?

d. Stop camera recording

Use Case: Stop camera recording

Primary actor: Homeowner

Goal In Context: To stop recording the camera.

Preconditions:

1. Systems should be ready, and internet should be set.
2. Appropriate user ID and passwords must be obtained.

3. The camera is currently recording.

Trigger: Homeowner decides to stop recording a camera.

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner begins camera recording – see use case : “Begin camera recording”
3. The homeowner selects “stop” for stop recoding.
4. The system sends stop recording request to camera.
5. The system changes the recording status to “off”.
6. The camera stops recording video.

Exceptions:

1-6a. An alarm condition is encountered - See use case: "alarm condition encountered."

3b. The camera is disabled - “stop” button is disabled. See use case : “Enable camera”

Priority: Medium priority.

When available: First increment

Frequency of use: Frequent.

Channel to actor: Web application.

Secondary actor: System administrator, Camera, Database

Channels to secondary actors:

1. System administrator: PC-based system
2. Camera: wireless connectivity
3. Database: HTTP/HTTPS Request (API call)

Open Issues:

1. What if the homeowner forgets the specific password for the camera?
2. What if a specific camera is broken?

e. Replay camera recording

Use Case: Replay camera recording

Primary actor: Homeowner

Goal In Context: To replay recording of the camera.

Preconditions:

1. Systems should be ready, and internet should be set.
2. Appropriate user ID and passwords must be obtained.

Trigger: Homeowner decides to replay the recording 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 homeowner selects “pick a camera”
4. The system displays the floor plan of the house.
5. The homeowner selects a camera icon from the floor plan
6. The system asks a password if the selected camera has a password.
7. The homeowner enters the password.
8. The system validates the password.
9. The system displays the state of the selected camera.
10. The homeowner selects “show” for replay recoding.
11. The system requests recorded videos to database.
12. The database sends recorded videos to system.
13. The system displays the list of recoded video rows of the selected camera.
14. The homeowner selects specific row from recording list.
15. The system displays the recorded output in the viewing window at a rate of one frame per second.
16. The homeowner navigates the video backward or forward by interacting with the timeline control located at the bottom of the screen.

Exceptions:

1-16a. An alarm condition is encountered - See use case: "alarm condition encountered."

3b. Homeowner selects "all cameras" - See use-case: "view thumbnail snapshots”
6b. The camera does not have a password - Go to procedure 9.
8b. The password is incorrect or not recognized - If input tries are less than three then prompts for reentry. Otherwise lock system for predefined time.
8c. The password is incorrect or not recognized and no input tries are remain - The system prevent the homeowner from accessing the camera.

10b. The camera is disabled -“show” button is disabled . See use case : “Enable camera”.

13b. There is no recoding for the camera - Show empty list with the UI of text “No recoding available”.

16b. The video is starting point - Only navigate to backward (later) direction.

16c. The video is ending point - Only navigate to forward (earlier) direction.

Priority: Low priority.

When available: First increment

Frequency of use: Occasional.

Channel to actor: Web application.

Secondary actor: System administrator, Camera, Database.

Channels to secondary actors:

1. System administrator: PC-based system
2. Camera: wireless connectivity
3. Database: HTTP/HTTPS Request (API call)

Open Issues:

1. What if the homeowner forgets the specific password for the camera?

2. What if the recorded video is not available for technical reasons? (The file cannot be found, is partially corrupted, or metadata indicates incomplete recording).
3. What if the homeowner wants to delete specific record of video?

f. Set camera password

Use Case: Set camera password

Primary actor: Homeowner

Goal In Context: To set password of the camera.

Preconditions:

1. Systems should be ready, and internet should be set.
2. Appropriate user ID and passwords must be obtained.

Trigger: Homeowner decides to set password 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 homeowner selects “pick a camera”
4. The system displays the floor plan of the house.
5. The homeowner selects a camera icon from the floor plan
6. The system asks a password if the selected camera has a password.
7. The homeowner enters the password.
8. The system validates the password.
9. The system displays the state of the selected camera.
10. The homeowner selects “set” to configure a camera password.
11. The system displays 4 digits of input fields for password and password confirmation.
12. The homeowner enters the password.
13. The system validates the entered password for consistency and format.

14. The system request database to set new password of camera.
15. Upon successful validation, the system changes the camera’s lock status to “on”.

Exceptions:

1-15a. An alarm condition is encountered - See use case: "alarm condition encountered."

3b. Homeowner selects "all cameras" - See use case: "view thumbnail snapshots”
6b. The camera does not have a password - Go to procedure 9.
8b. The password is incorrect or not recognized - If input tries are less than three then prompts for reentry. Otherwise lock system for predefined time.
8c. The password is incorrect or not recognized and no input tries are remain - The system prevent the homeowner from accessing the camera.

10b. The camera is disabled - “set” button is disabled. See use case : “Enable camera”.

13b. The password and the password confirmation do not match - The system displays a message: “The passwords do not match.”

13c. The password or password confirmation does not meet the required format - The system displays a message: “The password is not valid.”

Priority: Low priority.

When available: First increment

Frequency of use: Rare.

Channel to actor: Web application.

Secondary actor: System administrator, Database

Channels to secondary actors:

1. System administrator: PC-based system.
2. Database: HTTP/HTTPS Request (API call)

Open Issues:

1. What if the homeowner forgets the specific password for the camera?

g. Delete camera password

Use Case: Delete camera password

Primary actor: Homeowner

Goal In Context: To delete password of the camera.

Preconditions:

1. Systems should be ready, and internet should be set.
2. Appropriate user ID and passwords must be obtained.

Trigger: Homeowner decides to delete password of a camera.

Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner sets camera password - see use case: “Set camera password”
3. The homeowner selects “delete” to delete a camera password.
4. The system requests database to delete password.
5. The database deletes the password.
6. The system changes the camera’s lock status to “off”.

Exceptions:

1-6a. An alarm condition is encountered - See use case: "alarm condition encountered."

Priority: Low priority.

When available: First increment

Frequency of use: Rare.

Channel to actor: Web application.

Secondary actor: System administrator, Database

Channels to secondary actors:

1. System administrator: PC-based system with web browser.
2. Database: HTTP/HTTPS Request (API call).

Open Issues:

1. What if the homeowner forgets the specific password for the camera?

h. View thumbnail Shots

Use Case: View thumbnail Shots

Primary actor: Homeowner

Goal In Context: To view thumbnail shots of the cameras.

Preconditions:

1. Systems should be ready, and internet should be set.
2. Appropriate user ID and passwords must be obtained.

Trigger: Homeowner decides to view thumbnail shots of cameras.

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 homeowner selects “all cameras”
4. The system requests cameras to send all thumbnails.
5. Cameras sends each thumbnails to system.
6. The system displays the grid view of thumbnails of cameras, while the locked camera (camera that has password and not unlocked) is showing locked screen.
7. The homeowner selects the locked thumbnail view.
8. The system asks a password of the camera.
9. The homeowner enters the password.
10. The system requests database to get password.
11. The database send password to system.
12. The system validates the password.
13. The system displays the thumbnail of unlocked camera.

Exceptions:

1-13a. An alarm condition is encountered - See use case: "alarm condition encountered."

9b. The password is incorrect or not recognized - If input tries are less than three then prompts for reentry. Otherwise lock the camera thumbnail for predefined time.
9c. The password is incorrect or not recognized and no input tries are remain - The system prevent the homeowner from viewing the camera thumbnail.

Priority: Low priority.

When available: First increment

Frequency of use: Occasional.

Channel to actor: Web application.

Secondary actor: System administrator, Camera

Channels to secondary actors:

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

Open Issues:

1. What if the homeowner forgets the specific password for the camera?
2. What if the thumbnail of camera cannot be enabled for other reasons? (camera is broken, camera is hacked)

i. Enable camera

Use Case: Enable camera

Primary actor: Homeowner

Goal In Context: To enable the camera.

Preconditions:

1. Systems should be ready, and internet should be set.
2. Appropriate user ID and passwords must be obtained.
3. The camera is disabled.

Trigger: Homeowner decides to enable 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 homeowner selects “pick a camera”
4. The system displays the floor plan of the house.
5. The homeowner selects a camera icon from the floor plan
6. The system asks a password if the selected camera has a password.
7. The homeowner enters the password.
8. The system validates the password.
9. The system displays the state of the selected camera.
10. The homeowner selects “enable/disable” to enable a camera.
11. After enabling, the system changes the camera’s running status to “on.”

Exceptions:

1-11a. An alarm condition is encountered - See use case: "alarm condition encountered."

3b. Homeowner selects "all cameras" - See use case: "view thumbnail snapshots”
6b. The camera does not have a password - Go to procedure 9.
8b. The password is incorrect or not recognized - If input tries are less than three then prompts for reentry. Otherwise lock system for predefined time.
8c. The password is incorrect or not recognized and no input tries are remain - The system prevent the homeowner from accessing the camera.

Priority: Medium priority.

When available: First increment

Frequency of use: Rare.

Channel to actor: Web application.

Secondary actor: System administrator, Camera

Channels to secondary actors:

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

Open Issues:

1. What if the homeowner forgets the specific password for the camera?
2. What if the camera cannot be enabled for other reasons? (camera is broken, camera is hacked)

j. Disable camera

Use Case: Disable camera

Primary actor: Homeowner

Goal In Context: To disable the camera.

Preconditions:

1. Systems should be ready, and internet should be set.
2. Appropriate user ID and passwords must be obtained.
3. The camera is enabled.

Trigger: Homeowner decides to disable 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 homeowner selects “pick a camera”
4. The system displays the floor plan of the house.
5. The homeowner selects a camera icon from the floor plan
6. The system asks a password if the selected camera has a password.
7. The homeowner enters the password.
8. The system validates the password.
9. The system displays the state of the selected camera.
10. The homeowner selects “enable/disable” to enable a camera.
11. After disabling, the system changes the camera’s running status to “off.”

Exceptions:

1-11a. An alarm condition is encountered - See use case: "alarm condition encountered."

3b Homeowner selects "all cameras" - See use case: "view thumbnail snapshots”
6b. The camera does not have a password - Go to procedure 9.
8b. The password is incorrect or not recognized - If input tries are less than three then prompts for reentry. Otherwise lock system for predefined time.
8c. The password is incorrect or not recognized and no input tries are remain - The system prevent the homeowner from accessing the camera.

Priority: Medium priority.

When available: First increment

Frequency of use: Rare.

Channel to actor: Web application.

Secondary actor: System administrator, Camera

Channels to secondary actors:

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

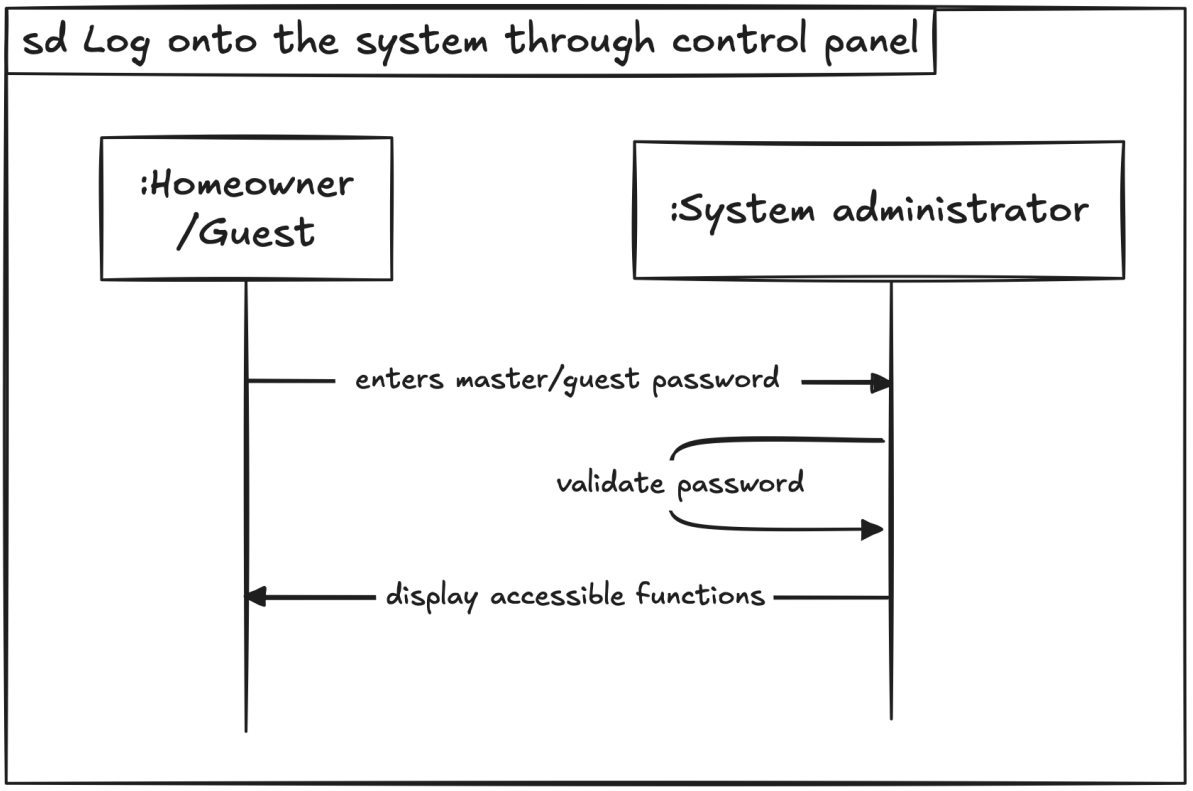
Open Issues:

1. What if the homeowner forgets the specific password for the camera?
2. What if the camera cannot be disabled for other reasons? (camera is broken, camera is hacked)

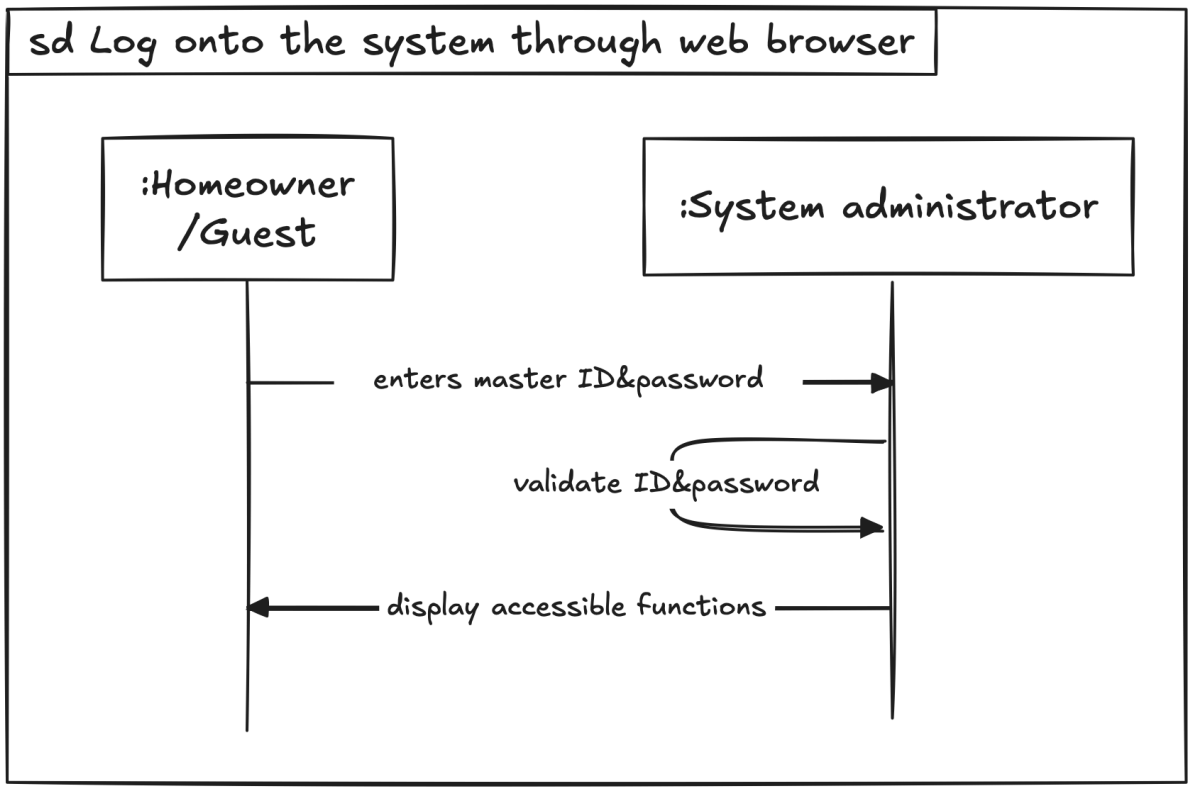
VII. Sequence Diagram

1. Common Sequence Diagram

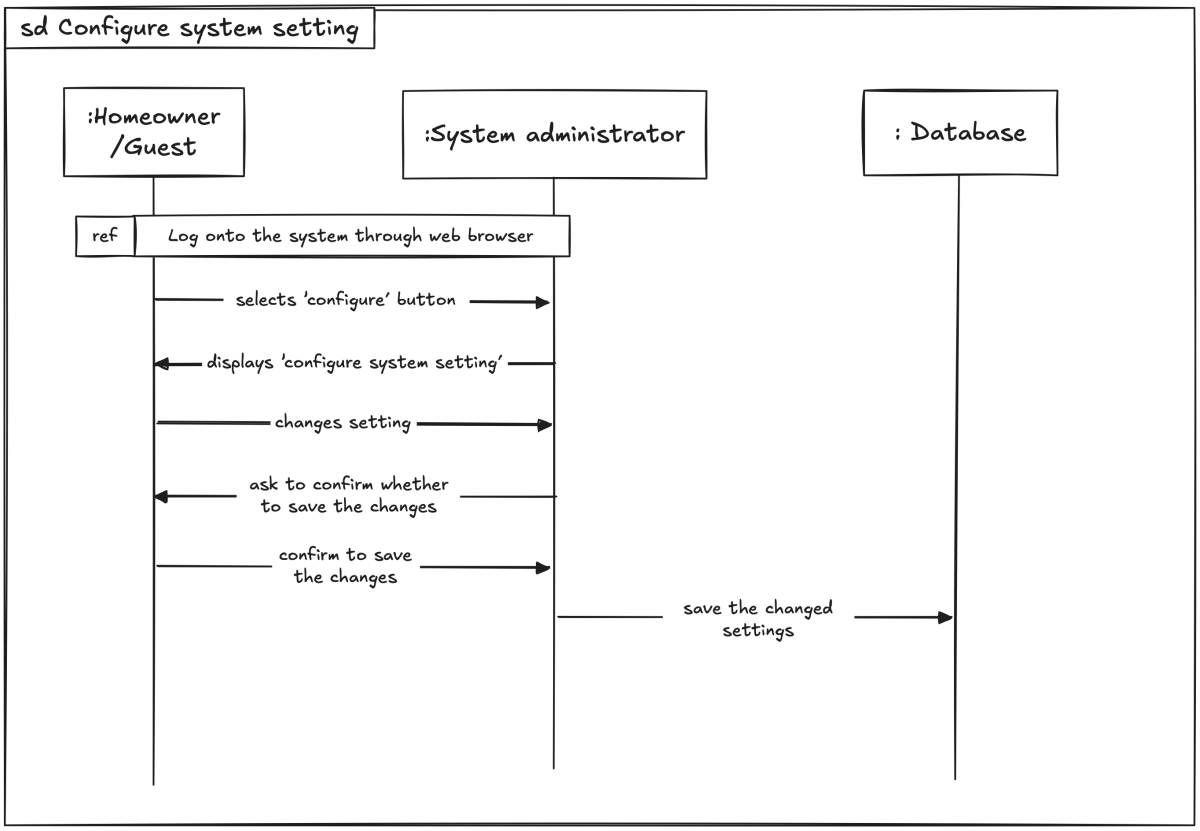
a. Log onto the system through control panel



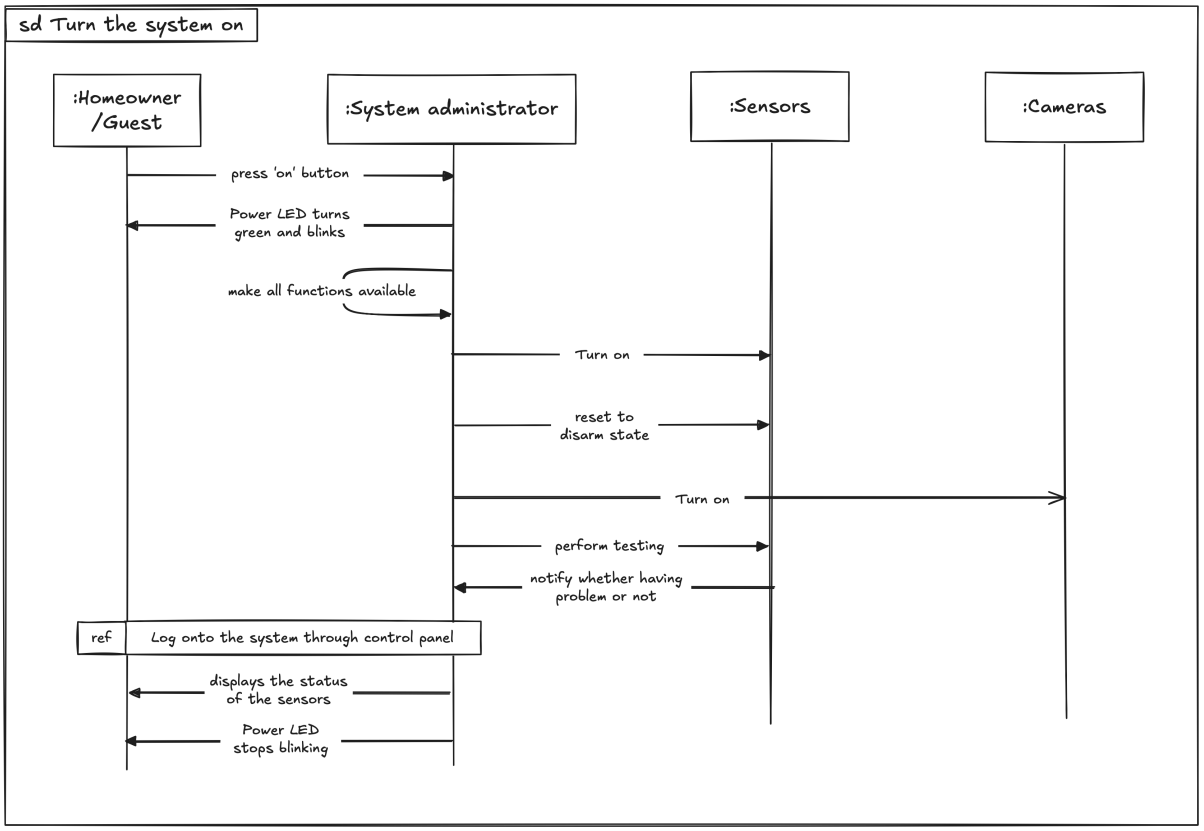
b. Log onto the system through web browse



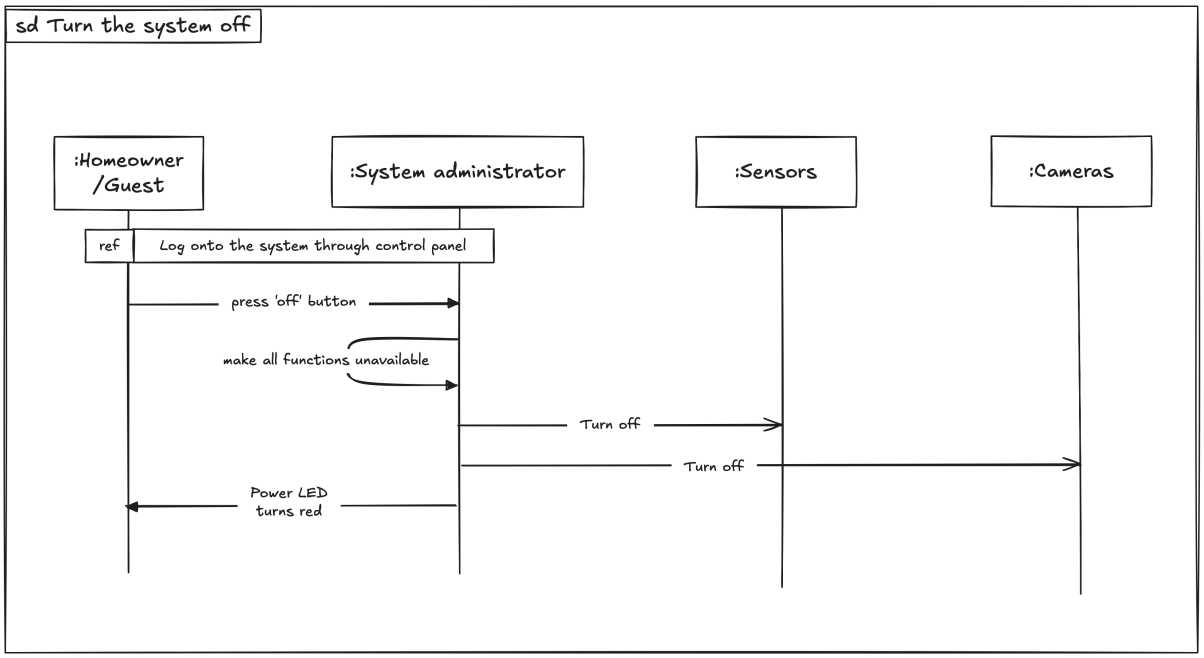
c. Configure system setting



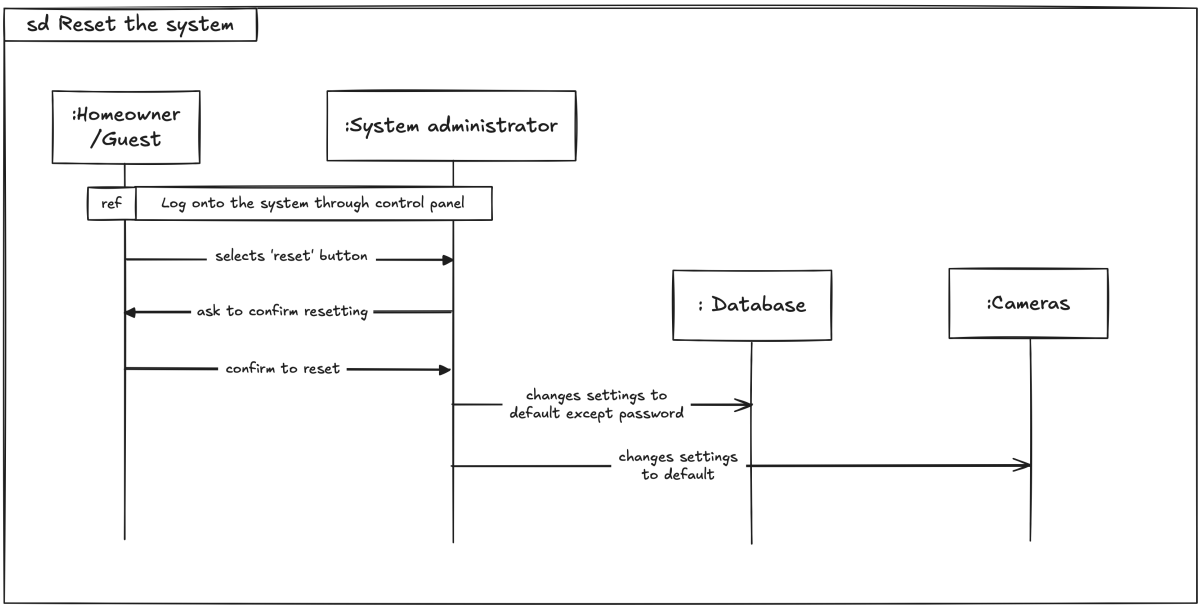
d. Turn the system on



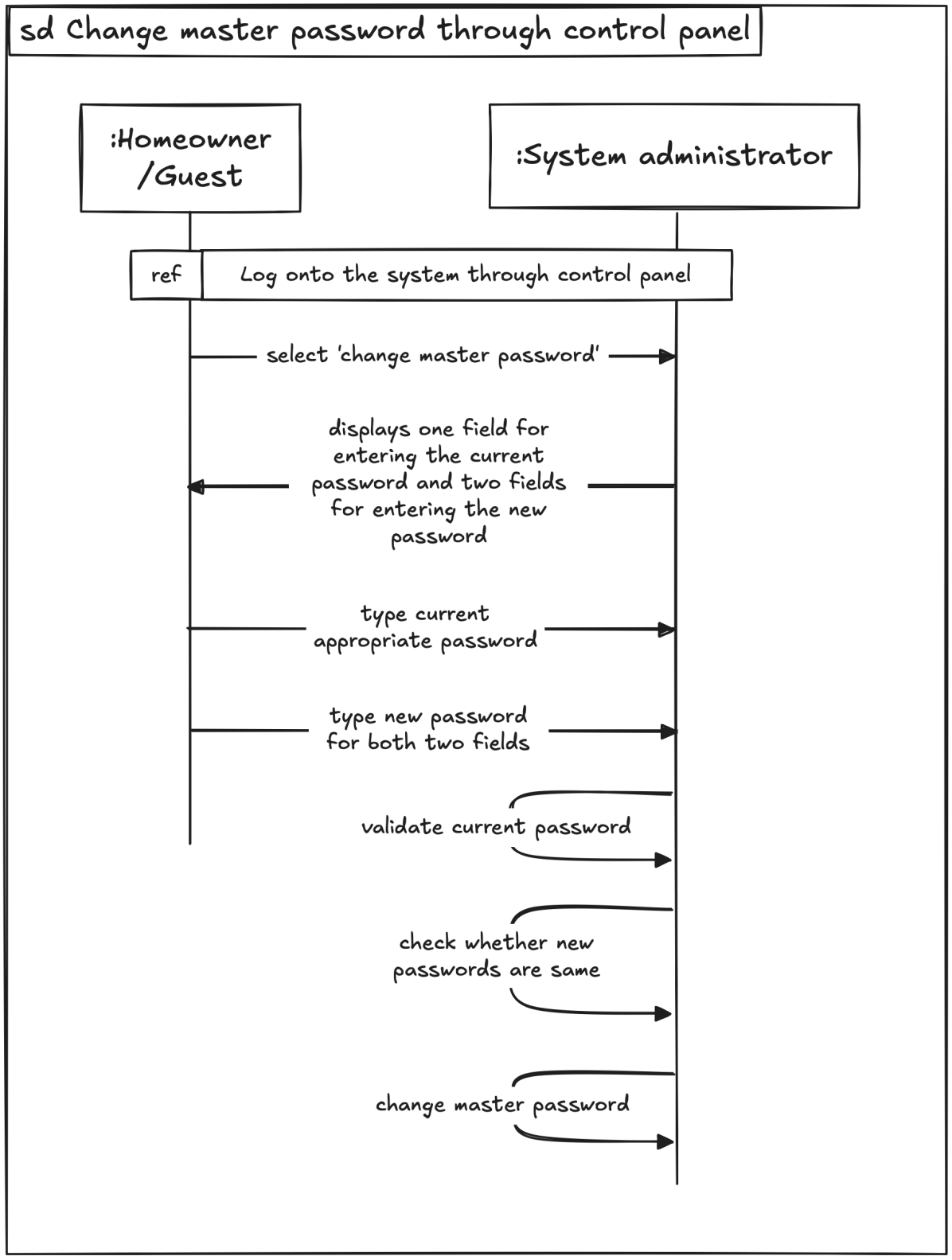
e. Turn the system off



f. Reset the system

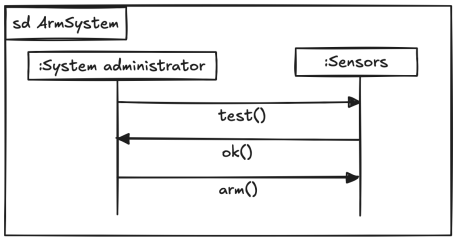


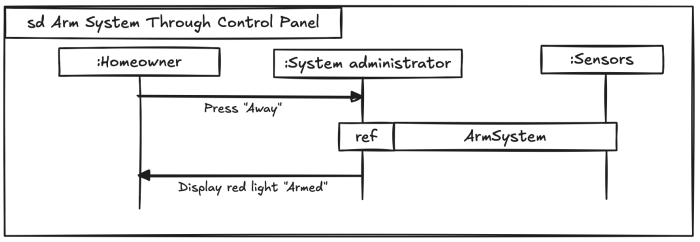
g. Change master password through control panel

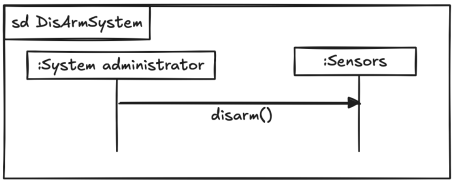


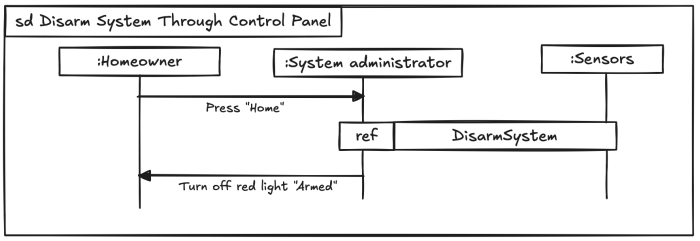
2. Security Sequence Diagram

a. Arm/disarm system through control panel

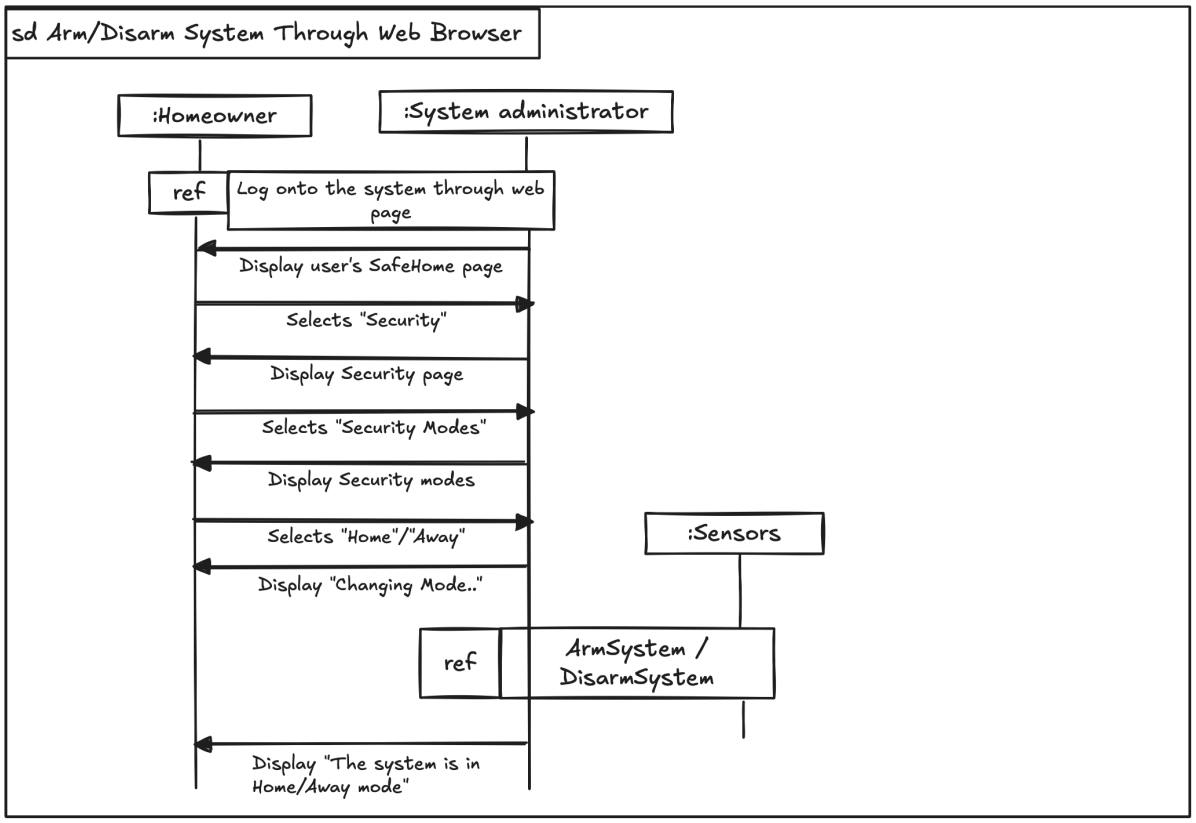




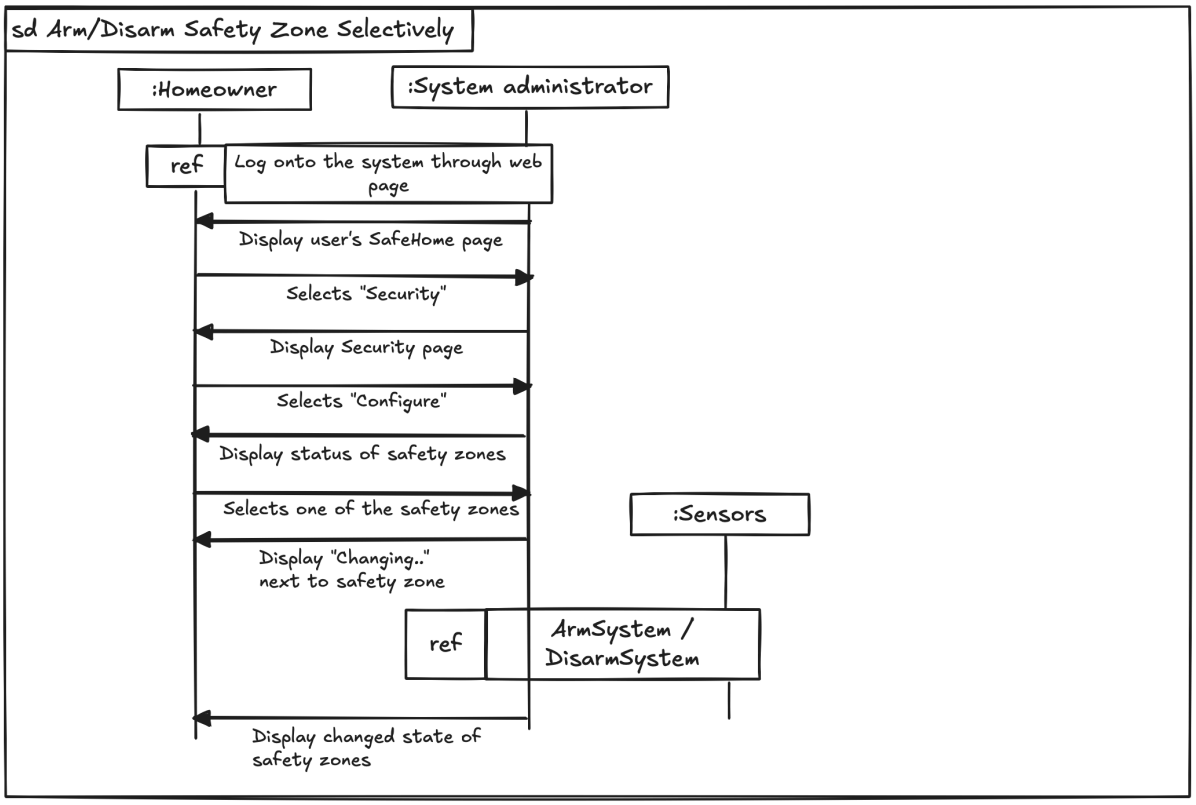




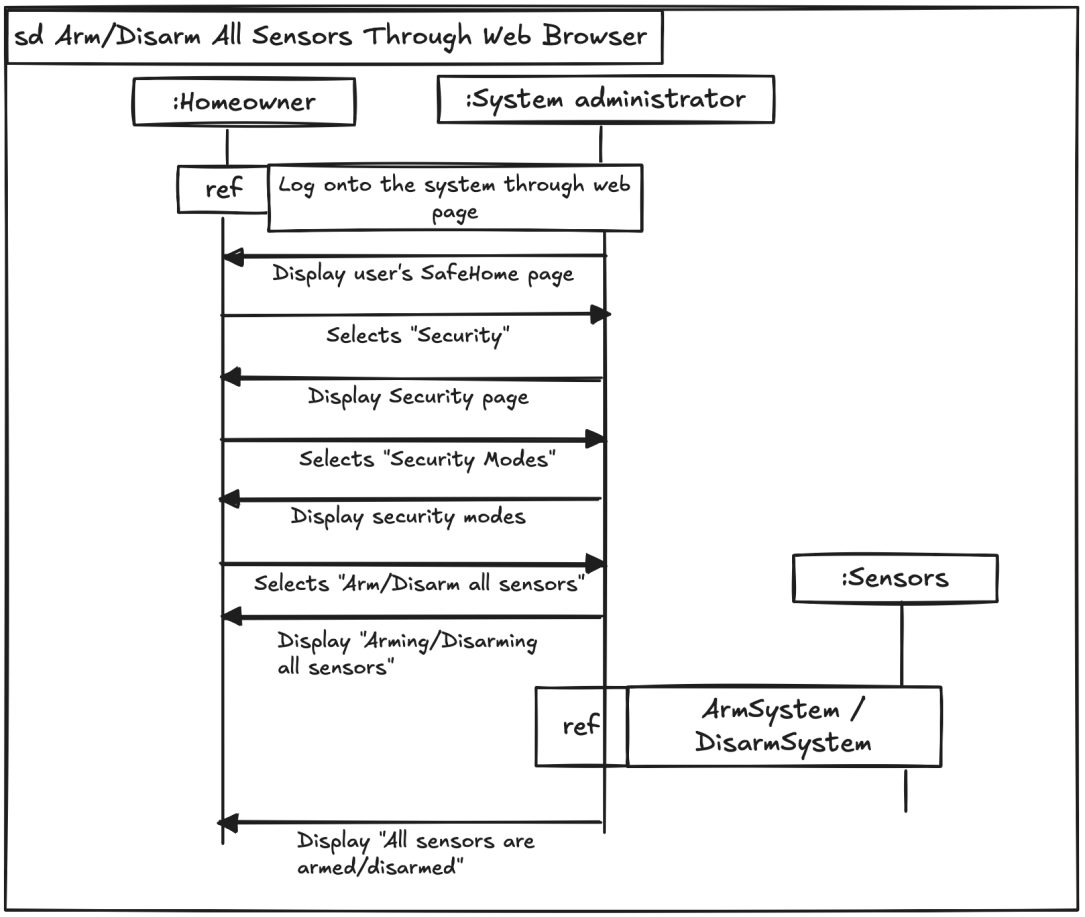
b. Arm/disarm system through web browser



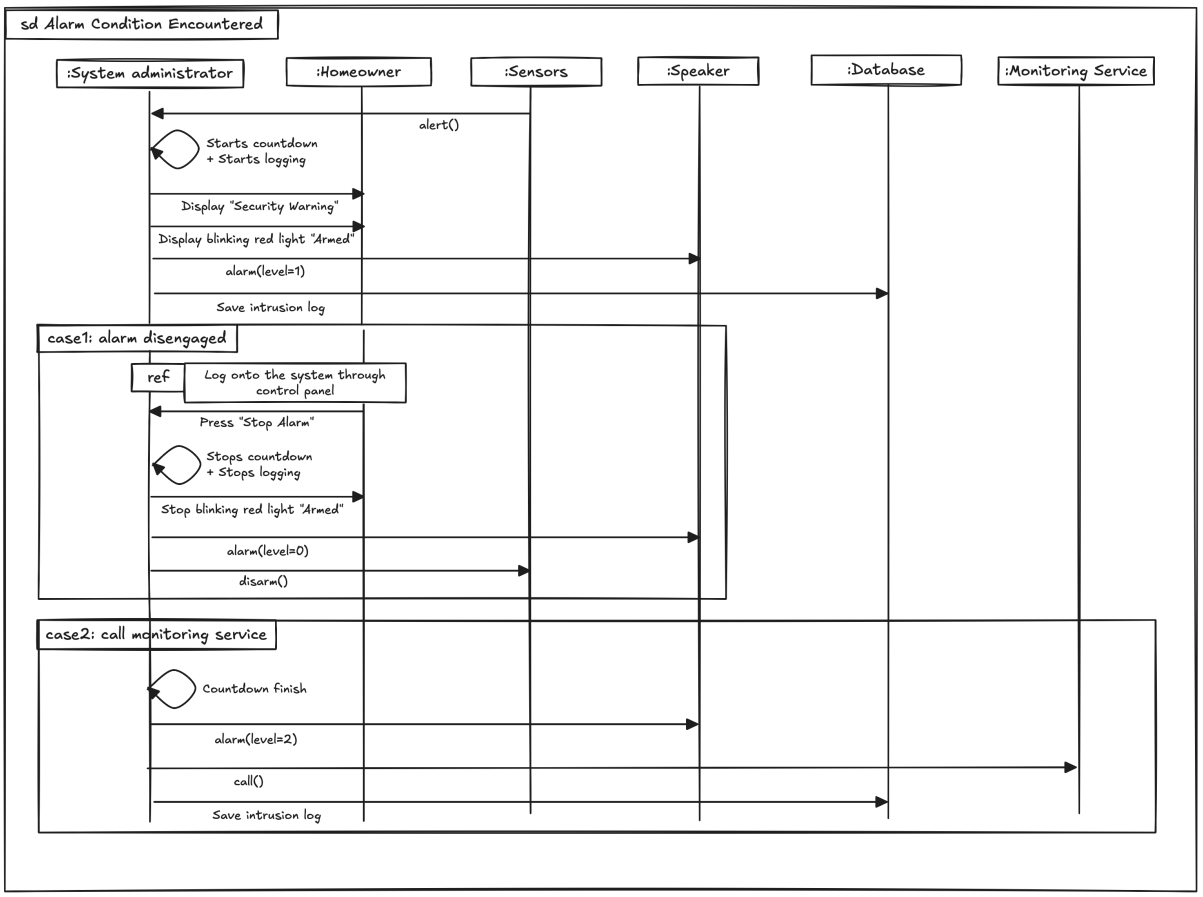
c. Arm/disarm safety zone selectively



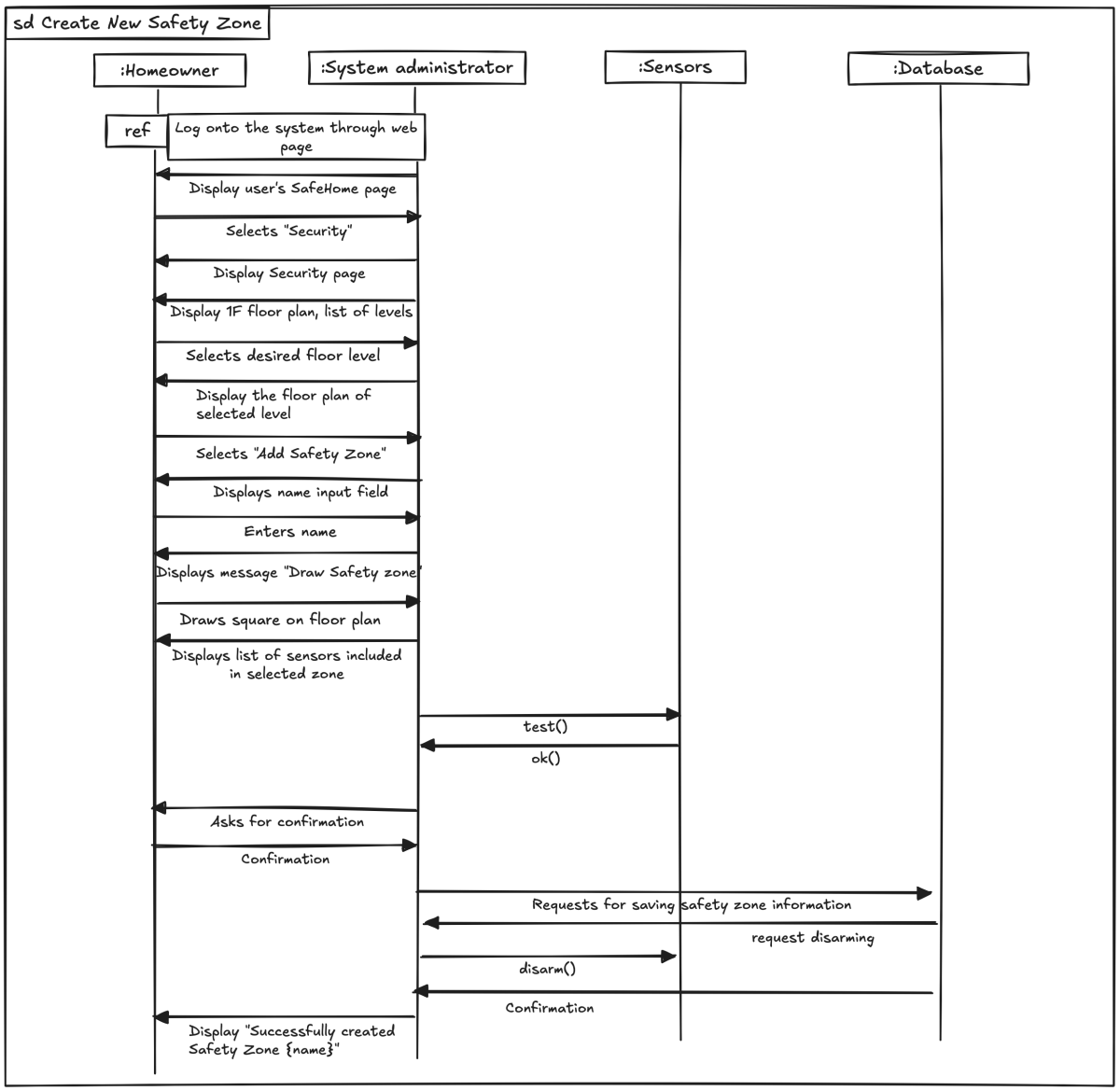
d. Arm/disarm all sensors through web browser



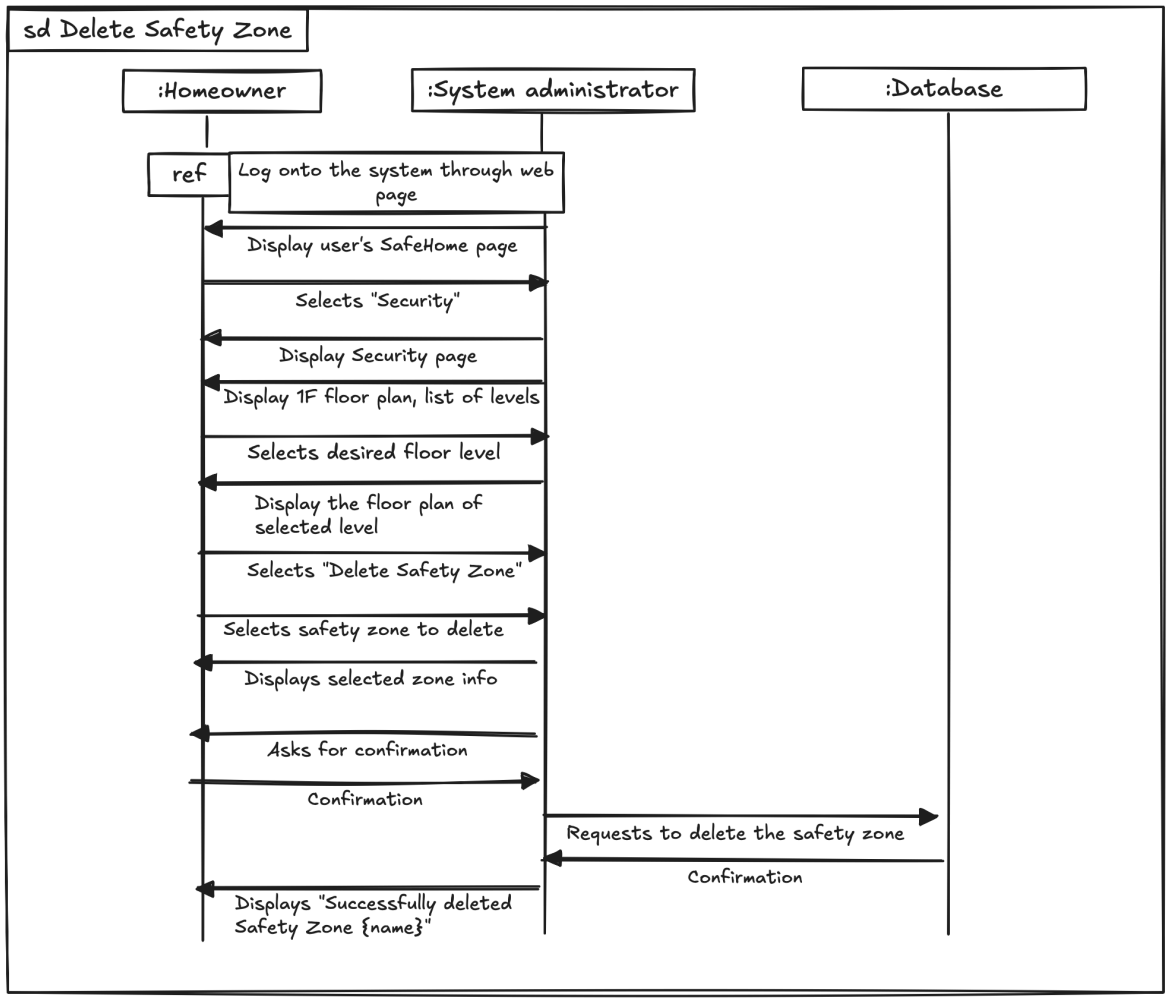
e. Alarm condition encounter



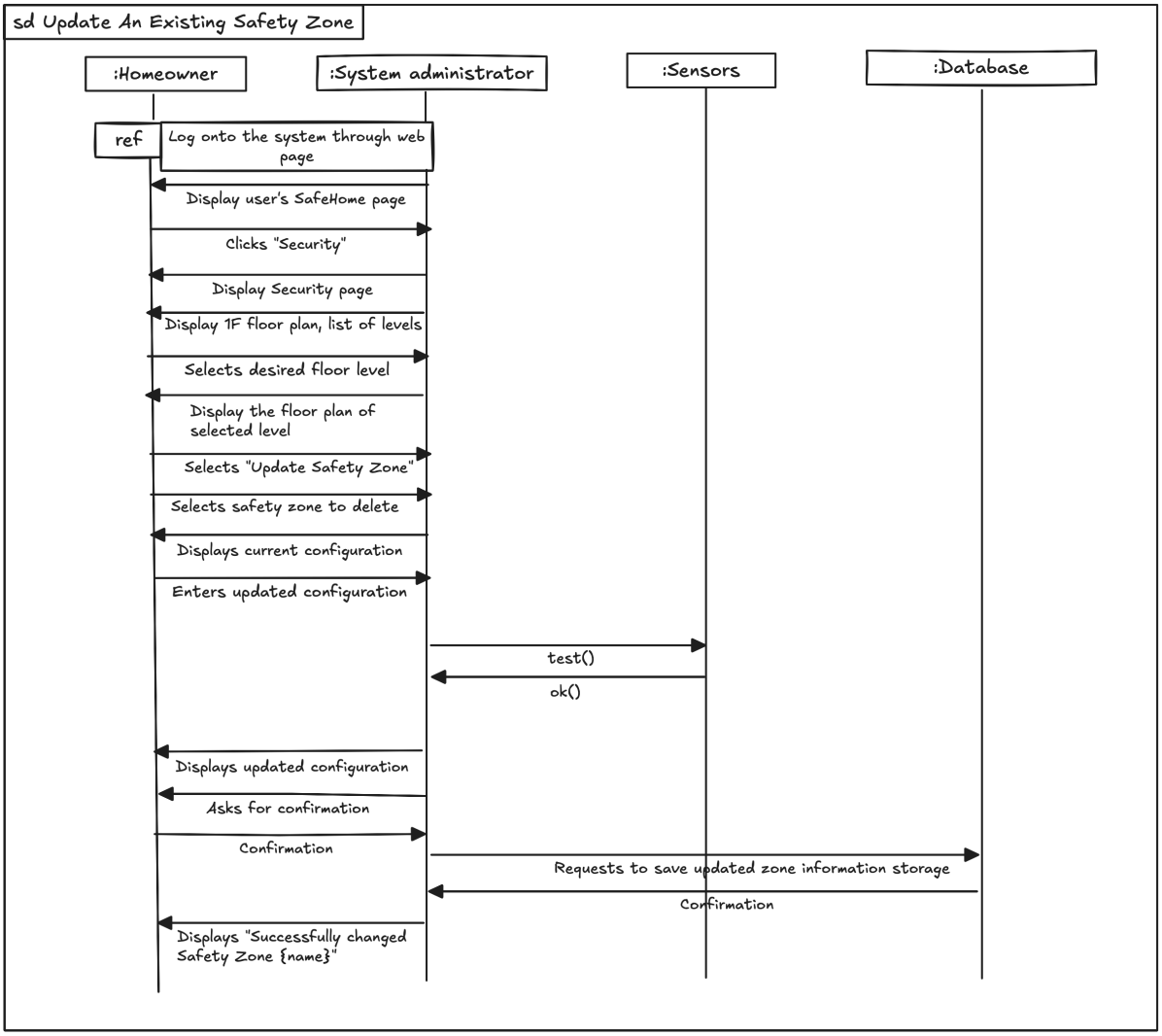
f. Create new safety zone



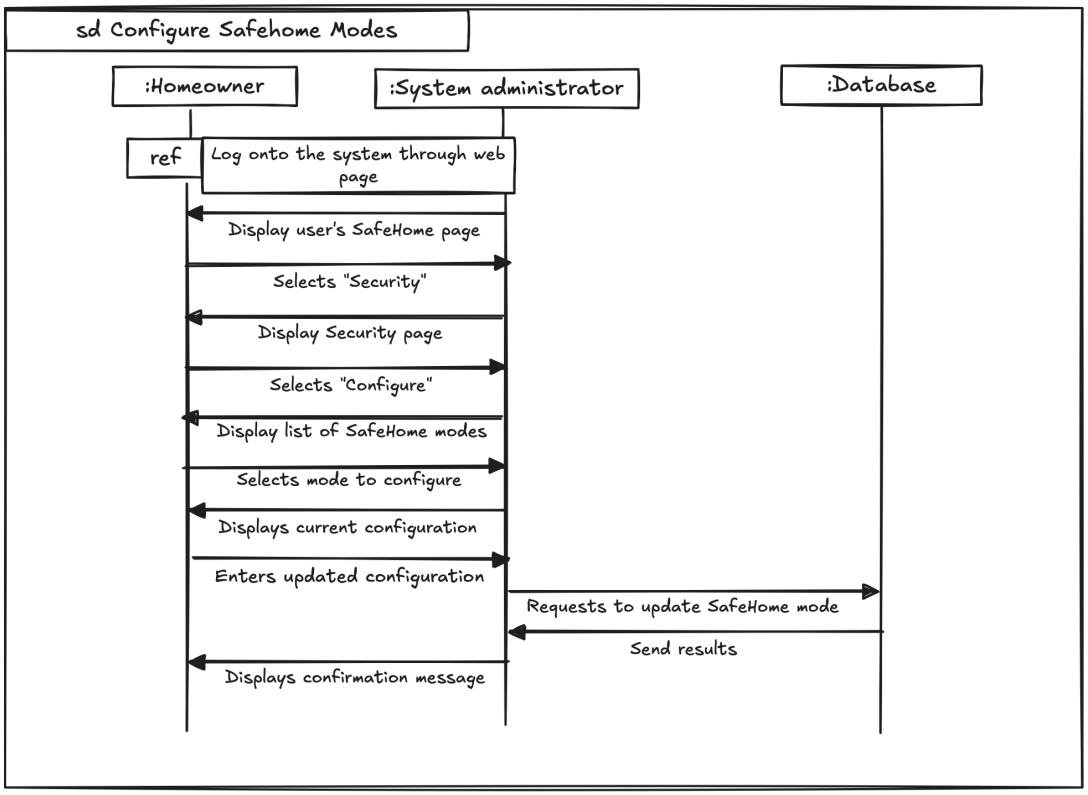
g. Delete safety zone



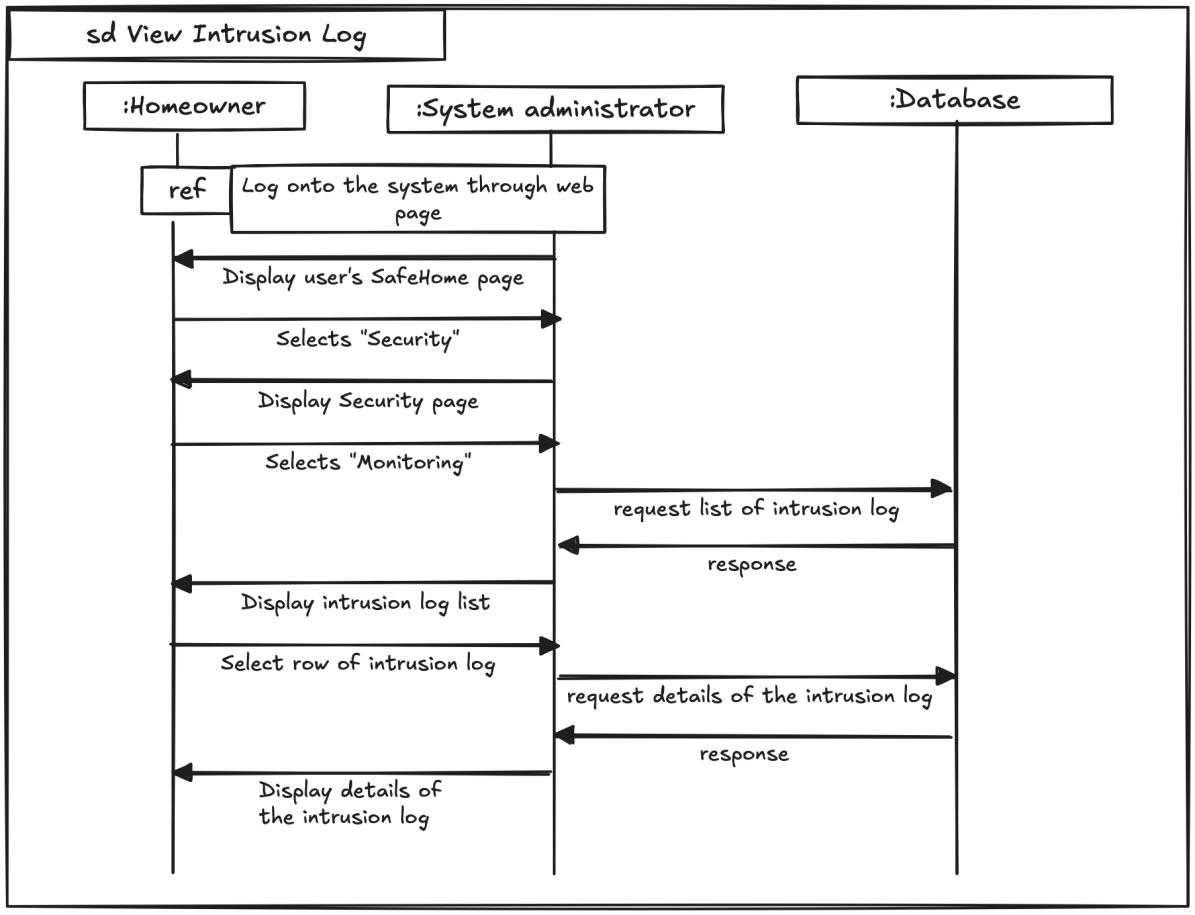
h. Update an existing safety zone



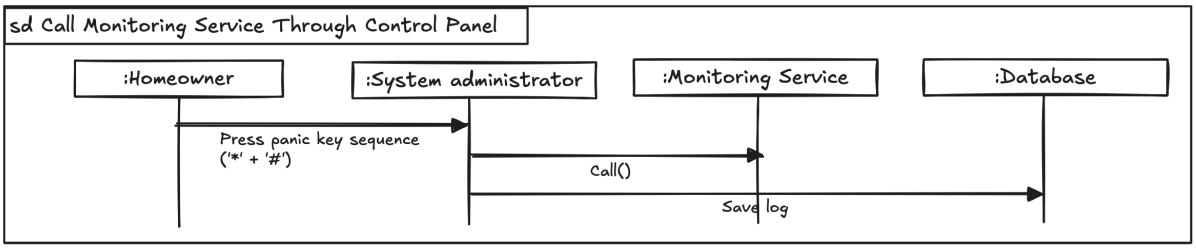
i. Configure Safehome modes



j. View intrusion log

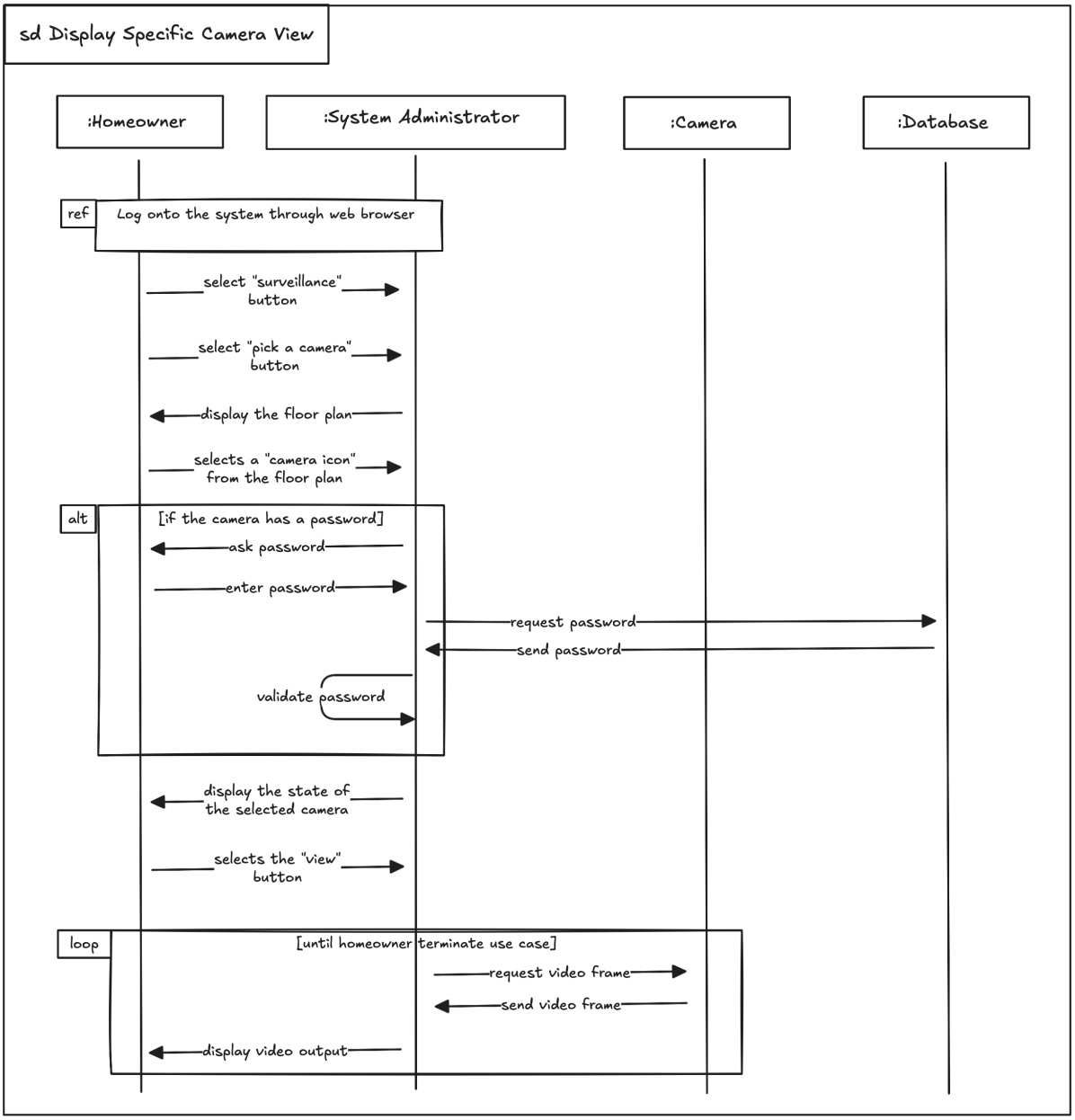


k. Call monitoring service through control panel

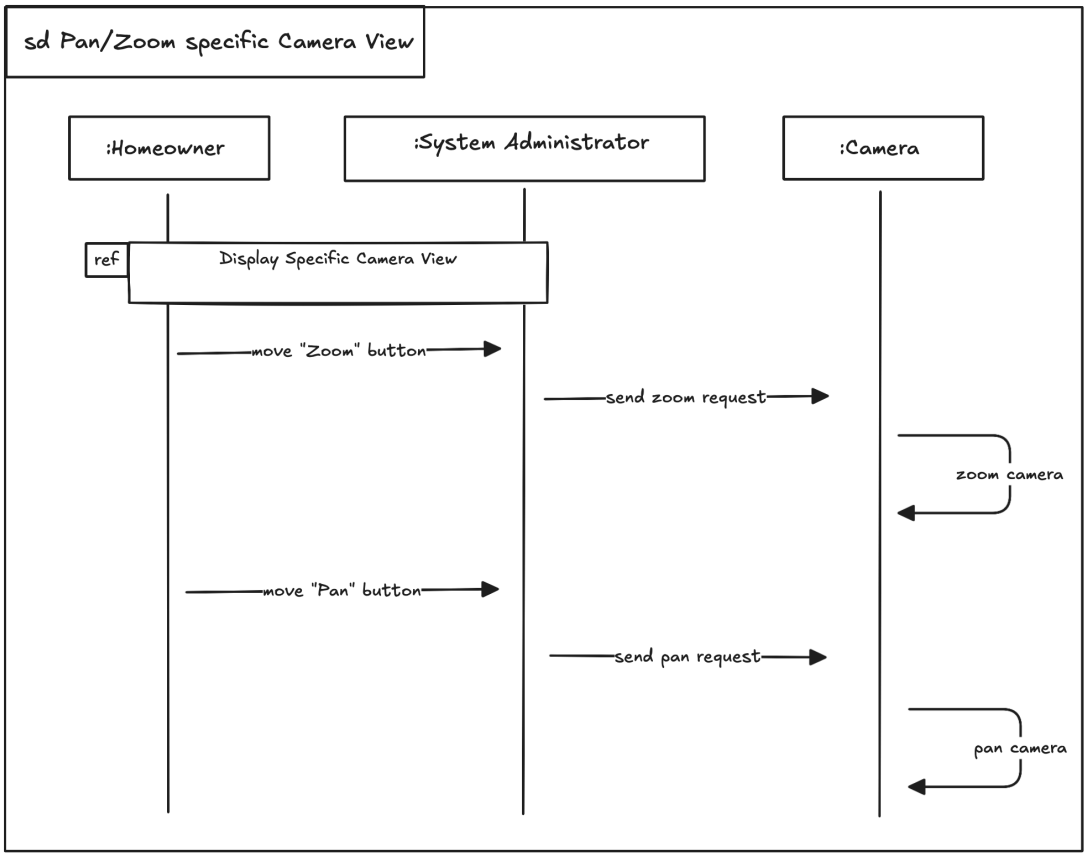


3. Surveillance Sequence Diagram

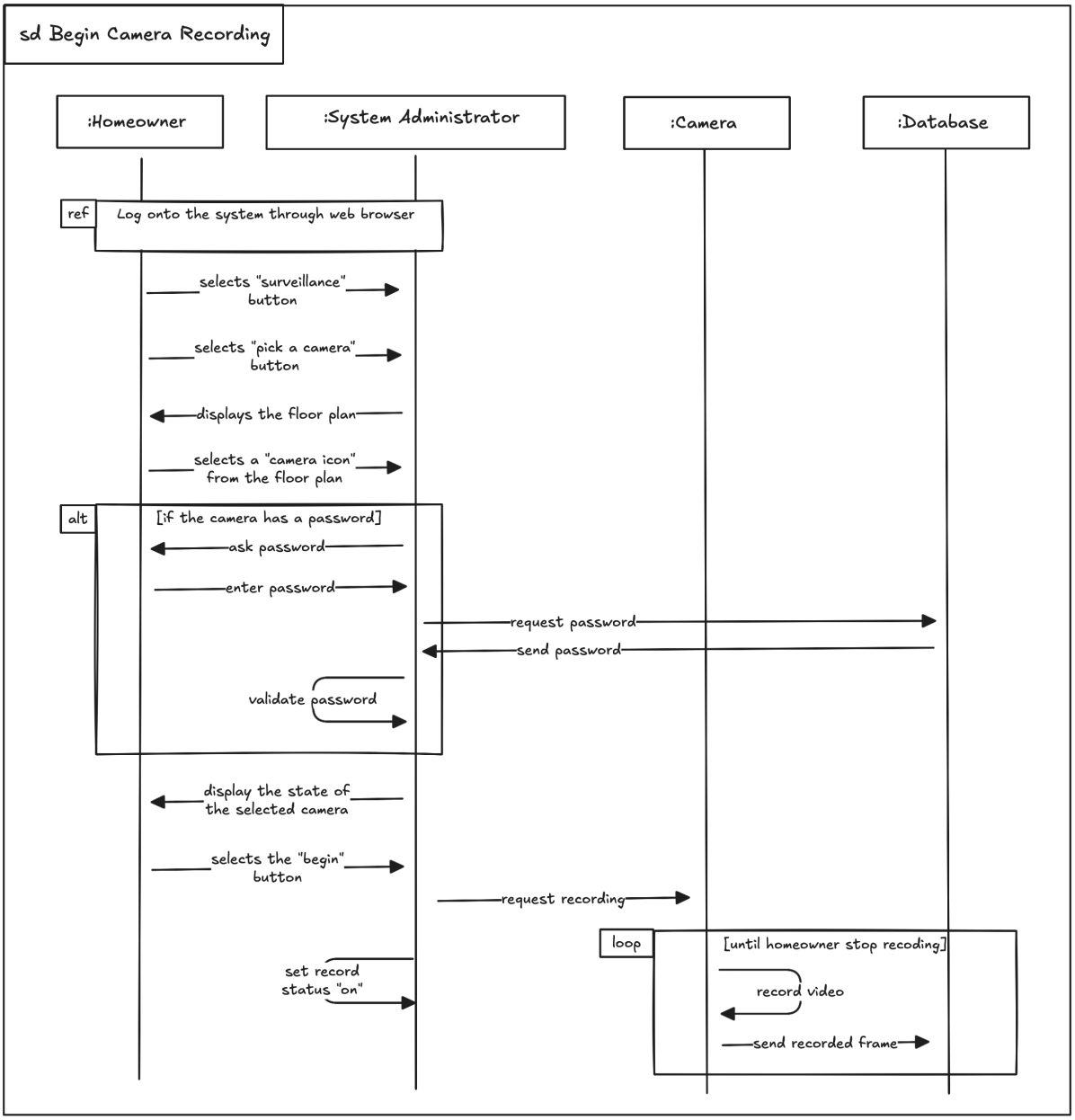
a. Display Specific camera view



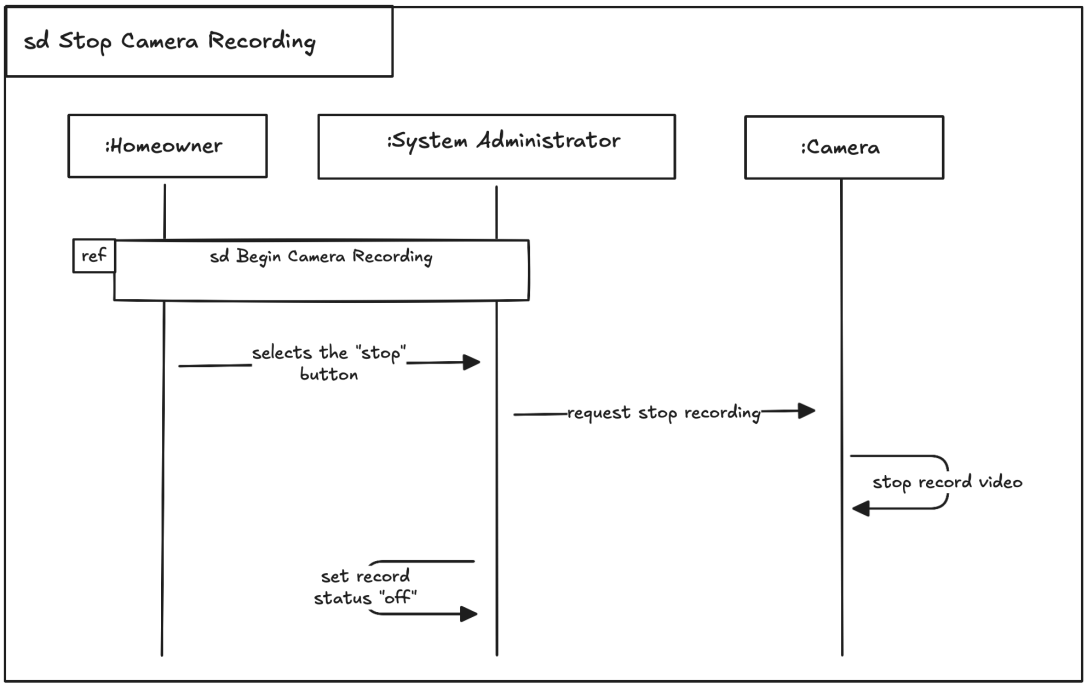
b. Pan/Zoom specific camera view



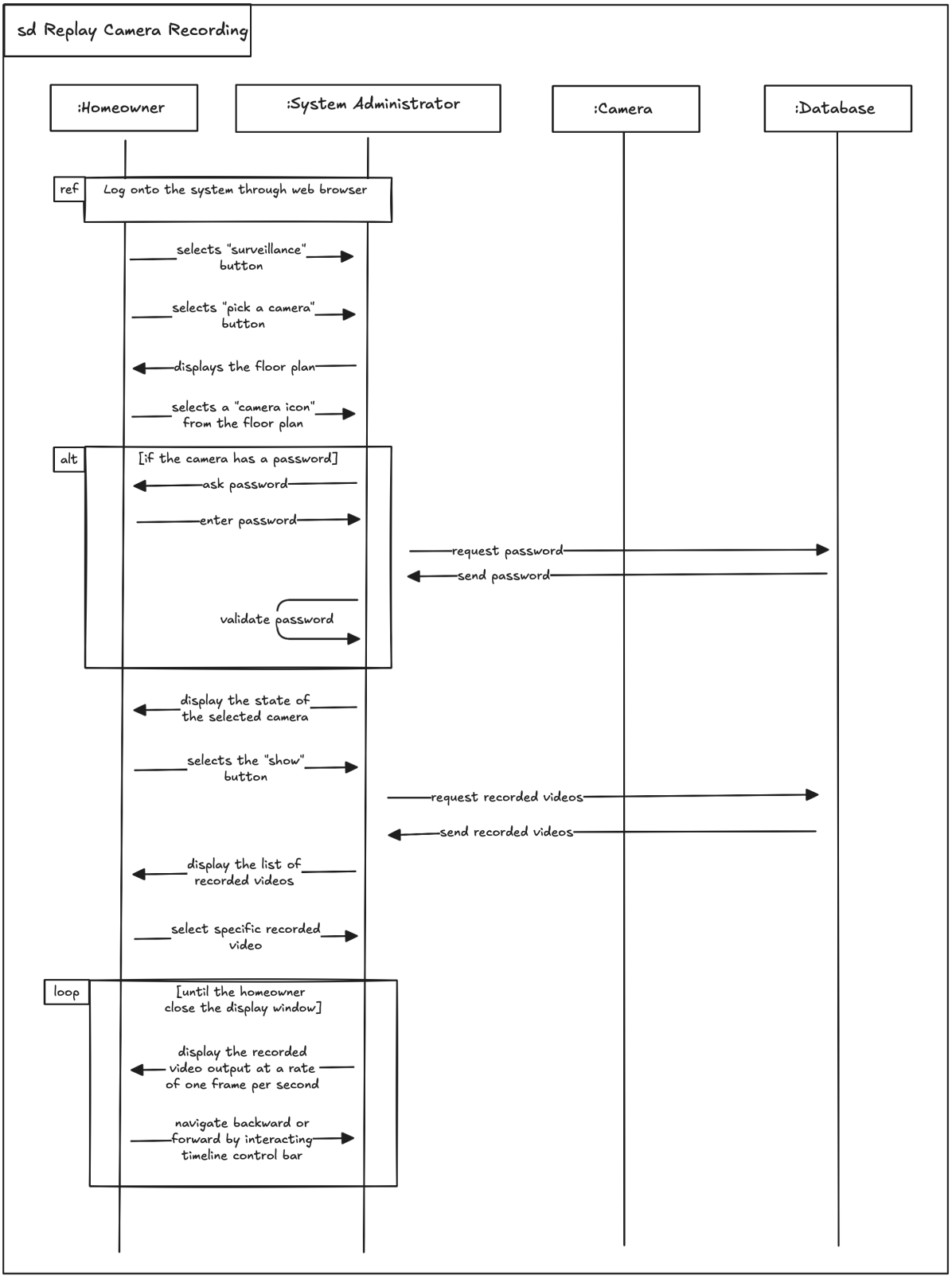
c. Begin camera recording



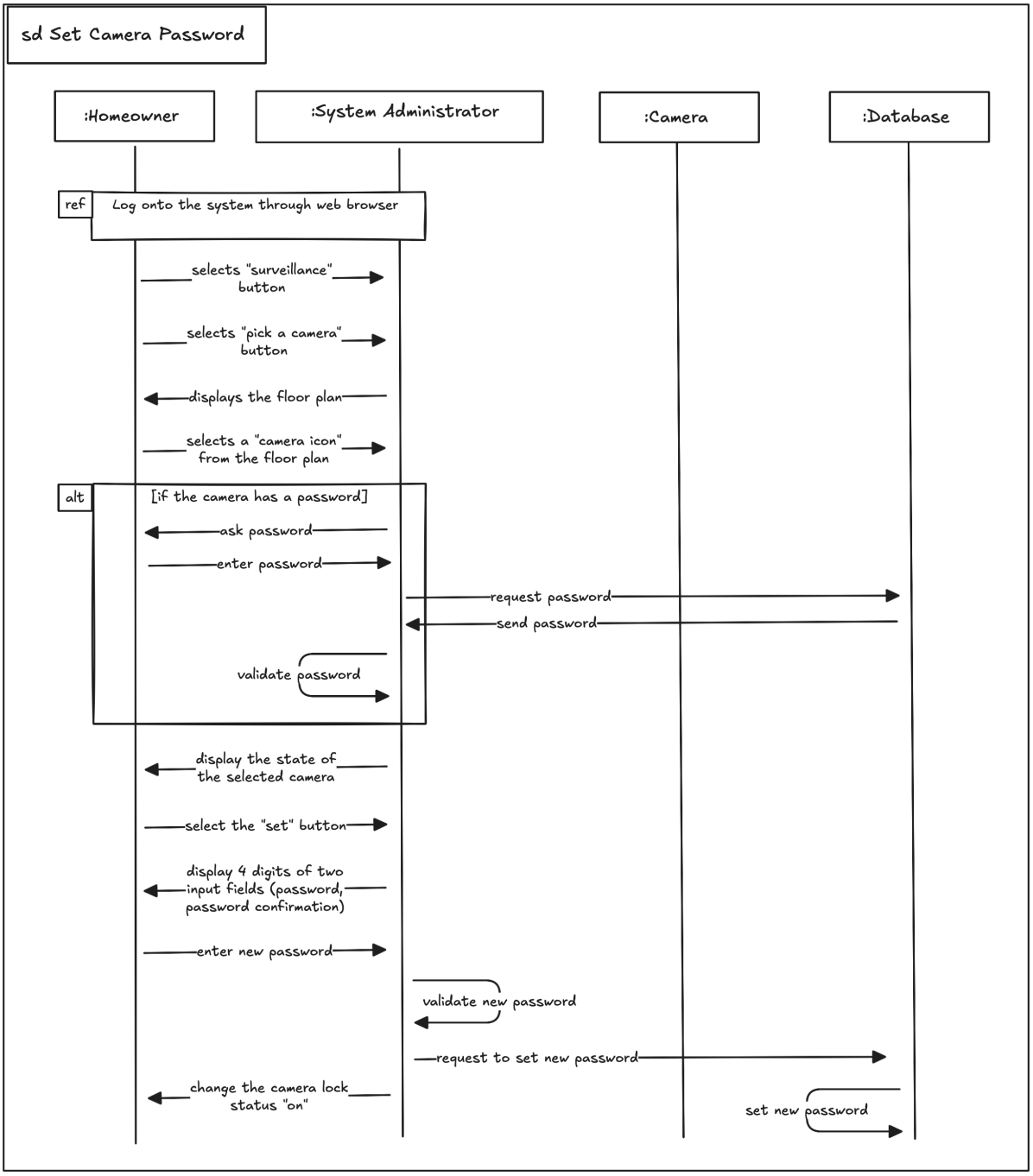
d. Stop camera recording



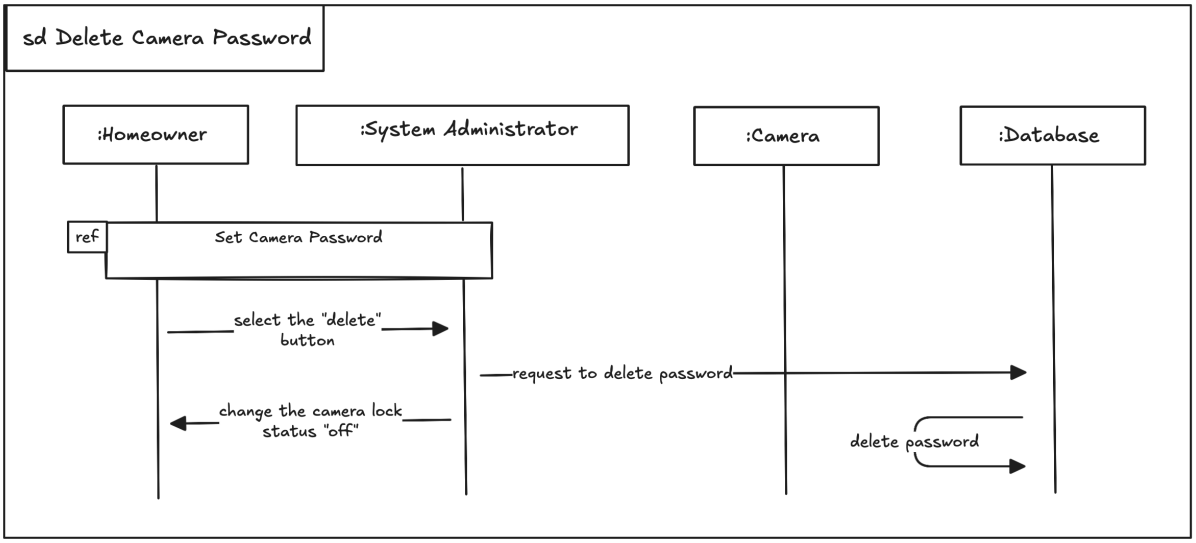
e. Replay camera recording



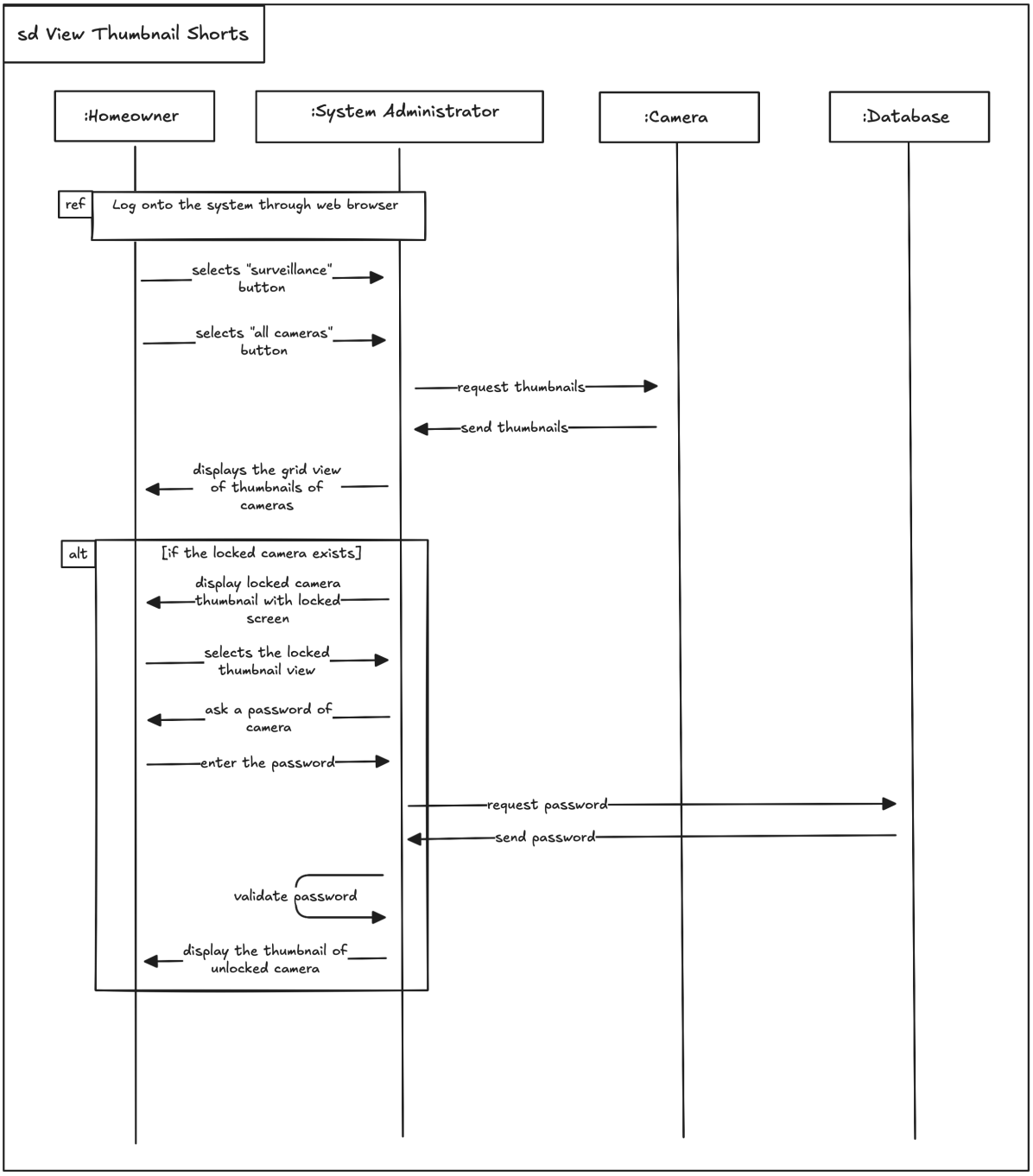
f. Set camera password



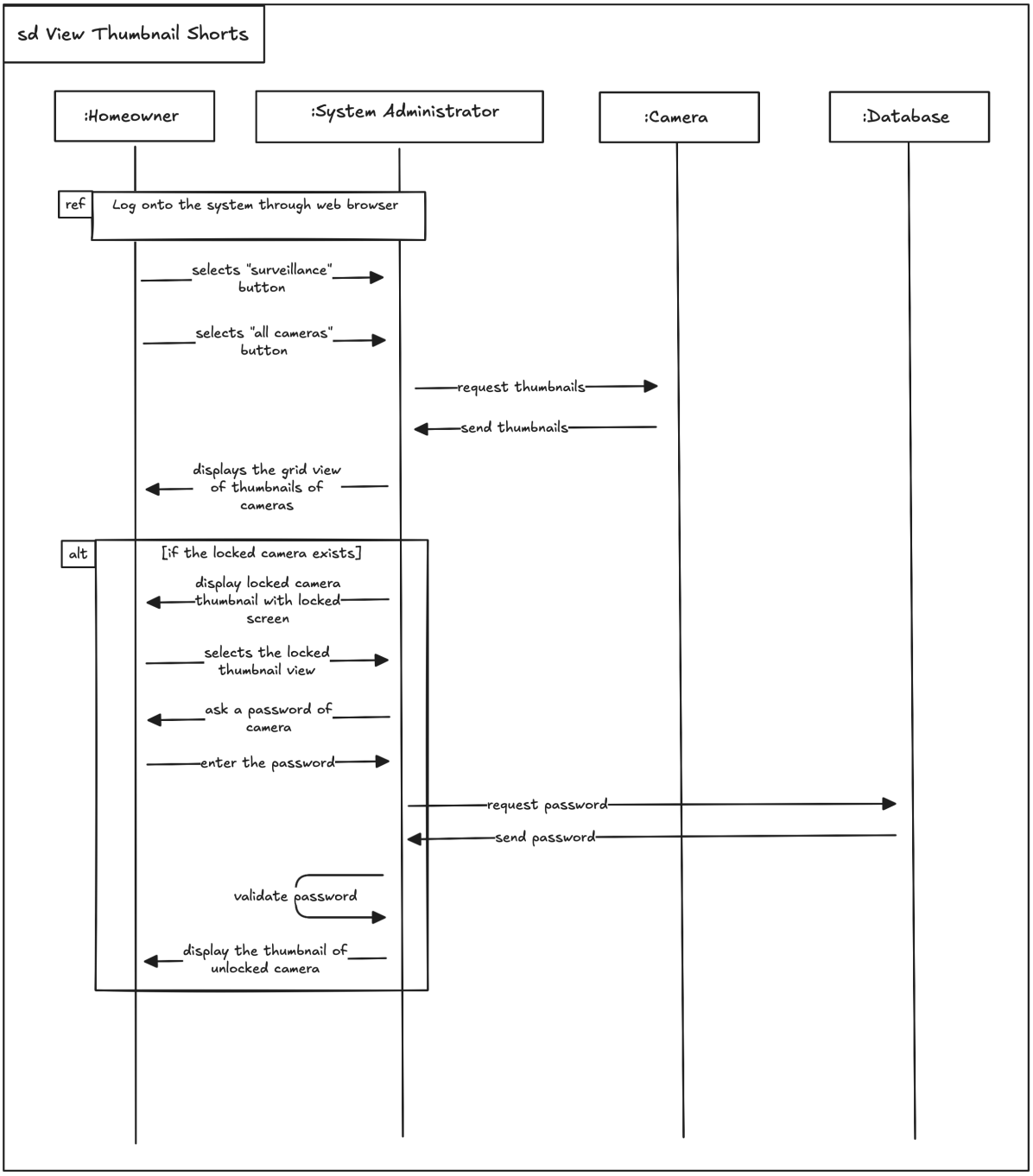
g. Delete camera password



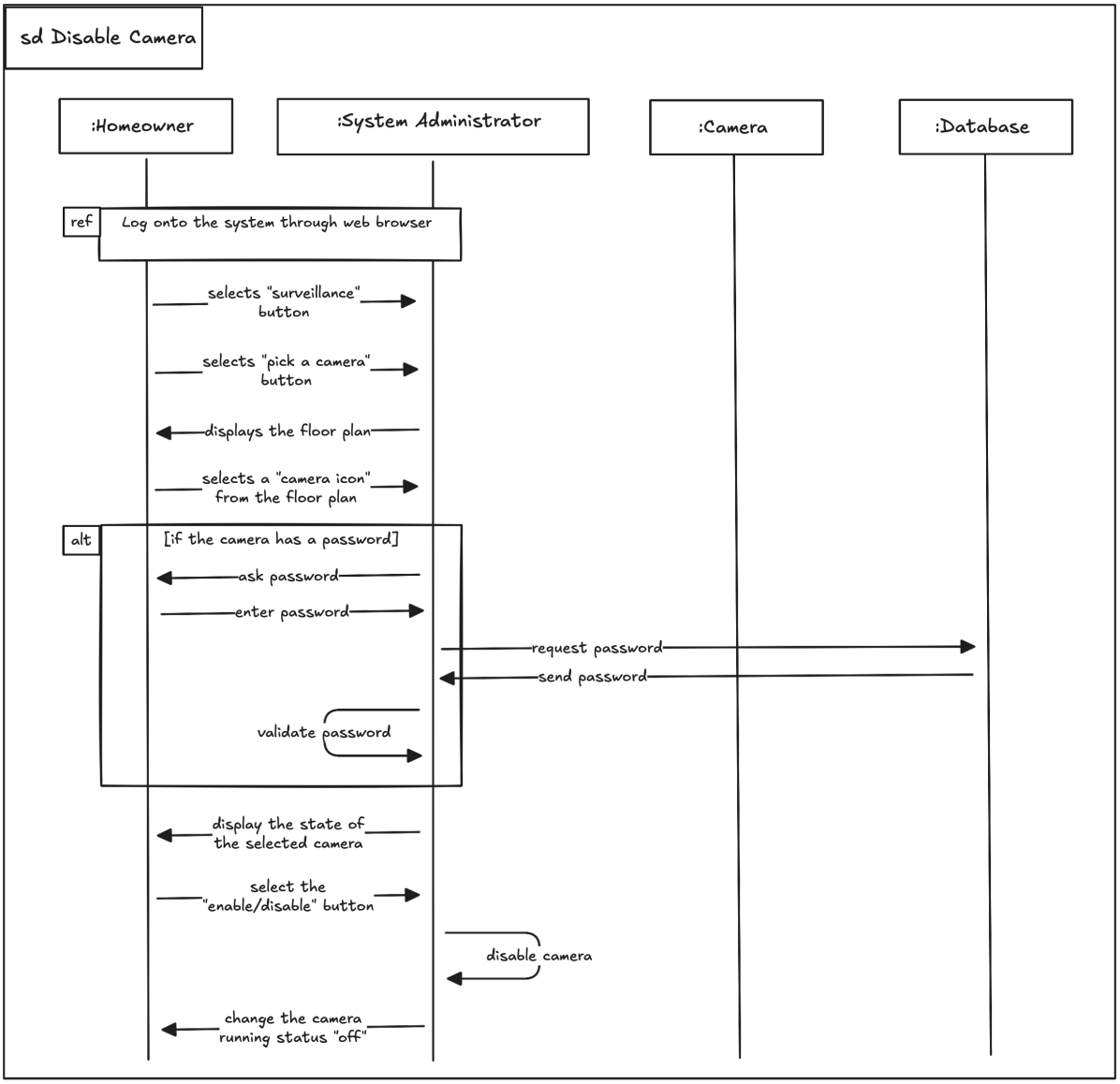
h. View thumbnail Shots



i. Enable camera



j. Disable camera



VIII. Who did what

Team member 최민준

1. Use case of common function
2. Use case diagram of common function
3. Sequence diagram of common function
4. Define terms

Team member 김민경

1. Use case of security function (f~k)
2. Use case diagram of security function (f~k)
3. Sequence diagram of security function (f~k)
4. Unifying format of SRS document

Team member 성대규

1. Use case of surveillance function.
2. Use case diagram of surveillance function.
3. Sequence diagram for surveillance function.
4. Integration & Refinement of Use case diagrams.
5. Integration & Refinement of Sequence diagrams.

Team member 조성호

1. Use case of security function (a~e)
2. Uses case diagram of security function (a~e)
3. Sequence diagram of security function (a~e)
4. Revised assumptions. Wrote related slide number and meeting number of the assumptions.

IX. Meeting logs

Description	Content
Meeting	SRS Meeting 1
When	2025-10-24 (금) 10:00–12:00
Location	학술문화관 그룹 스터디룸 3D
Participants	최민준, 김민경, 성대규, 조성호

Description	Content
Goal of meeting	To understand SafeHome product and write assumptions
What we discussed	1) Discussed about the contents of SafeHome dialog to understand SafeHome product. 2) Specified the boundary of our implementation 3) Discussed what is the alarm condition. 4) Read the provided assumptions, then added more assumptions on the boundary of this project.
Decision	We decided to write down use case scenario before the next meeting. 민준: Common use cases 성호, 민경: Security use cases 대규: Surveillence use cases

Description	Content
Meeting	SRS Meeting 2
When	2025-10-28 (화) 18:30–20:30
Location	학술문화관 그룹 스터디룸 3C
Participants	최민준, 김민경, 성대규, 조성호
Goal of meeting	Check current status of SRS specification and discuss details of requirement specification
What we discussed	1) Checked accuracy and unified details on use cases (common, security) 2) How to draw Sequence diagrams / Use case diagrams 3) Re-defined the alarm condition. 4) Added more assumptions including assumptions on concurrency as we review our use case scenarios. 5) Specified details of webpage interface / control panel buttons
Decision	Decided to draw use case diagram and sequence diagram with excaildraw. Decided to draw use case diagrams and sequence diagram before the next meeting

Description	Content
Meeting	SRS Meeting 3
When	2025-10-30 (목) 19:00–23:00
Location	학술문화관 그룸스터디룸 3D
Participants	최민준, 김민경, 성대규, 조성호

Description	Content
Goal of meeting	Review surveillence use cases and overall SRS document
What we discussed	1) Review surveilence use case scenario 2) Review use case 3) Simplify out-of-scope actors and exceptions 3) Standardize the format of diagrams and document
Decision	Until today midnight, make use case scenario format as same as use case diagram. Until tomorrow 9 p.m., complete the assigned tasks below. 민준: Glossary term definitions 대규: Use Case Diagram & Sequence Diagram standardization, remove “support technician” 성호: Assumption slide page, find meeting nouns 민경: Document standardization

Meeting Recording Transcription File in Korean : https://drive.google.com/drive/folders/1Nx5PRjSuJ0kEJYbBEzb_iLd_FGj7Au8x?usp=drive_link

Appendix A. Glossary

Term	Definition
Disarm state	A system state where all sensors are deactivated, and alarms trigger only for abnormal door or window openings. Intrusion logs continue to be recorded.
Disarm button	A button that changes all safety zones to the disarmed state when pressed.
Camera	A wireless surveillance device that allows the homeowner to view live video, record through the web interface.
Floor plan	A visual layout of the house showing the locations (coordinates) of sensors and cameras.
Alarm condition	A state triggered when one or more armed sensors detect a security hazard. The system issues an audible alarm, calls the monitoring service, and logs the event.
Error condition	Any unexpected or abnormal system state, such as ‘sensor malfunction’, ‘Surveillance function not configured for this system’ or ‘A floor plan is not available or has not been configured’.

Sensor	A hardware device that detects whether door or window is open, closed or open abnormally.
System administrator	The internal software entity that manages Safehome operations. It acts as a facilitator, not a human operator. ‘The system’ means system administrator.
Control panel	Communication media between user and system administrator. The central device installed near the house entrance. It allows login, system arming/disarming, alarm control, and displays system status.
Webpage	Communication media between user and system administrator. The remote web interface for accessing Safehome functions such as login, configuration, security, and surveillance.
Intrusion log	A record of intrusion or panic events detected by sensors. Accessible through the web interface.
Homeowner	The primary user of the Safehome system with full access privileges.
Guest	A user with limited privileges who can access only basic system functions.
System setting	Configurable parameters such as password, language, and alarm delay time that adjust system behavior to user preferences.
Default setting	The initial system configuration.
Power LED	The indicator light on the control panel showing power status: blinking green for startup, steady green for active, and red for powered off.
Armed LED	The indicator light on the control panel showing sensors’ status whether armed or disarmed. red light indicating armed or green light indicting disarmed
Sensor test	The automatic process to check the operational status of the sensor. Any malfunction is reported to the system administrator.
Password criteria	Control panel password: 4 numeric digits. Webpage password: at least 8 characters including letters.
Home state	The system mode indicating the homeowner is at home. Certain zones are disarmed, but perimeter sensors remain active.
Away state	The system mode indicating the homeowner is away. All sensors are armed to detect intrusion immediately.

Alarm levels	**Level 0**: Normal, peace state (no alarm). **Level 1**: Indoor alarm and countdown for monitoring service call. Sends notifications via the web browser **Level 2**: Loud external alarm (audible up to 30m) and web notification.
Recording status	Indicates whether a camera is currently recording ("on") or not ("off").