CS350 Safehome Project

Software Requirement Specification (SRS)

Project Team #8

Members:

20256450	**Jamal Alibalayev**
20256436	**Yonas Alexander Grossard Amin**
20256444	**Alan Pak To Cheung**
20256439	**Jongyoon Baek**

Korea Advanced Institute of Science and Technology

Table of Content

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.In future versions, SafeHome will be enhanced with advanced **account management** features, allowing homeowners to create and manage multiple user profiles with different access levels. Additionally, **camera recording and storage capabilities** will be integrated to enable continuous monitoring, playback, and evidence preservation, further strengthening the system's surveillance functions.

Safehome is thought to attract a 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 a Universal device by adding additional functionalities like management, subscription, etc.

2. Goal

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

Functional goal is to provide the followings:

1) Security functions
2) Surveillance functions

Non-functional goal is as follows:

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

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

1) *Completeness* - The Safehome system we develop has all the function specified in the function requirements below.
2) *Reliability* - The Safehome system we develops provide reliable services for all the 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) Security Management

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

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

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

2) Surveillance Management

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

II. Project Schedule

The project will follow the concept of the incremental software development model. In the first increment, the SafeHome system will focus on developing the core security, surveillance, and web access functions. Other features such as account management and camera scheduling will be added in later increments.

Plan for first increment

Beginning of the project	Oct 24, 2025
Initial requirement gathering	Oct 24 - Oct 31, 2025
Planning and creating analysis model	Nov 1 - Nov 7, 2025
Creating design model	Nov 7 - Nov 14, 2025
Construction & testing	Nov 14 - Dec 1, 2025
Testing & bug fixing	Dec 1 - Dec 8, 2025
First deployment	Dec 8 - Dec 20, 2025

ID	Name of Process	Begins	Ends	Working Period(days)
1	Initial Requirement Gathering	10/24/2025	10/31/2025	7
2	Planning and Creating Analysis Model	11/1/2025	11/7/2025	6
3	Creating Design Model	11/8/2025	11/14/2025	6
4	Construction and Testing	11/15/2025	12/1/2025	16
5	Testing of other team proejects	12/2/2025	12/8/2025	6
6	Final Submission of the project	12/9/2025	12/20/2025	11

III. Prototype GUI

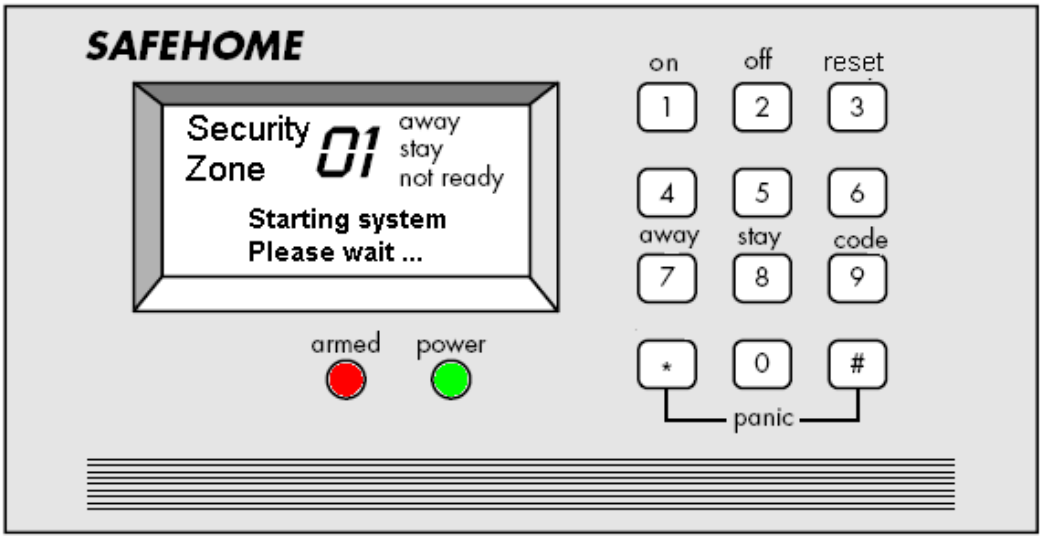

Fig 1. Control Panel

Fig 2. Login Screen

Fig 3. MainFunctions

Fig. 4 Security Function – Safety zone

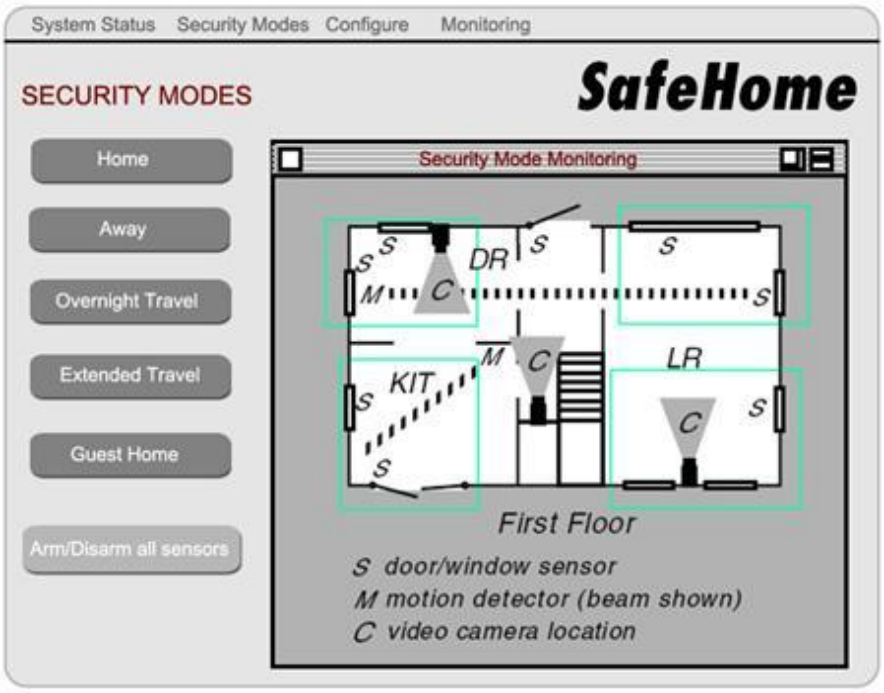

Fig. 5 Security Function – Security Mode

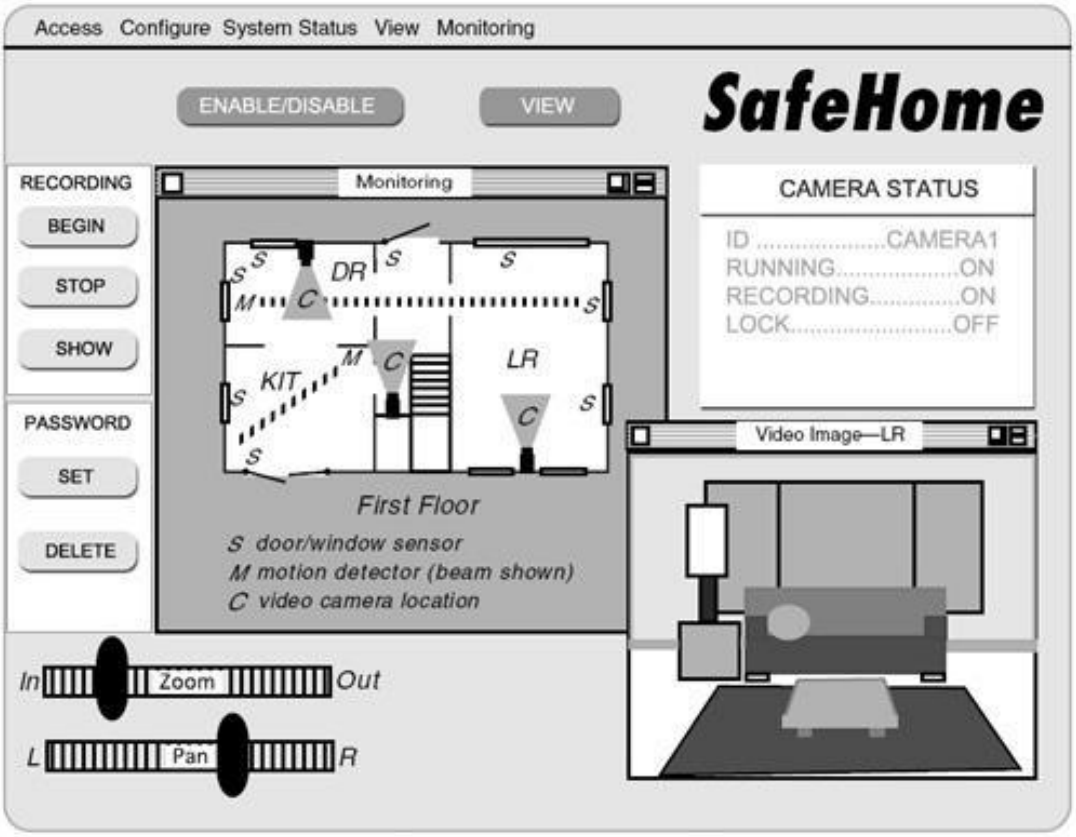

Fig. 6 Surveillance Function.

IV. Assumptions

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

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

3. “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.

4. We only control sensors through changing house safety situations or by arming/disarming safety zones.

5. Website’s name is “SafeHome Products Web Site”
6. The system's database is assumed to have sufficient capacity to store all camera recordings and log data generated under normal usage conditions.
7. All security sensors (doors, windows, motion detectors, and etc.) provide a binary output that reports one of two states: "secure" or "tripped."
8. It is assumed that a backup power system is in place to ensure that critical security functions (such as the main system and intrusion detection sensors) continue to operate even in the event of a power outage.
9. For security purposes, if a web browser user closes the page without logging out or there is no activity for 30 minutes, the session will automatically end (logout).
10. A stable internet connection is essential for all remote functions (access via a web browser). The system is designed to display appropriate error messages to the user if the internet connection fails.
11. Cameras connected to the system are assumed to support the "Pan/Zoom" and "Record" functions.
12. "Arm/Disarm" refers to setting the security status of the system or Safety Zone. "Enable/Disable" refers to setting the operation of individual devices, such as cameras.

13. All user interface names (e.g., button labels, page titles, and menu options) mentioned in the use case descriptions are **temporary identifiers used solely for descriptive clarity**. The final naming and layout of UI elements will be determined during the **system design phase** and are **not part of the functional requirements**.

14. **User Account Scope:**
    In the current increment, only *master* and *guest* user accounts are supported. Additional account types (e.g., custom user profiles for family members or other residents) and advanced permission management functionalities are **postponed to future development phases**.

V. Use Case Diagrams

1. Common Functions

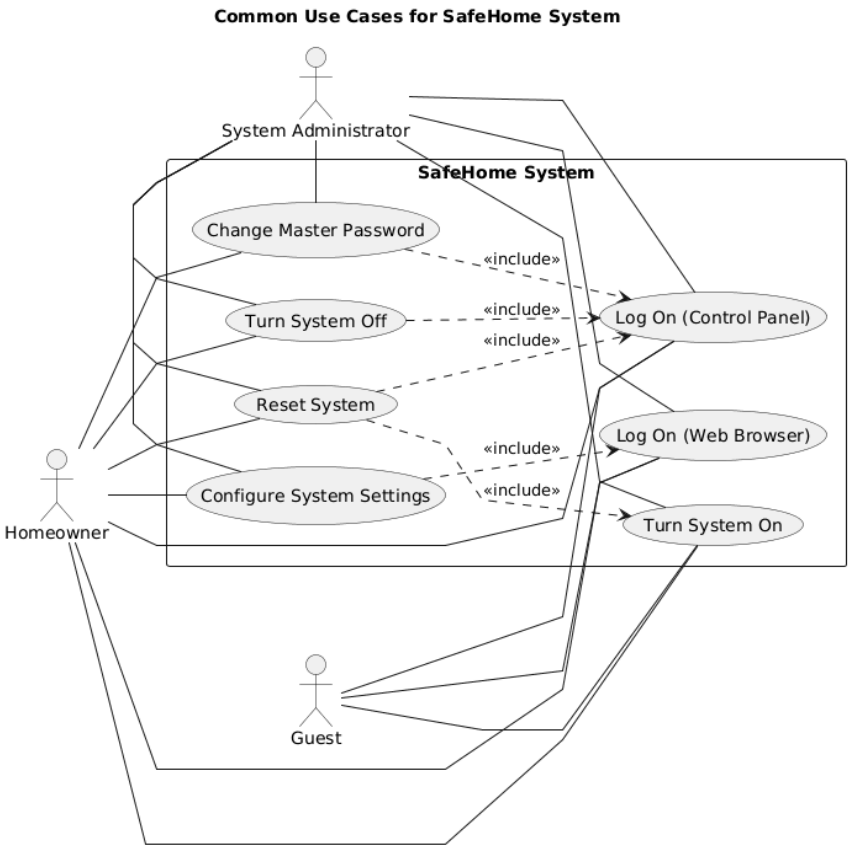

Figure 7. Common Functions Use Case Diagram

2. Security Functions

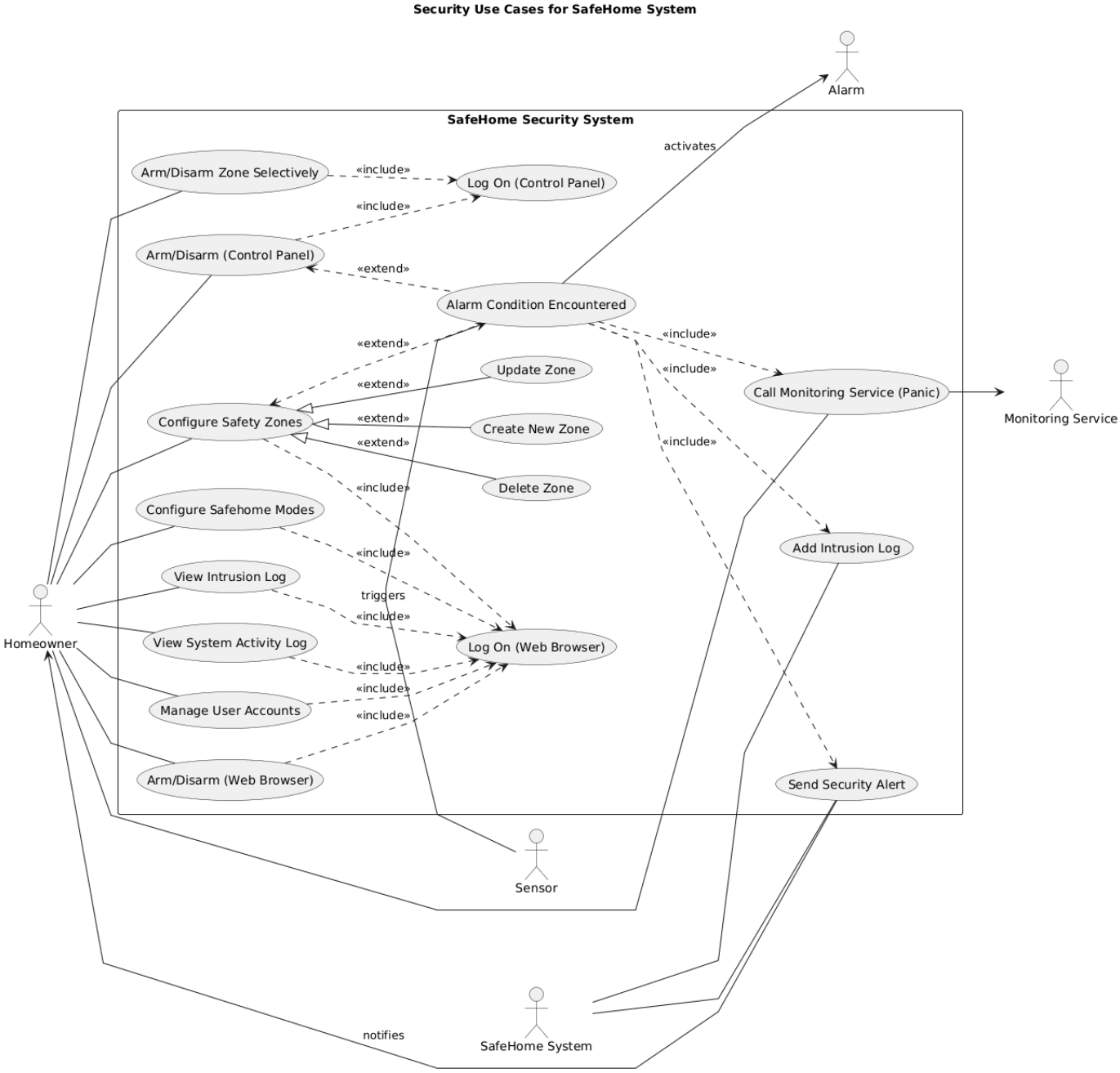

Figure 8. Security Functions Use Case Diagram

3. Configure Safety Zone Functions

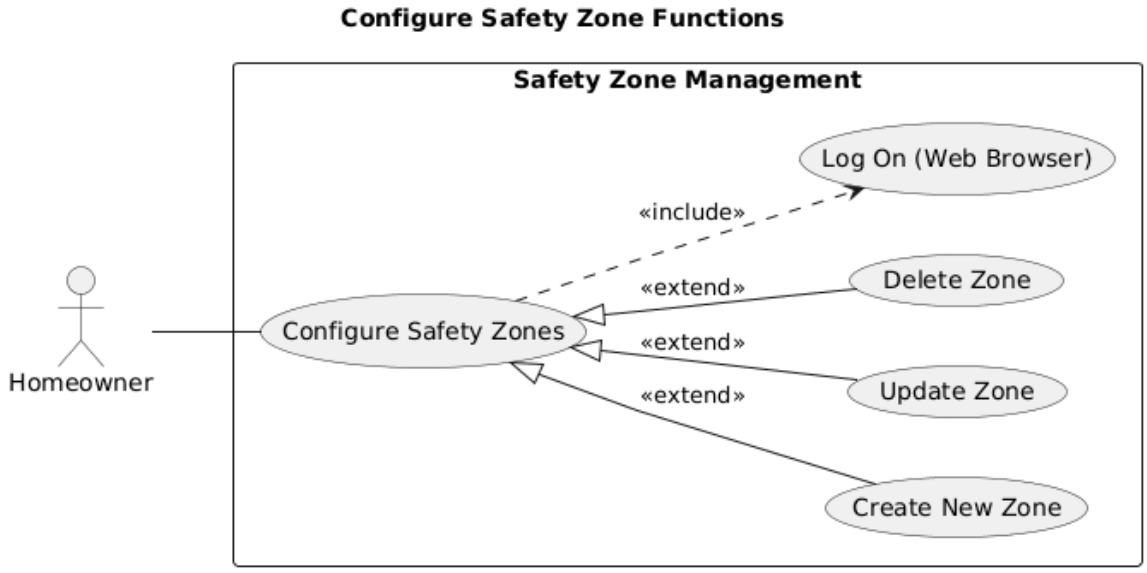

Figure 9. Security FunctionsConfigure Safety Zone Functions Use Case Diagram

4. Surveillance Functions

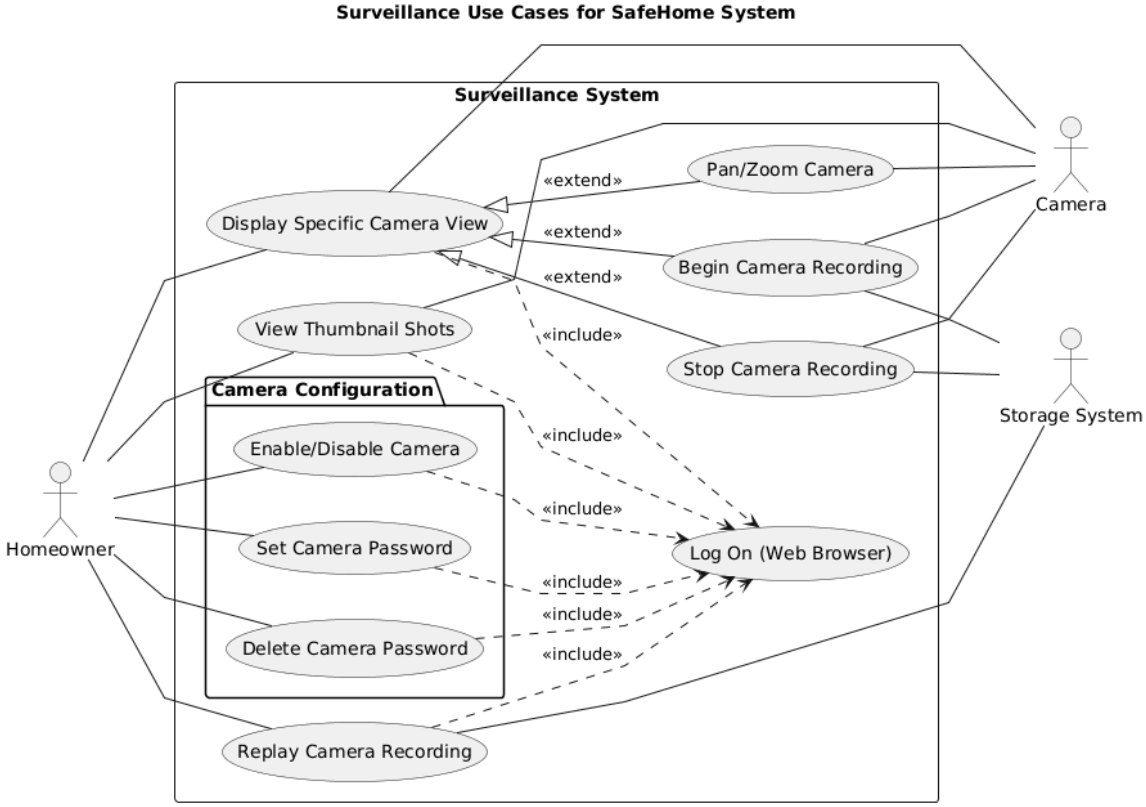

Figure 10. Surveillance Functions Use Case Diagram

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: The system has been configured. Appropriate password must be obtained.
Trigger: The homeowner/guest decides to log onto the system.
Scenario:

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

Exception:
3a. Password incorrect or not recognized.
.1: The system asks for password again.
.2: If the homeowner/guest enters incorrect or unrecognizable password three times in a row the system locks itself for predefined time.
4a. An alarm condition is encountered – see use case: “alarm condition encountered”
Priority: High priority, basic functions.
When available: First increment.
Frequency of use: Frequent.
Channel to actor: control panel
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?

References: page 18–20 in Safehome_dialog.pptx

b. Log onto the system through web browser

Use case: Log onto the system through web browser
Primary actor: Homeowner, Guest
Goal in context: To access the SafeHome system remotely through an Internet browser to perform available home control and monitoring functions.
Preconditions: The SafeHome system installed at the user’s home is fully configured, connected to the Internet, and online.
The SafeHome Web server is operational and accessible.

The homeowner or guest already possesses valid login credentials (user ID and password) that were created during initial registration or granted by the homeowner.

Trigger: The homeowner or guest decides to access the SafeHome system remotely through a web browser on their PC or Laptop.

Scenario:

1. The user opens an Internet browser on their PC and navigates to the **SafeHome Products Web site** (the official remote access portal).
2. The SafeHome website loads and displays the secure login page.
3. The user enters their **user ID** and **two authentication passwords** (a two-level login for security).
4. The system sends these credentials to the SafeHome server for verification.
5. The SafeHome server validates the credentials against its user database.
6. If the credentials are valid, the system connects the user to their specific home installation and displays the **main SafeHome dashboard** (with modules such as *Security*, *Surveillance*, *Configuration*, and *Monitoring*).
7. The user can now access authorized functions according to their role (homeowner or guest).

Exception:

3a. User ID is not recognized.
.1:The system asks for user ID again
3b. Password incorrect or not recognized.
.1: The system asks for password again.
.2: If the homeowner/guest enters incorrect or unrecognizable password three times in a row the system locks itself for predefined time.
4a. An alarm condition is encountered – see use case: “alarm condition encountered”

Priority: High priority, basic functions.
When available: First increment.
Frequency of use: Frequent.
Channel to actor: SafeHome Products Web site
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?

References: page 19–21 in Safehome_dialog.pptx

c. Configure system setting

Use case: Configure system setting

Primary actor: Homeowner

Goal in context: To modify basic operational parameters of the SafeHome system — including delay times, master and guest passwords, and alert contact numbers — through a secure web browser interface.

Preconditions: The **SafeHome system installed at the user's home** is configured, connected to the Internet, and online. The **SafeHome web server** is operational and can communicate with the home system. The **homeowner has valid login credentials** (user ID and password).

Trigger: The homeowner decides to modify SafeHome settings remotely through the web browser.

Include: 1 Common Use Cases : b. Log onto the system through web browser.

Scenario:

1. The homeowner opens a web browser and navigates to the **SafeHome Products Web site**.
2. The homeowner performs the **login procedure** as described in *"Log onto the system through web browser."*
3. After successful authentication, the SafeHome main dashboard appears.
4. The homeowner selects **"Configuration"** from the main function menu.
5. The system displays a list of configurable parameters:
   - Entry/exit delay times
   - Master password
   - Guest password
   - Contact phone numbers for alerts
   - Sensor naming and grouping options
6. The homeowner selects the parameter(s) to modify.
7. The system displays editable fields for the chosen parameter(s).
8. The homeowner enters the new values and confirms the changes.
9. The system validates all inputs and applies them to the home installation through the SafeHome control subsystem.
10. The system confirms that settings were successfully updated and logs the changes for audit purposes.

Exception:
4a. If the homeowner tries to access configuration without being logged in:
→ The system redirects to the login page (see *included use case*).

8a. If invalid data are entered (e.g., invalid phone number format, too short password):
→ The system displays an error message and requests correction.

9a. If communication with the home system fails (e.g., Internet or device error):
→ The system displays "Unable to update configuration at this time" and retains previous settings".

Priority:	High — necessary for initial setup and ongoing system management.
When available:	Second increment
Frequency of use:	Occasional (mainly during setup or maintenance).
Channel to actor:	SafeHome Products Web site
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?

References: page 24–25 in Safehome_dialog.pptx

d. Turn the system on

Use case:	Turn the system on
Primary actor:	Homeowner, Guest
Goal in context:	To activate the SafeHome system using the **physical control panel** installed at the home, making the security and monitoring subsystems ready for operation.
Preconditions:	The SafeHome control panel is powered and connected to the home system. The system hardware and sensors are properly installed and functional. The homeowner is physically present and has access to the control panel.
Trigger:	The homeowner/guest decides to log onto the system.

Scenario:
1. The homeowner approaches the control panel.
2. The control panel display red on the **"Power"** button
3. The homeowner presses the **"Power"** button.
4. The control panel sends the activation signal to the SafeHome system administrator.
5. The system begins initialization — power to sensors, cameras, and communication modules is activated.
6. The control panel shows a short **"Starting System…"** message while components are initializing.
7. The control panel receives confirmation from the system administrator

that initialization is complete.

8. The color of the "Power" button changes to the green

Exception:

3a. If the system power supply is interrupted, the control panel displays **"Unable to activate – power failure."**

5a. If one or more sensors or devices fail to respond during startup, the control panel displays **"Partial activation – check devices."**

7a. If initialization fails entirely, the system remains off and displays **"Startup failed – please contact support."**

Priority: High priority, basic functions.
When available: First increment.
Frequency of use: Frequent.
Channel to actor: control panel
Secondary actors: System administrator
Channel to secondary actors: Direct wired or wireless connection between control panel and SafeHome system administrator.

References: page 22–23 in Safehome_dialog.pptx

e. Turn the system off

Use case: Turn the system off
Primary actor: Homeowner
Goal in context: To deactivate (power down) the SafeHome system through the **physical control panel** installed in the home, stopping all active monitoring and sensor operations safely.
Preconditions: The SafeHome system is currently turned on and running.
The control panel is operational and connected to the system administrator.
The homeowner is physically present and has access to the control panel.

Trigger: The homeowner decides to turn off the SafeHome system.
Include: 1 Common Use Cases : a. Log onto the system through control panel.

Scenario:

1. The homeowner approaches the SafeHome control panel.
2. The homeowner performs the **login procedure** as described in *"Log onto the system through control panel."*
3. The control panel display shows **"System On – Ready."**
4. The homeowner presses the **"Turn Off"** or **"Deactivate System"** button.
5. The control panel sends a deactivation signal to the system administrator.
6. The system administrator sequentially powers down sensors, cameras, and other active subsystems.
7. The control panel shows a brief message such as **"Shutting down**

system…" while deactivation occurs.

8. Once shutdown completes, the display changes to **"System Off"**, and the **Power/Active** indicator light turns off.

Exception:

3a. If the system is already off, the control panel displays **"System is already turned off."**

5a. If one or more devices fail to shut down properly, the panel shows **"Partial shutdown – check devices."**

6a. If the connection between control panel and system administrator is lost during shutdown, the control panel displays "Communication error – unable to complete shutdown."

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

1. Direct wired or wireless connection between control panel and system administrator.

References: page 22–23 in Safehome_dialog.pptx

f. Reset the system

Use case: Reset the system
Primary actor: Homeowner
Goal in context: To restart the SafeHome system through the **physical control panel** in order to restore normal operation after a malfunction, error, or configuration change.
Preconditions: The SafeHome control panel and system administrator are physically powered and connected.
The system is either in an **"On"** or **"Error"** state.
The homeowner is physically present and has access to the control panel.
Trigger: The homeowner decides to reset the system (e.g., after an error message, a device failure, or a configuration update)
Include: 1)Common Use Cases : a. Log onto the system through control panel.

Scenario:

1. The homeowner approaches the control panel.
2. The homeowner performs the **login procedure** as described in *"Log onto the system through control panel."*
3. The control panel displays the current status (e.g., "System On," "Error," or "Partial Activation").
4. The homeowner selects "Reset System" from the control panel menu or presses the Reset button.

5. The control panel sends a reset signal to the SafeHome system administrator.
6. The system administrator terminates all current operations and reinitializes all subsystems (sensors, cameras, communication modules).
7. During the reset process, the control panel displays **"Resetting System – Please Wait…"**.
8. The system administrator verifies that all components respond correctly.
9. Once reinitialization completes successfully, the control panel displays **"System On – Ready."**

Exception:

5a. If a subsystem fails to restart, the control panel displays **"Reset incomplete – check device status."**

7a. If repeated resets fail, the system displays **"Critical error – service required."**

Priority: Middle
When available: First increment.
Frequency of use: Occasional — typically during maintenance or troubleshooting.
Channel to actor: control panel
Secondary actors: System administrator
Channel to secondary actors:
System administrator: PC-based system
References: page 24 in Safehome_dialog.pptx

g. Change master password through control panel

Use case: Change the master password through the control panel
Primary actor: Homeowner
Goal in context: To change the existing master password of the SafeHome system using the **physical control panel**, enhancing system security and preventing unauthorized access.
Preconditions: The SafeHome system is powered on and operational.
The control panel and system administrator are connected and functioning properly.
The homeowner knows the current master password.
Trigger: The homeowner decides to change the master password.
Includes: 1)Common Use Cases : a. Log onto the system through control panel.

Scenario:

1. The homeowner approaches the control panel.
2. The homeowner logs onto the system (see *"Log onto the system through control panel"*).
3. After successful login, the homeowner selects **"Change Master Password"** from the control panel menu.

4. The control panel prompts the homeowner to enter the **current master password**.
5. The homeowner enters the current password
6. The control panel validates the password with the system administrator.
7. Upon validation, the control panel prompts the homeowner to enter a **new 4-digit master password**.
8. The homeowner enters the new password.
9. The control panel requests re-entry of the new password for confirmation.
10. The homeowner re-enters the new password.
11. The system administrator verifies both entries match and updates the stored password in secure system memory.
12. The control panel displays **"Password successfully changed."**
13. **The system returns to the main menu.**

Exception:

5a. If the entered current password is incorrect, the control panel displays **"Invalid password – try again."** After three failed attempts, access to this function is locked for a predefined period.

10a. If the two new password entries do not match, the control panel displays **"Passwords do not match – re-enter."**

11a. If the system administrator cannot store the new password due to an internal error, the control panel displays **"Password change failed – please retry."**

Priority: High priority, essential security management function.
When available: First increment.
Frequency of use: Occasional — typically during setup or when the homeowner wishes to enhance security.
Channel to actor: control panel
Secondary actors: System administrator
Channel to secondary actors:

1. System administrator: PC-based system

Open issues:

1. Should password strength or rotation rules be enforced (e.g., prevent reuse of the last password)?
2. Should the system notify the user if the password was changed recently?
3. Should the password change be logged for audit purposes

References: page 20–21 in Safehome_dialog.pptx

2. Security Use Cases

a. Arm/disarm system through control panel

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

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

Exception:

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

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

Priority: Essential
Frequency of use: frequent
Channel to actor: control panel
Secondary actor: System administrator, Sensors (door, window and motion detection)
Channels to secondary actors:

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

Open issues:

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

Reference: p. 21, 39 in the safehome_dialog.pdf

b. Arm/disarm system through web browser

Use case: Arm/disarm system through web browser
Primary Actor: Homeowner
Goal in context: To remotely arm or disarm the SafeHome system via the **SafeHome Products Web site**, enabling control of the home security status while away.
Precondition: The SafeHome system installed at the user's home is online and reachable through the Internet. The homeowner has valid web login

credentials (user ID and two-level password). The web server is operational and connected to the home system.

Trigger: The homeowner decides to change the home's security status while away (e.g., to arm the system after leaving home or disarm it before returning).

Scenario:

1. The homeowner logs onto the **SafeHome Products Web site** — see use case: *"Log onto the system through web browser."*
2. The system displays the main dashboard with available functions.
3. The homeowner selects **"Security"** or **"Arm/Disarm System."**
4. The homeowner chooses either **Arm** (e.g., Away, Home) or **Disarm.**
5. The system sends the command through the web server to the home system administrator.
6. The system administrator activates or deactivates the connected sensors accordingly.
7. The system updates the status on the web interface and displays a confirmation message such as **"System Armed"** or **"System Disarmed."**

Exception:

2a. Invalid login credentials — handled through included use case *"Log onto the system through web browser."*

1-4. If the connection between the web server and home system fails, the interface displays **"Unable to connect to home system – please try again later."**

Priority:	Essential
Frequency of use:	Frequent
Channel to actor:	Web browser (via PC or laptop Internet connection).
Secondary actor:	System administrator, Sensors (door, window, motion detectors).

Channels to secondary actors:

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

Open issues:

1. Should remote arming require additional confirmation or two-factor verification for security?
2. Should partial arming (e.g., night mode) be available through the web interface?
3. Should email/SMS confirmation be sent after successful arming or disarming?

Reference: p. 20, 21, 27 in the safehome_dialog.pdf

c. Arm/disarm safety zone selectively

Use case:	Arm/disarm safety zone selectively
Primary Actor:	Homeowner
Goal in context:	To enable or disable specific safety zones (e.g., kitchen, garage, backyard) of the SafeHome system through the control panel, allowing partial control of monitored areas.
Precondition:	The system is running and accessible through the control panel. The homeowner has logged onto the system through the control panel. The system has predefined safety zones configured.
Trigger:	The homeowner decides to arm or disarm one or more individual safety zones (for example, to keep interior sensors off while sleeping but keep perimeter sensors on).

Scenario:

1. The homeowner logs onto the system through the control panel – see use case: *"Log onto the system through control panel."*
2. The homeowner selects **"Security Zones"** from the control panel menu.
3. The control panel displays a list or map of safety zones (e.g., Zone 1 – Garage, Zone 2 – Living Room).
4. The homeowner selects which zones to arm or disarm.
5. The control panel sends the command to the system administrator.
6. The system administrator activates or deactivates the sensors in the selected zones.
7. The control panel displays the updated status for each zone.

Exception:

2a. If a selected zone includes open doors or windows, the control panel displays **"Zone not secured – close windows/doors."**

1-4. If a zone sensor fails to respond, the system displays **"Sensor fault in Zone X – check device."**

Priority:	Middle
Frequency of use:	Moderate
Channel to actor:	Control panel.
Secondary actor:	System administrator, Sensors (door, window, and motion detectors).

Channels to secondary actors:

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

Open issues:

1. Should the homeowner be able to save multiple predefined zone profiles (e.g., "Night Mode," "Away Mode")?
2. Should the system automatically notify the user when a zone cannot be armed due to an open sensor?

3. Should the web browser also allow partial zone control in future increments?

p. 21, 39 in the safehome_dialog.pdf

d. Alarm condition encountered

Use Case:	Alarm condition encountered
Primary actor:	SafeHome system administrator
Goal In Context:	To automatically detect a potential intrusion, alert the homeowner and monitoring service, and log the event.
Preconditions:	The SafeHome system is running and is in an "armed" state. At least one security zone is active with configured sensors. Each armed security zone is configured with a type: 'Immediate' or 'Entry Delay'. 'Entry Delay' zones have a configured timer value of 60 seconds.
Trigger:	An active sensor within an armed security zone is tripped.

Include:

1)Security use cases: k. Call monitoring service through control panel
2)Security use cases: m. Send Security Alert to Homeowner
3)Security use cases: j. View intrusion log

Scenario:

1. An active sensor in an armed zone sends a trigger signal to the system.
2. The system verifies the signal and checks the configured 'Zone Type' (Immediate or Entry Delay) for the sensor's zone.
3. If the zone type is 'Immediate' (e.g., a window sensor), the system immediately transitions to the "Alarm" state. (Proceed to step 5). If the zone type is 'Entry Delay' (e.g., the front door), the system starts the 60s timer. The system monitors for a valid disarm command via the control panel or web browser while the timer is active.
4. If the delay timer expires with no valid disarm command, the system transitions to the "Alarm" state.
5. Once in the "Alarm" state, the system activates all configured local alarm devices.
6. The system displays a detailed alarm message on the control panel, specifying the triggered zone and sensor.
7. The system sends an alarm notification to all logged-in web browser sessions (see use case: “Send Security Alert to Homeowner”).
8. The system automatically initiates a call to the pre-configured monitoring service (see use case: “Call monitoring service through control panel”).
9. The system records the event details (timestamp, event type, triggered zone, sensor ID) into the intrusion log (see use case: “Add intrusion log”).

Exceptions:

8a. The call to the monitoring service fails to connect.
    1. The system retries the call up to three times at set intervals.

2. If all retries fail, the system logs the connection failure in the system event log.

Priority: Essential
When available: First Increment
Frequency of use: Infrequent
Channel to actor: N/A (System-initiated)
Secondary actor: Homeowner, Monitoring Service, Sensors, Alarm
Channels to secondary actors:

1. Homeowner: Control panel display, web browser interface
2. Monitoring Service: Phone line
3. Sensors: Wireless connectivity
4. Alarm: Direct system connection

Open Issues:

1. What specific information payload is transmitted to the monitoring service during an automated call?
2. How does the system differentiate between a sensor-triggered alarm and a user-initiated panic alarm in its notifications and logs?

Reference: p. 33, 58, 59, 63, 64, 95 in the safehome_dialog.pdf

e. Configure safety zone

Use Case: Configure safety zone
Primary actor: Homeowner
Goal In Context: To access the main interface for creating, viewing,updating, and deleting safety zones.
Preconditions: The homeowner has logged onto the system through the web browser. The system has been configured with sensors.
Trigger: The homeowner decides to manage the grouping of sensors into safety zones.
Scenario:

1. The homeowner logs onto the system through the web browser (see use case: “Log onto the system through web browser”).
2. The homeowner navigates to the "Security" section from the main menu.
3. The homeowner selects the "Safety Zone Configuration" option.
4. The system displays a list of all currently configured safety zones.
5. The system presents the homeowner with options to manage these zones, such as "Create new safety zone," "Update an exist safety zone," and "Delete safety zone”.
6. The homeowner selects an action to proceed:
    a. If "Create" is selected (see use case: “Create new safety zone”)
    b. If "Update" is selected (see use case: “Update an exist safety zone”)
    c. If "Delete" is selected (see use case: “Delete safety zone”)

Exceptions:

4a. If no safety zones have been configured, the system displays a message "No safety zones found" and enables only the "Create new safety zone" option.

1-6. An alarm condition is encountered (see use case: “alarm condition encountered.”)

Priority:	Essential
When available:	First Increment
Frequency of use:	Infrequent
Channel to actor:	web browser
Secondary actor:	SafeHome system

Channels to secondary actors:

1. SafeHome system: Web application interface

Open Issues:

1. Is there a maximum number of safety zones that can be created?
2. Can a single sensor be assigned to more than one safety zone simultaneously?

Reference: p. 21, 39, 70, 71 in the safehome_dialog.pdf

f. Create new safety zone

Use Case:	Create new safety zone
Primary actor:	Homeowner
Goal In Context:	To define a new grouping of sensors that can be armed or disarmed together.
Preconditions:	The homeowner is on the "Safety Zone Configuration" page (see use case: “Configure safety zone”). The system has one or more unassigned sensors.
Trigger:	The homeowner selects the "Create new safety zone" option.

Scenario:

1. The homeowner clicks the "Create new safety zone" button from the safety zone configuration screen.
2. The system displays a form with a field for the zone name and a list of available, unassigned sensors.
3. The homeowner enters a unique name for the new safety zone.
4. The homeowner selects one or more sensors from the list to assign to the new zone.
5. The homeowner clicks the "Save" button.
6. The system validates the provided information.
7. The system saves the new safety zone and its associated sensors.
8. The system displays a confirmation message("Safety zone created successfully") and refreshes the list of safety zones to include the new zone.

Exceptions:

6a. The homeowner enters a zone name that is empty or already in use.

1. The system displays an error message ("Zone name must be unique and cannot be empty") and does not create the zone.

6b. The homeowner does not select any sensors to assign to the zone.

1. The system displays an error message ("A new safety zone must include at least one sensor") and does not create the zone.

1-8. An alarm condition is encountered (see use case: “alarm condition encountered.”)

Priority: Essential
When available: First Increment
Frequency of use: Infrequent
Channel to actor: web browser
Secondary actor: SafeHome system, Sensors
Channels to secondary actors:

1. SafeHome system: Web application interface
2. Sensors: Wireless connectivity

Open Issues:

1. Should there be a character limit for the safety zone name?

Reference: p. 21, 39, 70, 71 in the safehome_dialog.pdf

g. Delete safety zone

Use Case: Delete safety zone
Primary actor: Homeowner
Goal In Context: To permanently remove an existing safety zone from the system configuration.
Preconditions: The homeowner is on the "Safety Zone Configuration" page. At least one safety zone exists.
Trigger: The homeowner decides to remove a safety zone that is no longer needed.

Scenario:

1. The system displays the list of existing safety zones on the configuration page.
2. The homeowner selects the safety zone they wish to remove.
3. The homeowner clicks the "Delete" button corresponding to the selected zone.
4. The system presents a confirmation prompt to the homeowner such as "Are you sure you want to delete it? This action cannot be undone."
5. The homeowner confirms the deletion action.
6. The system removes the safety zone from the configuration. All sensors previously assigned to this zone become "unassigned."
7. The system displays a success message: "Safety zone has been deleted" and updates the list of safety zones.

Exceptions:

5a. The homeowner cancels the action at the confirmation prompt.

1. The system closes the prompt and makes no changes to the safety zone configuration.

1-7. An alarm condition is encountered (“Alarm Condition Encountered.”)

Priority: Essential
When available: First Increment
Frequency of use: Infrequent
Channel to actor: web browser
Secondary actor: SafeHome system
Channels to secondary actors:

1. SafeHome system: Web application interface

Open Issues:

1. What is the system's behavior if a homeowner attempts to delete a safety zone that is currently part of an active Safehome mode configuration?

Reference: p. 21, 39, 70, 71 in the safehome_dialog.pdf

h. Update an existing safety zone

Use Case: Update an existing safety zone
Primary actor: Homeowner
Goal In Context: To modify the name or sensor of an existing safety zone.
Preconditions: The homeowner is on the "Safety Zone Configuration" page. At least one safety zone exists.
Trigger: The homeowner decides to change the configuration of an existing safety zone.

Scenario:

1. The system displays the list of existing safety zones.
2. The homeowner selects the safety zone they wish to modify and clicks the "Update" button.
3. The system displays a form with the current zone name and a list of its assigned sensors, which also shows a list of unassigned sensors that can be added.
4. The homeowner modifies the zone name and/or changes the sensor selection by adding or removing sensors.
5. The homeowner clicks the "Save Changes" button.
6. The system validates the updated information.
7. The system saves the changes to the safety zone configuration.
8. The system displays a confirmation message: "Safety zone updated successfully”, and returns the user to the updated list of safety zones.

Exceptions:

6a. The homeowner changes the zone name to one that is empty or already in use by another zone.
    1. The system displays an error message: "Zone name must be unique and cannot be empty" and does not save the changes.

6b. The homeowner removes all sensors from the zone.
    1. The system displays an error message: "A safety zone must

have at least one sensor" and does not save the changes.

1-8. An alarm condition is encountered (see use case: “alarm condition encountered.”)

Priority: Essential
When available: First Increment
Frequency of use: Infrequent
Channel to actor: web browser
Secondary actor: SafeHome system, Sensors
Channels to secondary actors:

1. SafeHome system: Web application interface
2. Sensors: Wireless connectivity

Open Issues:

1. If a safety zone is updated, how does this affect existing Safehome modes that include this zone? Does the mode update automatically, or does it require manual reconfiguration?

Reference: p. 21, 39, 70, 71 in the safehome_dialog.pdf

i. Configure Safehome modes

Use Case: Configure Safehome modes
Primary actor: Homeowner
Goal In Context: To define which safety zones are armed for each of the system's predefined operational modes.
Preconditions: The homeowner has logged onto the system through the web browser. At least one safety zone has been created.
Trigger: The homeowner decides to customize the arming behavior for different system modes.

Scenario:

1. The homeowner logs onto the system through the web browser (see use case: “Log onto the system through web browser”)
2. The homeowner navigates to the "Security Mode Configuration" page.
3. The system displays a list of configurable modes (e.g., away, home, extended travel, overnight travel).
4. The homeowner selects a mode to configure (e.g., "home").
5. The system presents a list of all existing safety zones with an option to include them in the selected mode.
6. The homeowner selects the safety zones that should be armed when the "home" mode is activated.
7. The homeowner saves the configuration for the selected mode.
8. The system validates and stores the settings.
9. The system displays a confirmation message, "Mode configuration saved successfully."

Exceptions:

7a. The homeowner attempts to save a mode configuration without selecting any safety zones.

1. The system displays a warning message: "At least one

safety zone must be selected for this mode to be effective."

1-9. An alarm condition is encountered ("Alarm Condition Encountered")

Priority: Essential
When available: First Increment
Frequency of use: Infrequent
Channel to actor: web browser
Secondary actor: SafeHome system
Channels to secondary actors:

1. SafeHome system: Web application interface

Open Issues:

1. Are the mode names predefined by the system, or can the homeowner create, rename, or delete modes?

Reference: p. 21, 39 in the safehome_dialog.pdf

j. View intrusion log

Use Case: View intrusion log
Primary actor: Homeowner
Goal In Context: To review a historical record of all alarm events triggered by sensors.
Preconditions: The homeowner has logged onto the system through the web browser.
Trigger: The homeowner decides to review past security incidents.
Include: Common Use Cases: "Log onto the system through web browser."

Scenario:

1. The homeowner logs onto the system through the web browser (use case: "Log onto the system through web browser.")
2. The homeowner navigates to the "Logs" or "Security History" section of the web interface.
3. The homeowner selects the "Intrusion Log" option.
4. The system retrieves all recorded intrusion events from its database.
5. The system displays the events in a list, sorted with the most recent event first. Each entry includes the date, time, the name of the safety zone where the event occurred, and the specific sensor that triggered the alarm.

Exceptions:

5a. No intrusion events have been recorded.

1. The system displays a message such as "No intrusion events to display."

Priority: Essential
When available: First Increment
Frequency of use: Occasional
Channel to actor: web browser

Secondary actor: SafeHome system
Channels to secondary actors:
1. SafeHome system: Web application interface

Open Issues:
1. Does the system provide functionality to filter the intrusion log by date range or by a specific safety zone?
2. Is there a storage limit for the log, and what happens when it is reached (e.g., oldest entries are deleted)?

k. Call monitoring service through control panel

Use Case: Call monitoring service through control panel
Primary actor: Homeowner
Goal In Context: To manually initiate an emergency call to the monitoring service in a perceived emergency situation.
Preconditions: The SafeHome system is powered on. The monitoring service's phone number has been configured in the system settings.
Trigger: The homeowner presses the dedicated "panic button" on the control panel or “Alarm condition encountered”.

Scenario:
1. If the use case initiated by the homeowner: the homeowner presses and holds the designated panic button on the control panel for 2 seconds to prevent accidental activation.
2. The system immediately initiates a phone call to the pre-configured monitoring service.
3. The system transmits relevant data to the monitoring service, such as the home address and the nature of the alarm.
4. The system activates local audible and visual alarms to deter intruders and alert occupants.
5. The control panel displays a message indicating that the emergency service has been called: "EMERGENCY SIGNAL SENT.”

Exceptions:

2a. The phone line is busy or the call fails to connect.
   1. The system retries the call three times.
   2. If all retries fail, the system logs the failure and continues with local alarms.

1-5. When alarm condition is encountered from a sensor simultaneously, system prioritizes the ongoing alarm sequence and ensures the call to the monitoring service includes all relevant event data.

Priority: Essential
When available: First Increment
Frequency of use: Very Infrequent
Channel to actor: Control panel
Secondary actor: SafeHome system, Monitoring Service
Channels to secondary actors:

1. SafeHome system: Direct hardware interaction
2. Monitoring Service: Phone line

Open Issues:

1. Is there a mechanism to cancel a panic call if it was initiated by mistake?
2. Does the system open a two-way audio channel with the monitoring service through the control panel after the call is connected?

Reference: p. 58, 63, 64 in the safehome_dialog.pdf

l. Manage User Accounts and Permissions

Use Case:	Manage User Accounts and Permissions
Primary actor:	Homeowner (with administrative rights)
Goal In Context:	To create, modify, and delete user accounts, and to grant access rights to control what other users can do.
Preconditions:	The homeowner has logged onto the system through the web browser with an administrative account.
Trigger:	The homeowner decides to add a new user, change an existing user's permissions, or remove a user from the system.
Include:	1)Common Use Cases: b)“Log onto the system through web browser.”

Scenario:

1. The homeowner logs onto the system through the web browser (use case: “Log onto the system through web browser.”)
2. The homeowner navigates to the "User Management" section of the web interface.
3. The system displays a list of all current user accounts.
4. The homeowner selects an option to "Add New User," "Edit User," or "Delete User."
5. Assuming the user selected "Add New User", the system presents a form for the new user's details such as username, p.w. and a list of assignable permissions.
6. The homeowner enters the new user's information.
7. The homeowner selects the specific permissions for the new user (e.g., arm/disarm system, view logs, access specific cameras).
8. The homeowner saves the new user account.
9. The system validates the information, creates the account, and displays a confirmation message. The new user now appears in the user list.

Exceptions:

4b. The homeowner attempts to delete the primary master account.
    1. The system displays an error message stating the master account cannot be deleted

6a. The homeowner enters a username that is already taken or provides an invalid password format.
    1. The system displays an error message and prevents the

account from being created.

1-9.An alarm condition is encountered (“alarm condition encountered.”)

Priority: Desirable
When available: Second Increment
Frequency of use: Infrequent
Channel to actor: web browser
Secondary actor: SafeHome system
Channels to secondary actors:
1. SafeHome system: Web application interface

Open Issues:

1. Account system is too complex to be described in one use case, it needs to be extended
2. What is the complete list of assignable permissions?
3. Is there a limit to the number of user accounts that can be created?

Important note: Account system is too complex to be described in only one use case. Its requirements needs to be extended and moved to the separate group of use cases which will be postponed until the next phases of the project or will be dropped if the team cannot meet the deadlines.

Reference: p. 20, 21, 70, 76 in the safehome_dialog.pdf

m. Send Security Alert to Homeowner

Use Case: Send Security Alert to Homeowner
Primary actor: SafeHome system
Goal In Context: To immediately notify the homeowner via personal communication channels when a security alarm is triggered.
Preconditions: An alarm condition has been encountered. The homeowner's contact information is configured in the system settings.
Trigger: The SafeHome system enters the "Alarm" state as part of the "Alarm condition encountered" use case.

Scenario:
1. The SafeHome system enters the "Alarm" state.
2. The system retrieves the pre-configured contact details for the homeowner.
3. The system composes an alert message containing key information: event type (e.g., "Intrusion Alert"), date, time, and the location (triggered zone and sensor).
4. The system sends the alert message to the homeowner's configured contact channels.

Exceptions:
2a. No contact information is configured for the homeowner

1. The system logs the failure to send an alert and proceeds with other alarm actions (siren, monitoring service call).

4a. The system fails to send the notification

1. The system logs the delivery failure.

Priority: Essential
When available: First Increment
Frequency of use: Infrequent
Channel to actor: N/A (System-initiated)
Secondary actor: Homeowner
Channels to secondary actors:

1. Homeowner: Email, SMS, or other configured notification channels.

Open Issues:

1. Can the homeowner configure multiple contact info to receive alerts?
2. Is the content of the alert message customizable by the homeowner?

n. View System Activity Log

Use Case: View System Activity Log
Primary actor: Homeowner
Goal In Context: To review a comprehensive record of all significant system events for auditing or troubleshooting purposes.
Preconditions: The homeowner has logged onto the system through the web browser.
Trigger: The homeowner decides to review the history of system operations.

Scenario:

1. The homeowner logs onto the system through the web browser (Use case: “Log onto the system through web browser.”)
2. The homeowner navigates to the "Logs" or "System History" section of the web interface.
3. The homeowner selects the "System Activity Log" option.
4. The system retrieves all recorded activity events from its database.
5. The system displays the events in a list, sorted with the most recent event first. Each entry includes the timestamp, the user who initiated the action (e.g., "Homeowner," "Guest," "System"), the event type (e.g., "Login," "Arm System," "Settings Changed"), and a brief description.

Exceptions:

5a. No system activity has been recorded yet

1. The system displays a message such as "No system activity to display."

1-5. An alarm condition is encountered (“Alarm Condition Encountered.”)

Priority: Essential
When available: First Increment
Frequency of use: Occasional
Channel to actor: PC-based system with web browser
Secondary actor: SafeHome system
Channels to secondary actors:

1. SafeHome system: Web application interface

Open Issues:

1. Can the activity log be filtered by user, event type, or date range to make it easier to find specific information?
2. Is there a feature to export the activity log for archival purposes?

o. Add intrusion log

Use Case: Add intrusion log
Primary actor: SafeHome system
Goal In Context: To automatically record a new entry in the intrusion log whenever an alarm event occurs.
Preconditions: The SafeHome system is powered on and at least one safety zone is armed.
Trigger: An alarm event has been generated by the system (e.g., from "Alarm condition encountered").

Scenario:

1. The SafeHome system receives an alarm event from the security subsystem.
2. The system gathers relevant event information, including: timestamp of the event, safety zone name where the intrusion occurred ,sensor ID or type that triggered the event, event type (e.g., intrusion, panic alarm), system status at the time of the alarm (e.g., armed mode)
3. The system creates a new record using this information.
4. The system saves the record to the intrusion log database.
5. The system confirms successful storage internally.
6. The new record becomes visible in the homeowner's interface through "View intrusion log."

Exceptions:

5a. Log database unreachable or full.
→ The system temporarily stores the entry in a local cache and retries periodically.
6a. Data validation fails (e.g., missing sensor data).
→ The system records a minimal entry with timestamp and an error flag.

Priority: Essential
When available: First Increment
Frequency of use: Infrequent (only during alarm events)
Channel to actor: N/A (System-initiated)
Secondary actor: System administrator
Channels to secondary actors:
System administrator: PC-based system

Open Issues:

Should failed logging attempts be reported to the homeowner?
Should intrusion logs be immutable (read-only) once created?
What is the maximum size or retention period of the intrusion log?

3. Surveillance Use Cases

a. Display Specific camera view

Use Case:	Display Specific camera view
Primary actor:	Homeowner
Goal In Context:	To see specific camera's view
Preconditions:	System should be ready, and internet should be set; appropriate user ID and passwords must be obtained.
Trigger:	Homeowner decides to take a look of a camera.

Scenario:

1. The homeowner logs onto the system – see use case : "Log onto the system through web browser"
2. The homeowner selects "surveillance" from the major function buttons.
3. The 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 the "view" button.
11. The system displays video output within the viewing window at one frame per second.

Exceptions:

2a. Surveillance function not configured for this system - system displays appropriate error message; see use-case: "Configure surveillance function"(not in the scope of our project)

3a. Homeowner selects "all cameras" - see use-case: "view thumbnail snapshots"

4a. A floor plan is not available or has not been configured--display appropriate error message and see use-case: "configure floor plan." (not in the scope of our project spec)

6a. If the camera does not have a password, go to procedure 9

8a. The password is incorrect or not recognized - if input tries are less than three then prompts for reentry. Otherwise lock system for predefined time.

8b. The password is incorrect or not recognized and no input tries remain? The system prevent the homeowner from accessing the camera

10a. If the camera is disabled, "view" button is disabled – see use case : "Enable camera"

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

encountered."

When available: First increment
Frequency of use: Many times per day
Channel to actor: PC-based system with web browser
Secondary actor: Support technician, Webmaster, Camera
Channels to secondary actors:

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

Open Issues:

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

Reference: p.32-34 in the safehome_dialog.pdf

b. Pan/Zoom specific camera view

Use Case: Pan/Zoom specific camera view
Primary actor: Homeowner
Goal In Context: To adjust the viewing angle or magnification of a specific camera for a better view
Preconditions: System should be ready, and internet should be set; appropriate user ID and passwords must be obtained; Already displaying the Specific camera view
Trigger: The homeowner decides to change the camera's perspective while viewing the live feed

Scenario:

1. The user(Homeowner) already selected a specific camera and displaying the camera’s view - see use case: Display Specific camera view
2. The system displays the camera view along with pan (e.g., up, down, left, right arrows) and zoom (e.g., '+' and '-' buttons) controls
3. The homeowner selects the pan or zoom controls
4. The system sends the corresponding command to the camera
5. The camera adjusts its physical orientation (pan) or digital magnification (zoom)
6. The system displays the updated video feed from the camera in near real-time

Exceptions:

2a. The selected camera does not support pan/zoom functionality - The pan/zoom controls are disabled or hidden.
3a. The camera has reached its maximum pan or zoom limit - The system ignores further commands in that direction.
1-6. An alarm condition is encountered - see use case: "alarm condition encountered."

When available: First increment
Frequency of use: Many times per day
Channel to actor: PC-based system with web browser.
Secondary actor: Camera.<Cam.No>
Channels to secondary actors:

1. Camera wireless connectivity

Open Issues:

1. What is the acceptable latency between user input and the camera's response?

Reference: p.30-31 in the safehome_dialog.pdf

c. Begin camera recording

Use Case: Begin camera recording
Primary actor: Homeowner
Goal In Context: To start recording the video feed from a specific camera for later review
Preconditions: The homeowner is viewing a specific camera feed; Sufficient storage space must be available for the recording
Trigger: The homeowner decides to capture the current events shown by a camera

Scenario:

1. The homeowner is viewing a specific camera (see use case: Display Specific camera view)
2. The homeowner selects the "Record" button on the interface
3. The system verifies that storage space is available
4. The system begins capturing and saving the video stream from the camera.
5. The system provides a clear visual indicator that recording is in progress (e.g., the "Record" button changes to a "Stop" button, a red dot appears on the screen)

Exceptions:

2a. No recording is in progress - The "Stop" button is disabled or clicking it has no effect

4a. An error occurs while saving the file - The system notifies the homeowner of the failure

1-5. An alarm condition is encountered - see use case: "alarm condition encountered."

When available: First increment.
Frequency of use: Few times(3-4times) per month
Channel to actor: PC-based system with web browser
Secondary actor: Camera.<Cam.No>, Storage system
Channels to secondary actors:

1. Camera: wireless connectivity
2. Local or cloud storage interface

Open Issues:

1. What video format and resolution will be used for recordings?

2. How will the system manage storage when it becomes full (e.g., overwrite oldest recording, stop recording and alert user)?
3. Should the "scheduled recording" or "auto-recoeding" being add?(e.g. Record from 10:00am-9:00pm each Monday-Friday)

Reference: p.31 in the safehome_dialog.pdf

d. Stop camera recording

Use Case: Stop camera recording
Primary actor: Homeowner
Goal In Context: To stop an ongoing recording for a specific camera
Preconditions: A recording is currently in progress for the camera being viewed
Trigger: The homeowner decides the event they wanted to capture has ended

Scenario:

1. The system is currently recording a camera feed (following the "Begin camera recording" use case).
2. The homeowner selects the "Stop" button
3. The system stops capturing the video stream
4. The system finalizes and saves the recorded video file to storage.
5. The system removes the visual indicator for recording.

Exceptions:
2a. No recording is in progress - The "Stop" button is disabled or clicking it has no effect
4a. An error occurs while saving the file - The system notifies the homeowner of the failure. (e.g. not enough memory for saving)
1-5. An alarm condition is encountered - see use case: "alarm condition encountered."
When available: First increment.
Frequency of use: Few times(3-4times) per month
Channel to actor: PC-based system with web browser
Secondary actor: Camera.<Cam.No>, Storage system
Channels to secondary actors:

1. Camera: wireless connectivity
2. Local or cloud storage interface

Open Issues:

1. What is the naming convention for saved video files to ensure they are easily identifiable?

e. Replay camera recording

Use Case: Replay camera recording
Primary actor: Homeowner
Goal In Context: To view a previously recorded video

Preconditions: The homeowner is logged into the web application
At least one video has been recorded and saved
Trigger: The homeowner wants to review a past event
Scenario:

1. The homeowner logs onto the system – see use case : “Log onto the system through web browser”
2. The homeowner navigates to the surveillance section and selects an option to view recordings (e.g., "Replay" or "View Recordings")
3. The system displays a list of available recordings, organized by camera, date, and time
4. The homeowner selects a specific recording from the list
5. The system retrieves the video file from storage
6. The system displays the recorded video in a player interface with controls (e.g., play, pause, seek bar, volume)

Exceptions:
3a. No recordings are available - The system displays a message "No recordings found."
4a. The selected recording file is corrupted or cannot be found - The system displays an error message
1-6. An alarm condition is encountered - see use case: "alarm condition encountered."
When available: First increment.
Frequency of use: Few times(3-4times) per month
Channel to actor: PC-based system with web browser
Secondary actor: Storage system
Channels to secondary actors:

1. Local or cloud storage interface

Open Issues:

1. How will the system handle playback of very large video files to ensure smooth performance?
2. Will there be a feature to export or delete recordings?

f. Set camera password

Use Case: Set the password for a specific camera
Primary actor: Homeowner
Goal In Context: To setup a password to secure the feed of a specific camera
Preconditions: System should be ready, and internet should be set; appropriate user ID and passwords must be obtained.
Trigger: Homeowner decides to setup a password for a specific camera.
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 major function buttons.
3. The homeowner selects “Camera password”
4. The system displays the available Cameras

5. The homeowner chooses one Camera
6. The homeowner chooses “Set password”
7. The homeowner inputs a password for this Camera
8. The system updates by asking a for this password when it is chosen in the “Display specific camera view”

Exceptions:

6a. If the camera already has a password, the button does not work and displays “Password already set” message.

7a. Verify that the password has the correct input-format (eg. 4 int pin, 8 alphanumerical..)

When available: First increment
Frequency of use: Once/Infrequent
Channel to actor: PC-based system with web browser
Secondary actor: SafeHome system
Channels to secondary actors:

SafeHome system: Web application interface

Open Issues:

1. What to do if the Homeowner forgets the password.

Reference: p.31 in the safehome_dialog.pdf

g. Delete camera password

Use Case: Delete the password for a specific camera
Primary actor: Homeowner
Goal In Context: To delete the password of a specific camera
Preconditions: System should be ready, and internet should be set; appropriate user ID and passwords must be obtained.
Trigger: Homeowner decides to delete the password of a specific camera.

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 major function buttons.
3. The homeowner selects “Camera password”
4. The system displays the available Cameras
5. The homeowner chooses one Camera
6. The homeowner chooses “Delete password”
7. The homeowner deletes the password for this Camera
8. The system updates by no longer asking a for this password when it is chosen in the “Display specific camera view”

Exceptions:

6a. If the camera does not have a password, the button does not work and displays “This camera has no password” message.

When available: First increment
Frequency of use: Infrequent
Channel to actor: PC-based system with web browser
Secondary actor: SafeHome system

Channels to secondary actors:

SafeHome system: Web application interface

Open Issues:

?

h. View thumbnail Shots

Use Case:	Display all *unlocked* camera view at the same time
Primary actor:	Homeowner
Goal In Context:	To see every angle of the home covered by cameras
Preconditions:	System should be ready, and internet should be set; appropriate user ID and passwords must be obtained.
Trigger:	Homeowner decides to look at all the cameras at once

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 "overview"
4. The system displays all *available* cameras without a password, along with a list of all *blocked* cameras with a "unblock" button next to it.
5. The homeowner selects the "unblock" button of a *blocked* camera
6. The system asks for a password.
7. The homeowner enters the password.
8. The system validates the password.
9. The system adds the camera to the display.

Exceptions:

4a. If one camera does not work, display all the others and a message "Error with Camera #"

8a. The password is incorrect or not recognized - if input tries are less than three then prompts for reentry. Otherwise lock system for predefined time.

8b. The password is incorrect or not recognized and no input tries remain? The system prevent the homeowner from accessing the camera

When available:	First increment
Frequency of use:	Many times per day
Channel to actor:	PC-based system with web browser
Secondary actor:	Support technician, Webmaster, Camera

Channels to secondary actors:

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

Open Issues:

1. Is there enough internet bandwidth to receive the live recording of all the available cameras ?

Reference: p.31 in the safehome_dialog.pdf

i. Enable camera

Use Case: Enable a Camera
Primary actor: Homeowner
Goal In Context: Enable a Camera that was disabled
Preconditions: System should be ready, and internet should be set;
appropriate user ID and passwords must be obtained
Camera must be plugged in and connected.
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 homeowner chooses one Camera
5. The homeowner selects "Enable/Disable"
6. The system updates to activate the camera and allow to see the feed

Exceptions:
5a. If the camera is already Enabled, refer to use case "Disable camera"
When available: First increment
Frequency of use: Infrequent
Channel to actor: PC-based system with web browser
Secondary actor: SafeHome system
Channels to secondary actors:
SafeHome system: Web application interface
Open Issues:

1. If the camera had a password before being disabled, does it keep the password when it is reenabled ?

j. Disable camera

Use Case: Disable a Camera
Primary actor: Homeowner
Goal In Context: Disable a Camera that was enabled
Preconditions: System should be ready, and internet should be set;
appropriate user ID and passwords must be obtained
Camera must be plugged in and connected.
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 homeowner chooses one Camera
5. The homeowner selects "Enable/Disable"

6. The system updates to deactivate the camera, i.e. no longer allow to see the feed.

Exceptions:

5a. If the camera is already Disabled, refer to use case “Enable camera”

When available: First increment
Frequency of use: Infrequent
Channel to actor: PC-based system with web browser
Secondary actor: SafeHome system
Channels to secondary actors:

SafeHome system: Web application interface

Open Issues:

1. If the camera had a password before disabling, do we keep track of this password ?

VII. Sequence Diagram

1. Common Sequence Diagram

a. Log onto the system through control panel

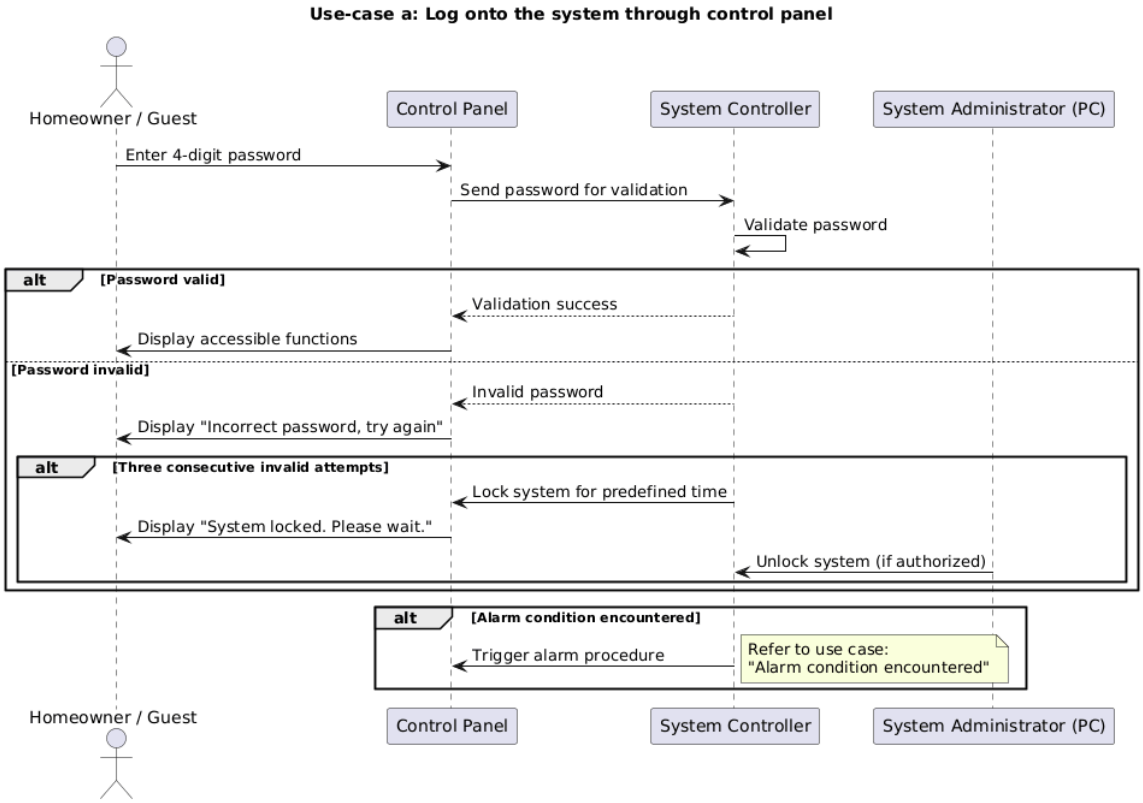

Figure 11. Log onto the system through control panel Sequence Diagram

b. Log onto the system through web browser

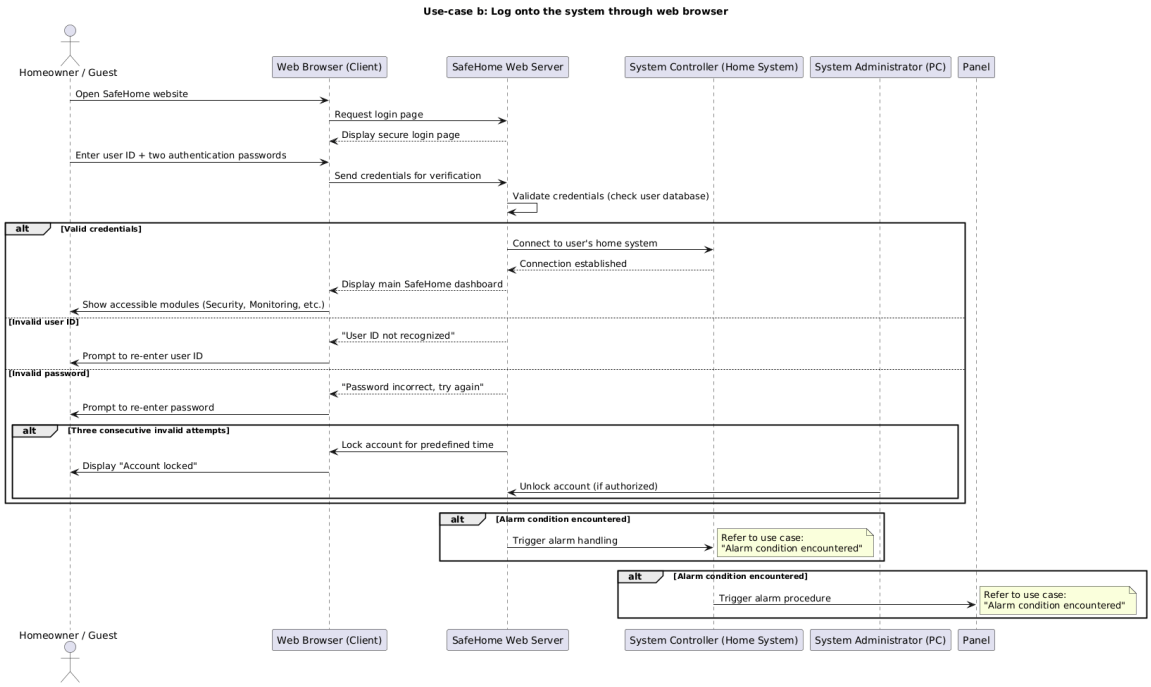

Figure 12. Log onto the system through web browser Sequence Diagram

c. Configure system setting

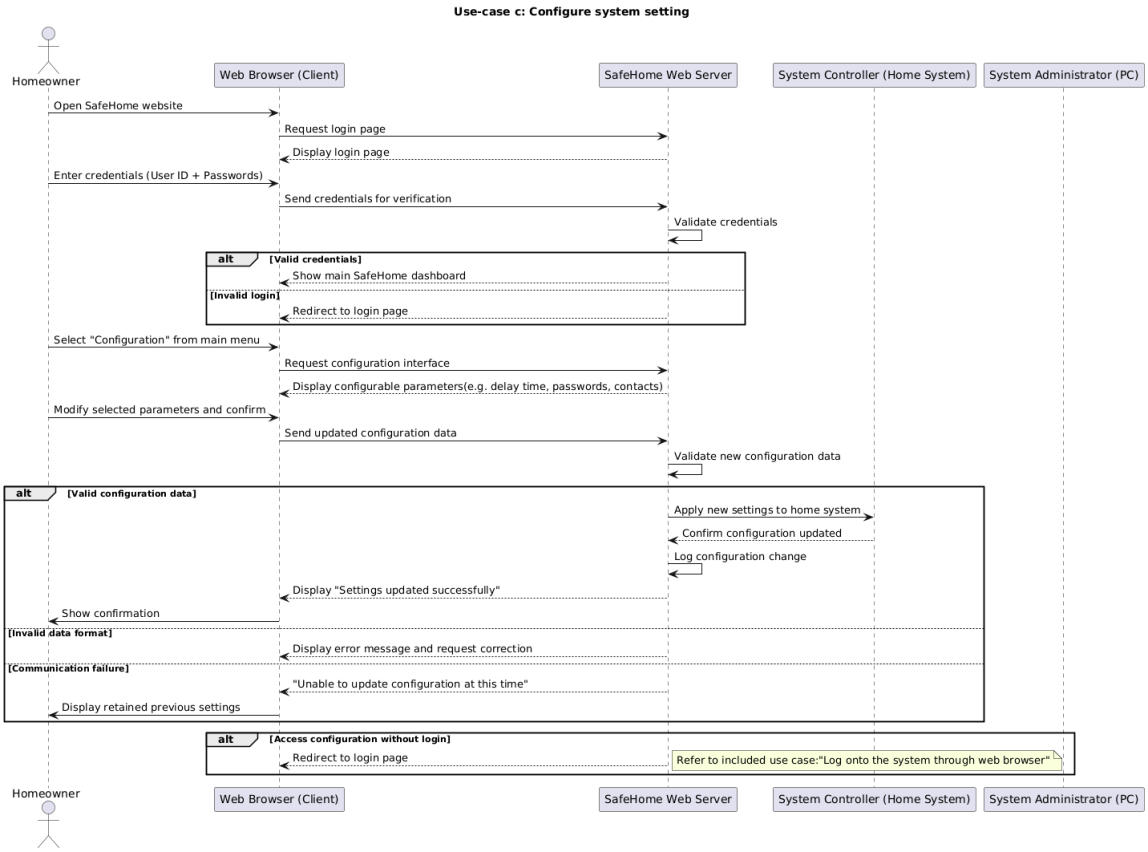

Figure 13. Configure system setting Sequence Diagram

d. Turn the system on

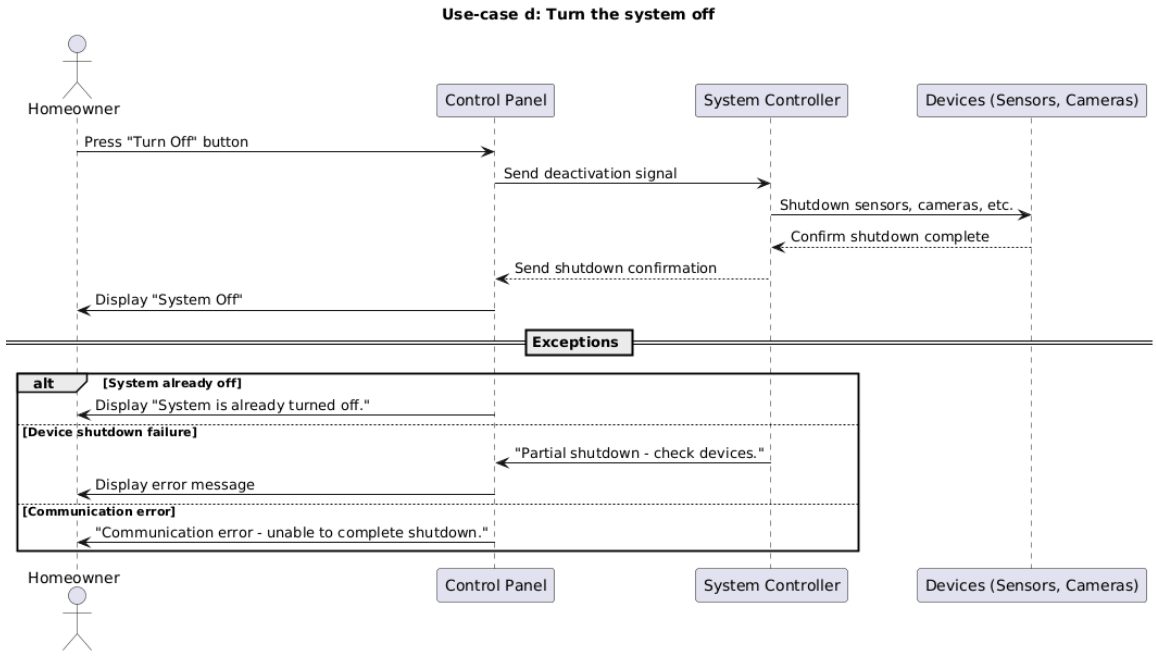

Figure 14. Turn the system on Sequence Diagram

e. Turn the system off

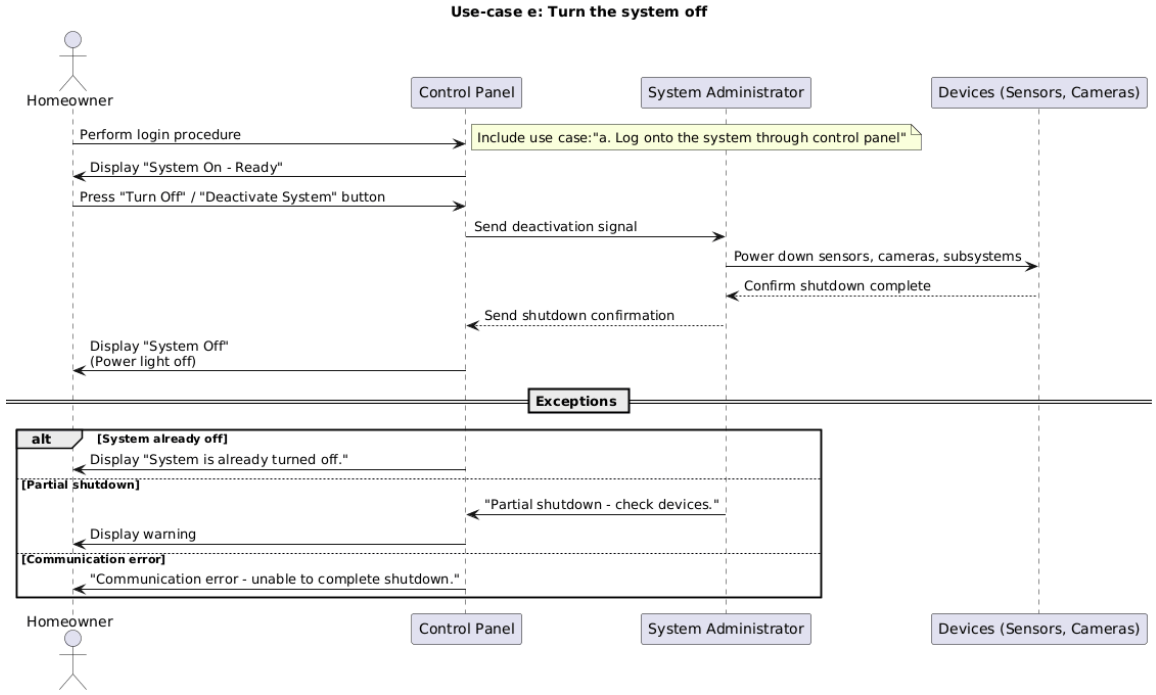

Figure 15. Turn the system off Sequence Diagram

f. Reset the system

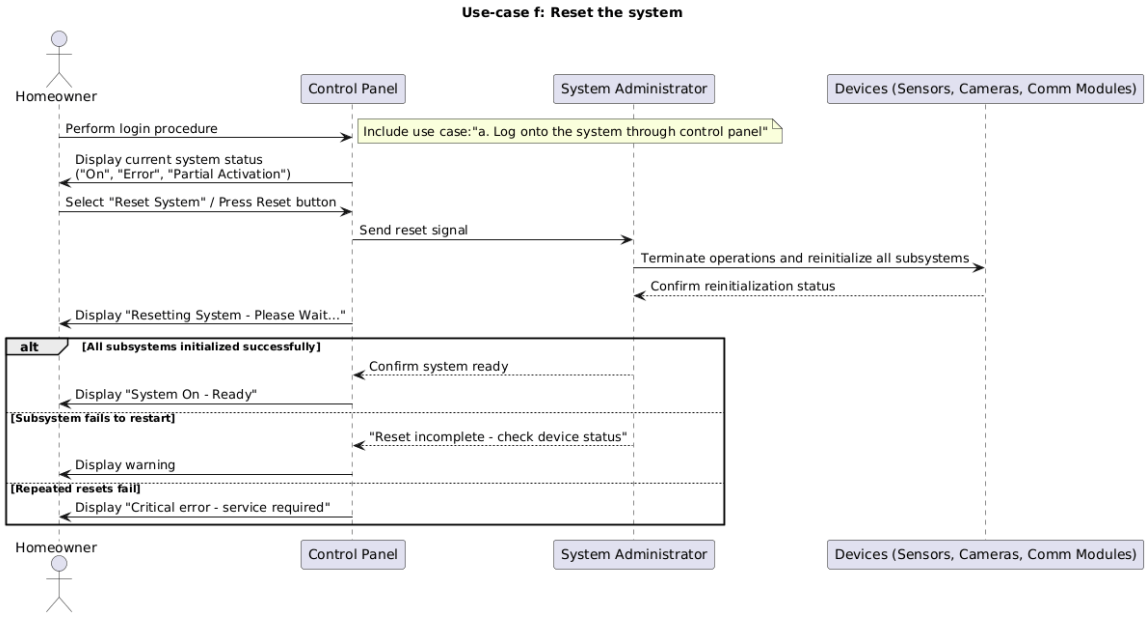

Figure 16. Reset the system off Sequence Diagram

g. Change master password through control panel

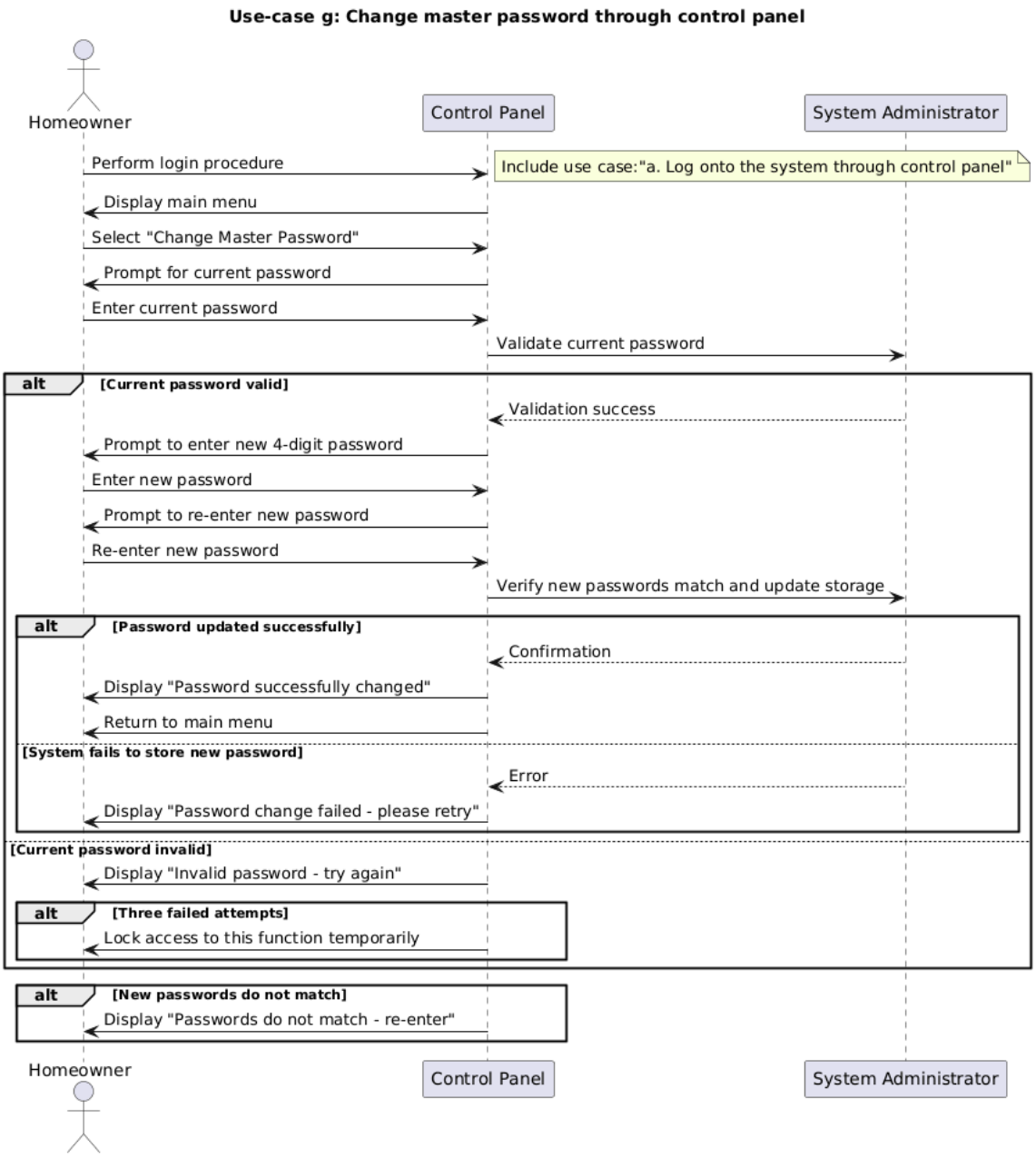

Figure 17. Reset the system off Sequence Diagram

Reference in SEPA dialog slide: slide X, meeting log YY.MM.DD, and/or item Z in page W

2. Security Sequence Diagram

a. Arm/disarm system through control panel

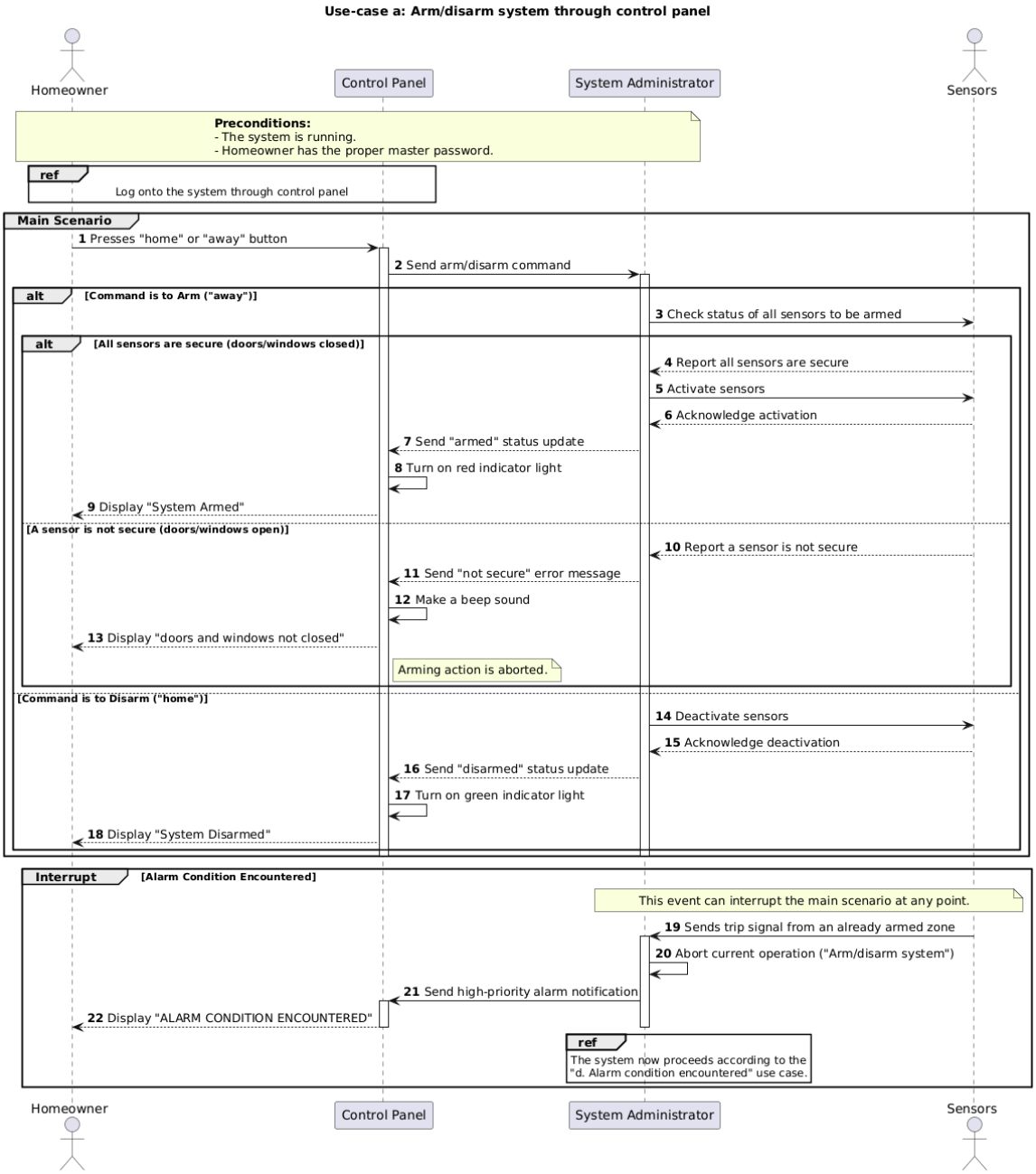

Figure 18. Arm/disarm system through control panel Sequence Diagram

b. Arm/disarm system through web browser

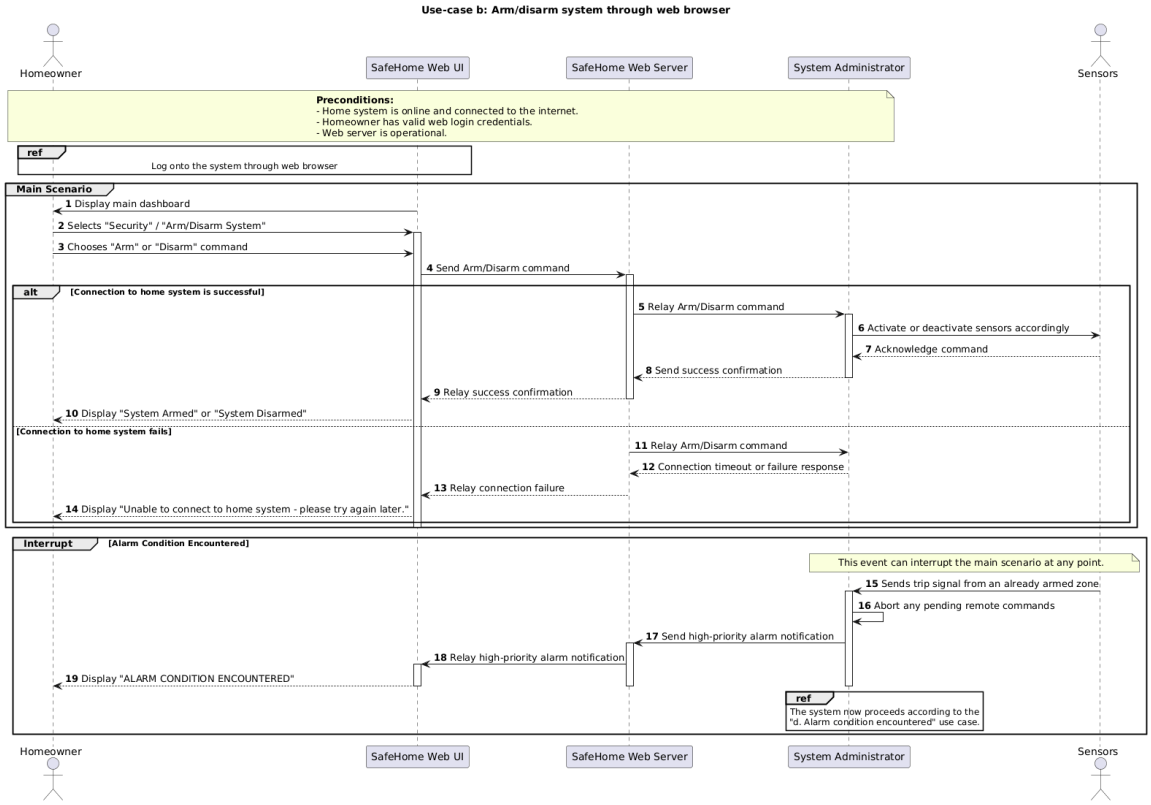

Figure 19. Arm/disarm system through web browser Sequence Diagram

c. Arm/disarm safety zone selectively

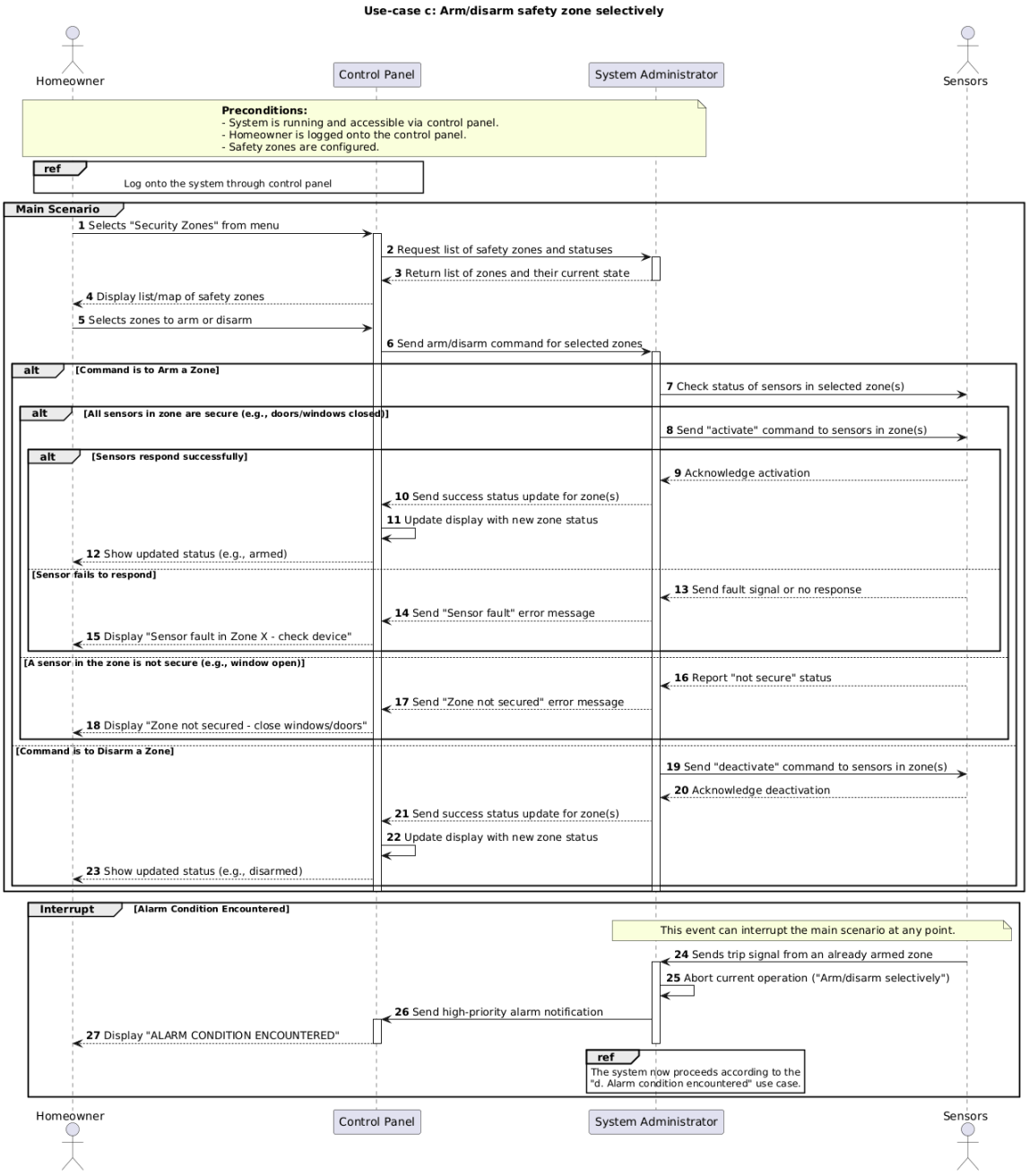

Figure 20. Arm/disarm system safety zone selectivity Sequence Diagram

d. Alarm condition encountered

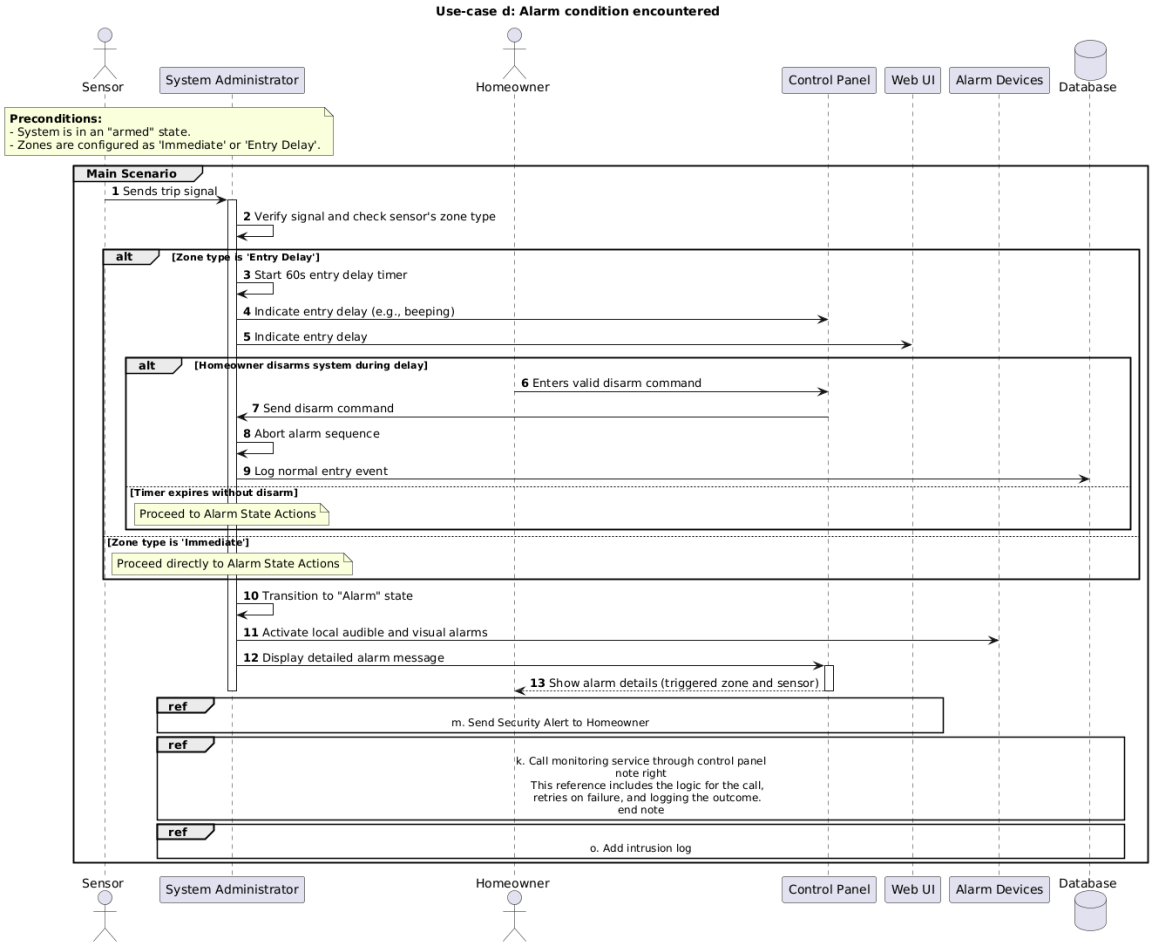

Figure 21. Alarm condition encountered Sequence Diagram

e. Configure safety zone

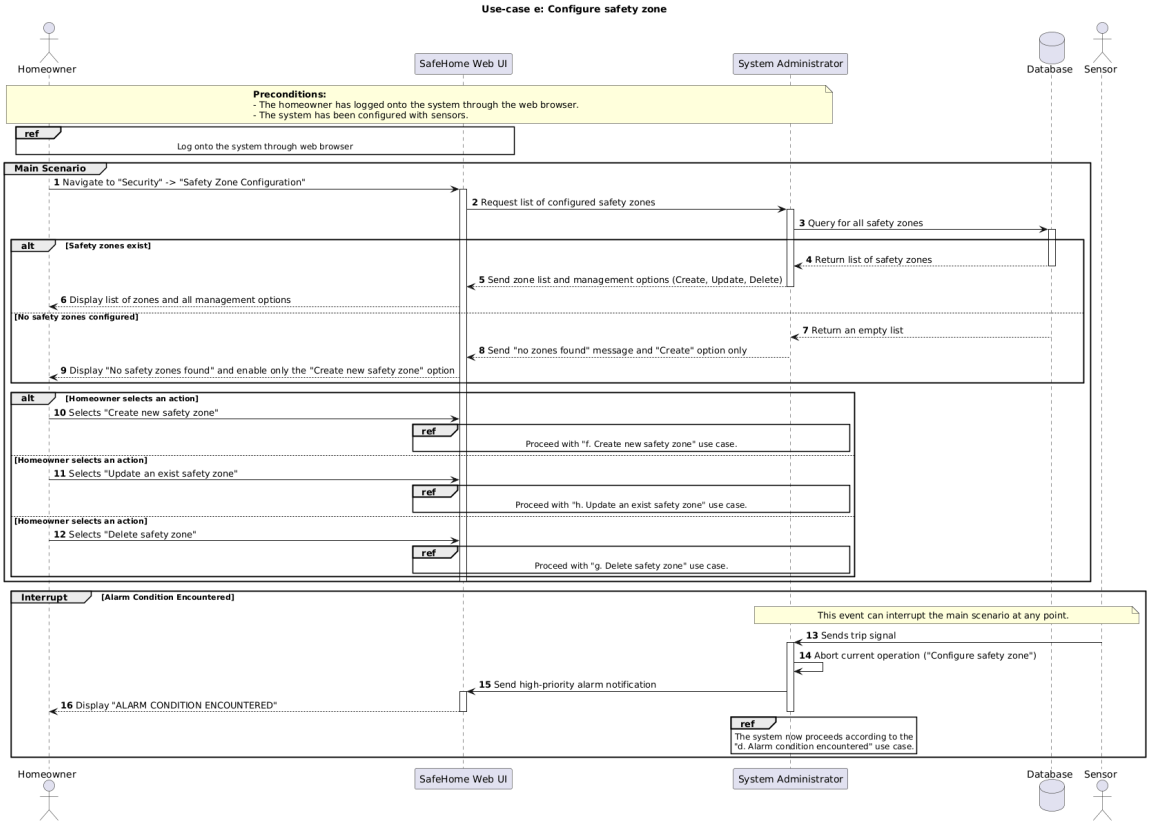

Figure 22. Configure safety zone Sequence Diagram

f. Create new safety zone

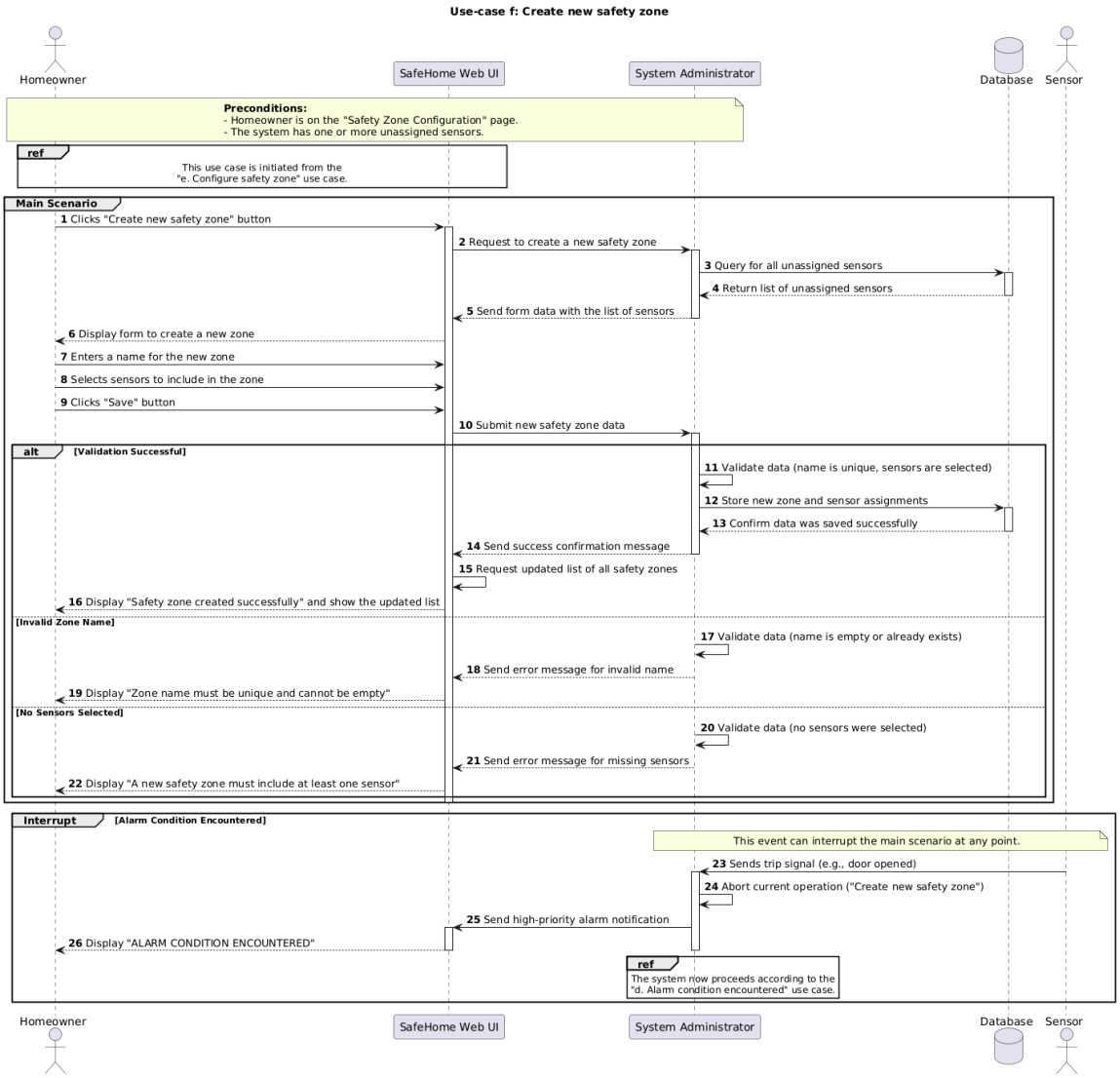

Figure 23. Create new safety zone Sequence Diagram

g. Delete safety zone

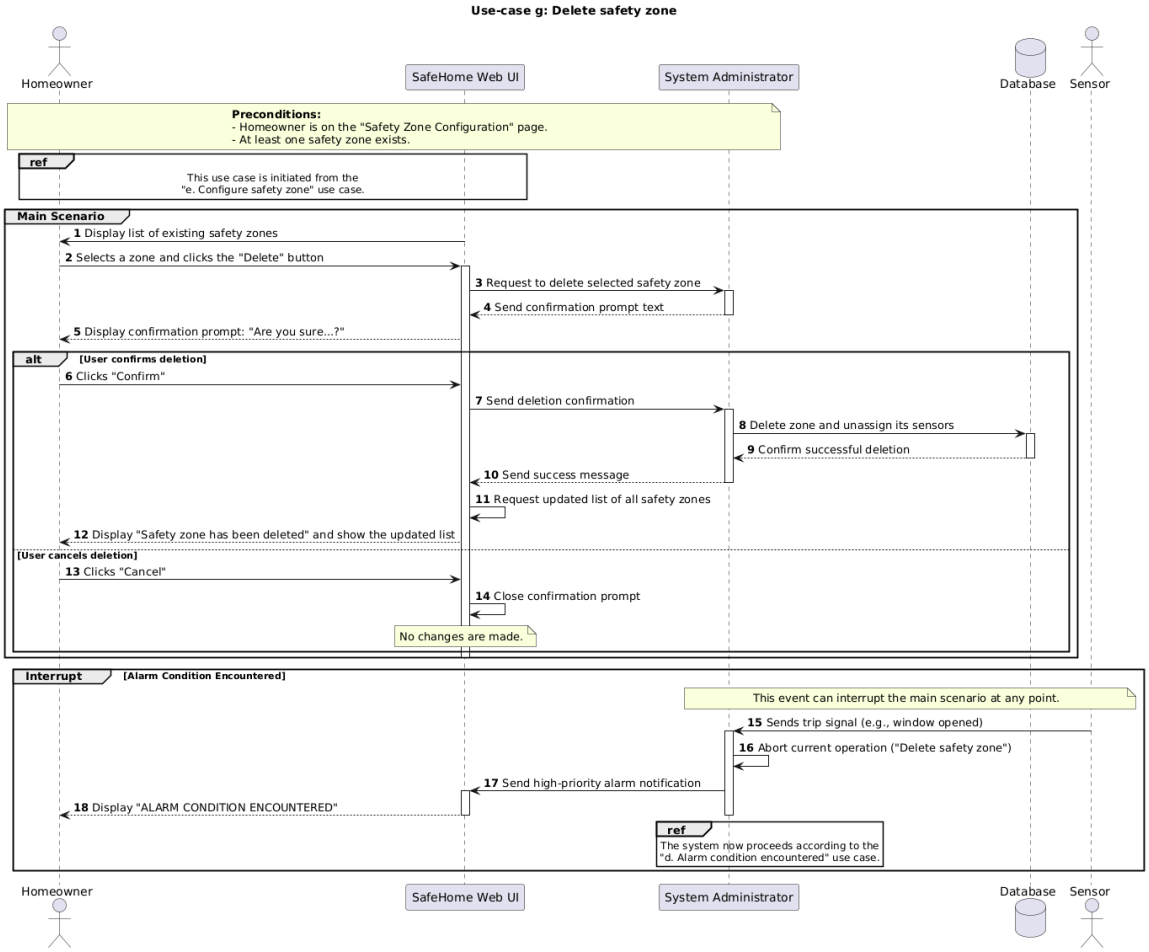

Figure 24. Delete safety zone Sequence Diagram

h. Update an existing safety zone

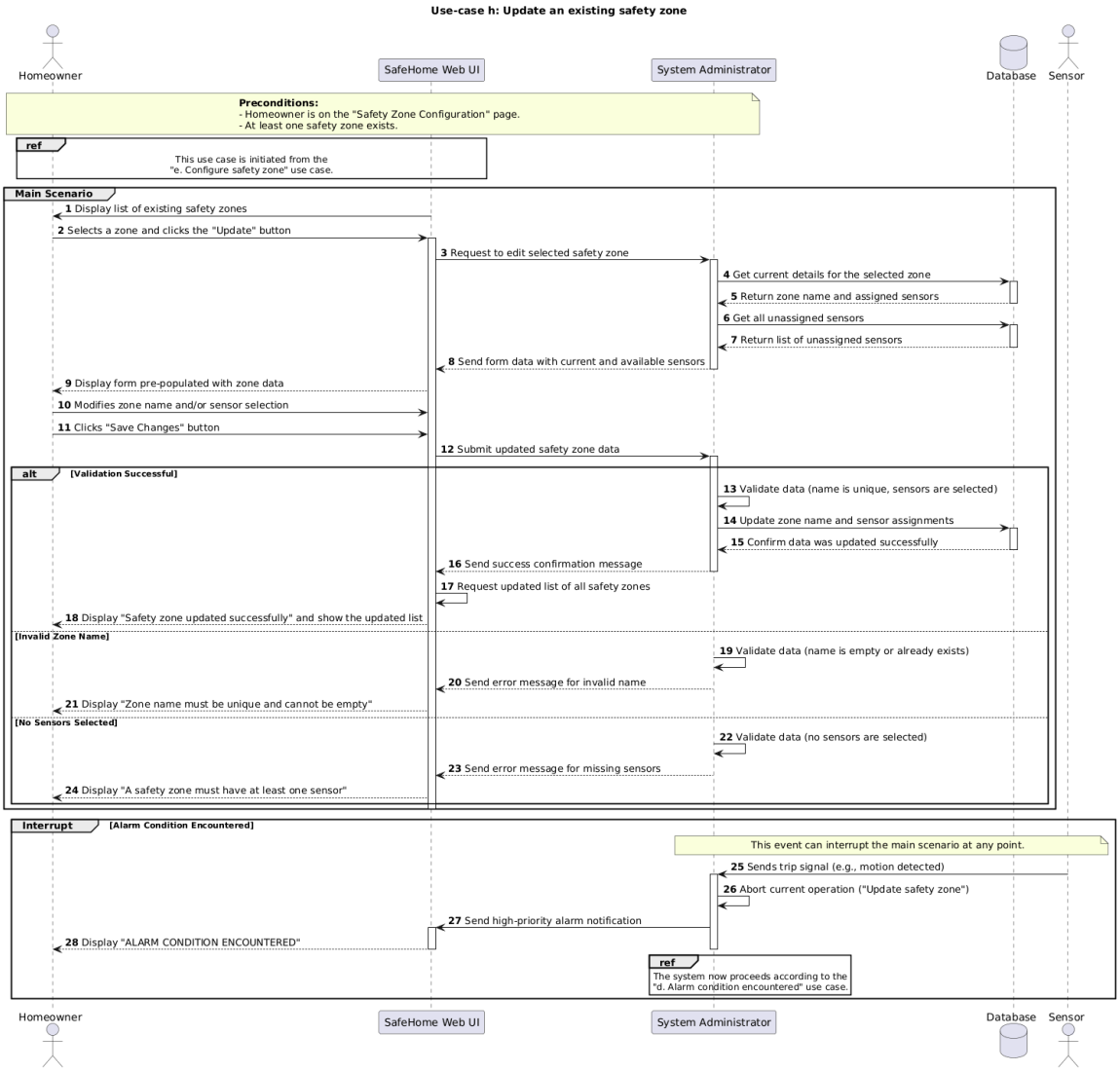

Figure 25. Update an existing safety zone Sequence Diagram

i. Configure Safehome modes

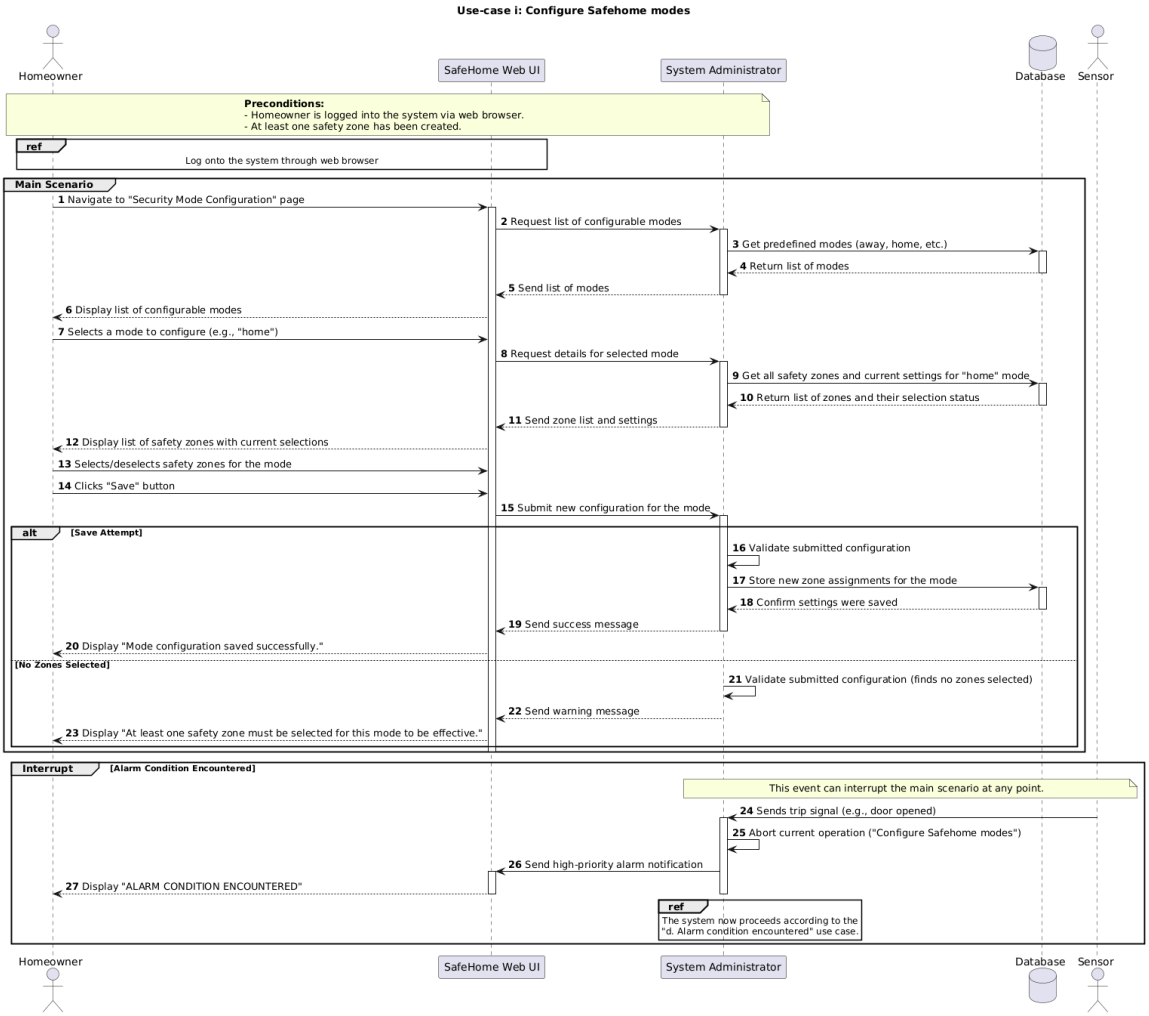

Figure 26. Configure Safehome modes Sequence Diagram

j. View intrusion log

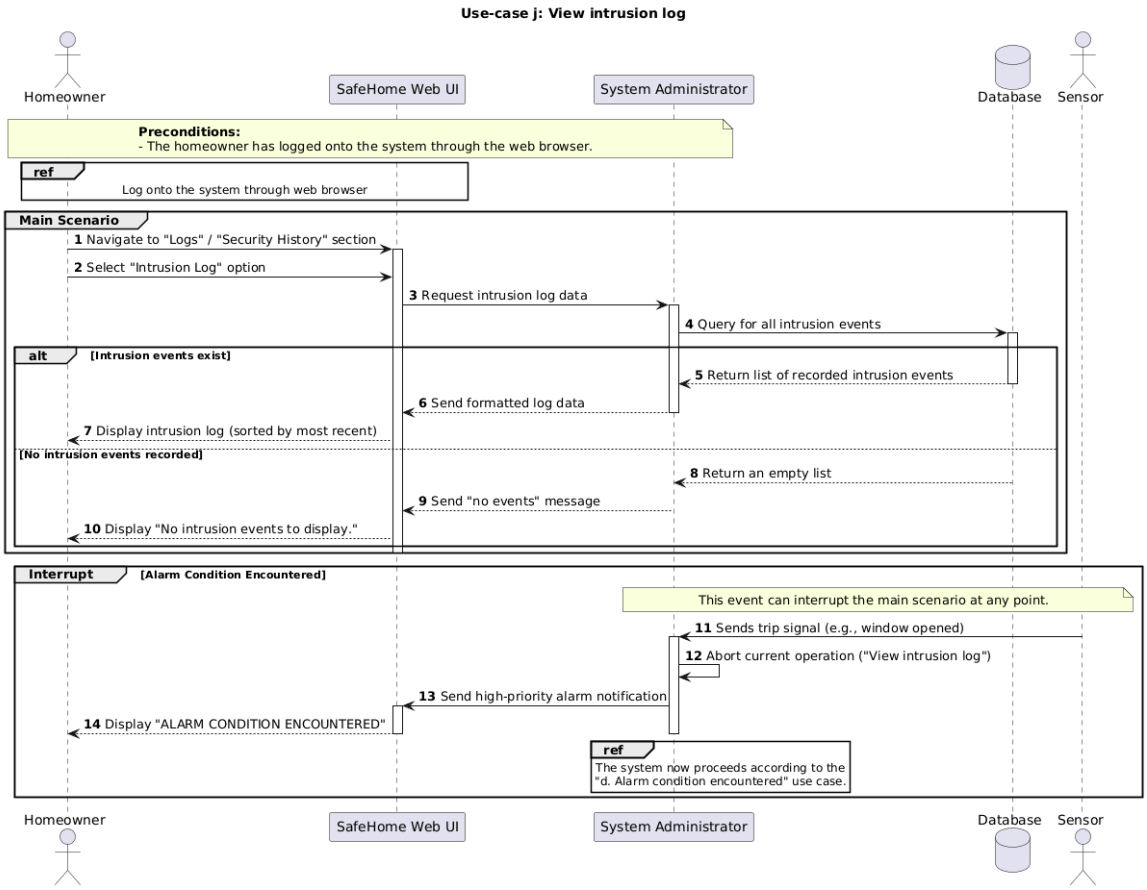

Figure 27. View intrusion log Sequence Diagram

k. Call monitoring service through control panel

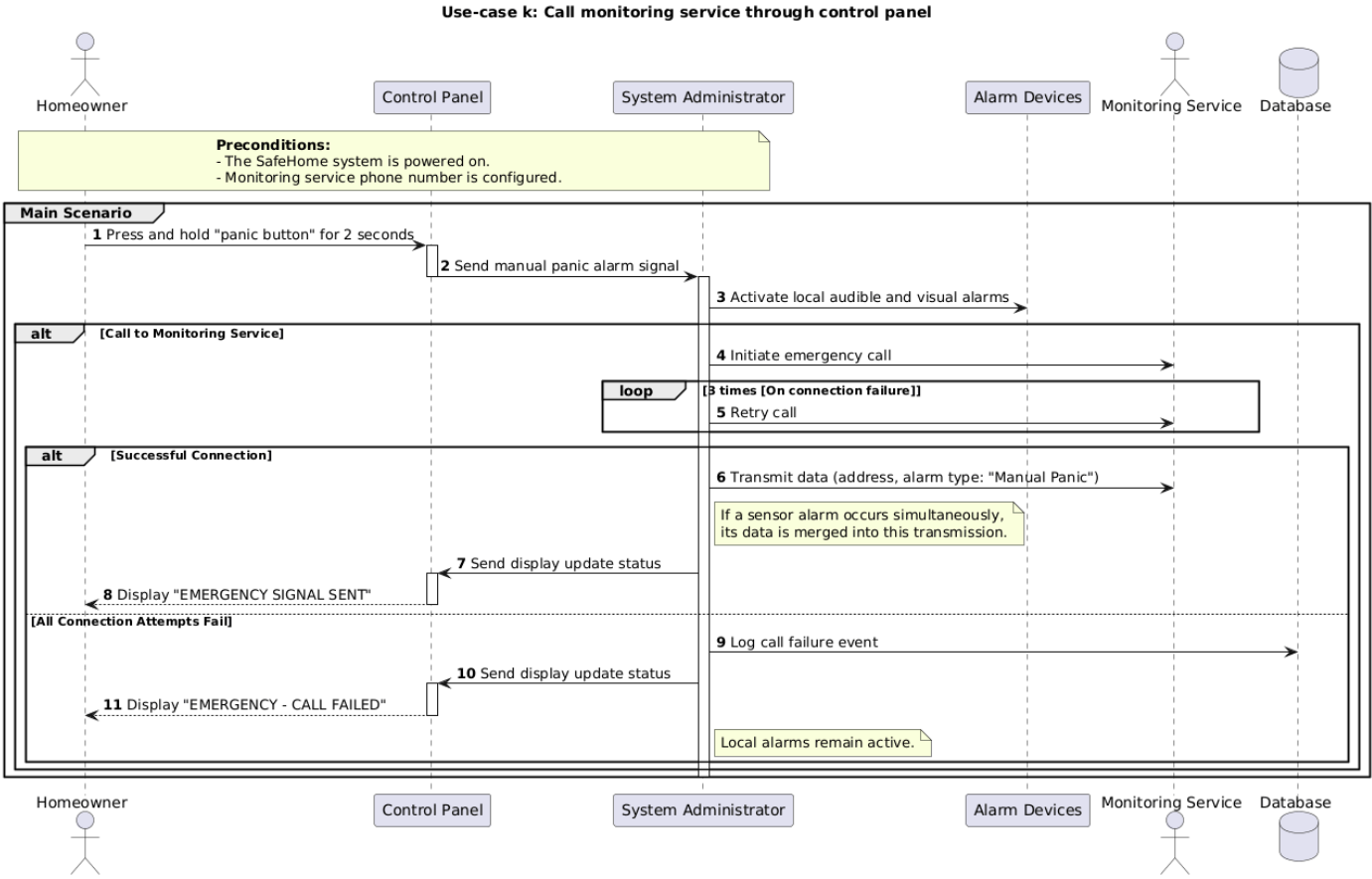

Figure 28. Call monitoring service through control panel Sequence Diagram

l. Manage User Accounts and Permissions

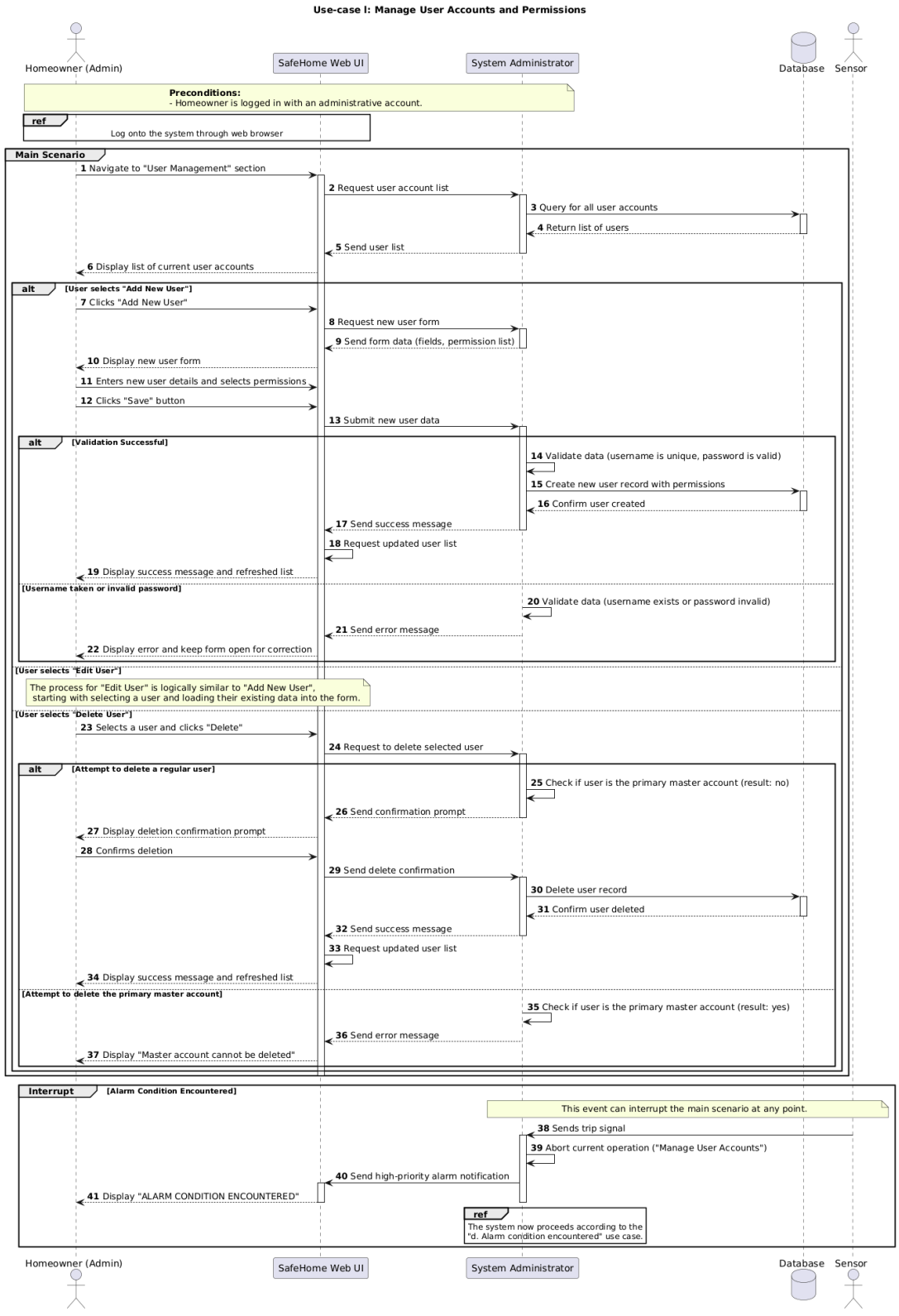

Figure 29. Manage User Accounts and Permissions Sequence Diagram

m. Send Security Alert to Homeowner

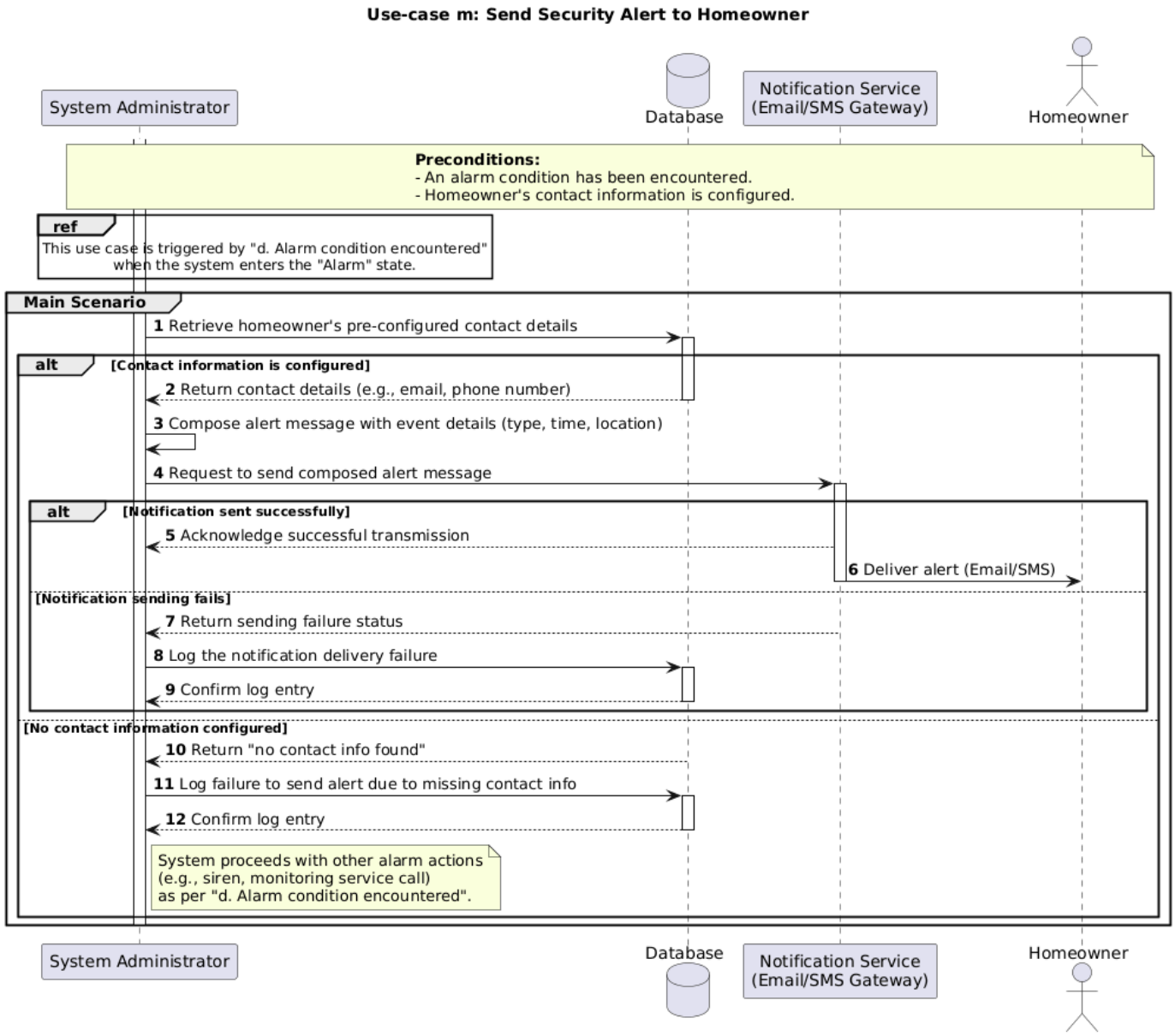

Figure 30. Send Security Alert to Homeowner Sequence Diagram

n. View System Activity Log

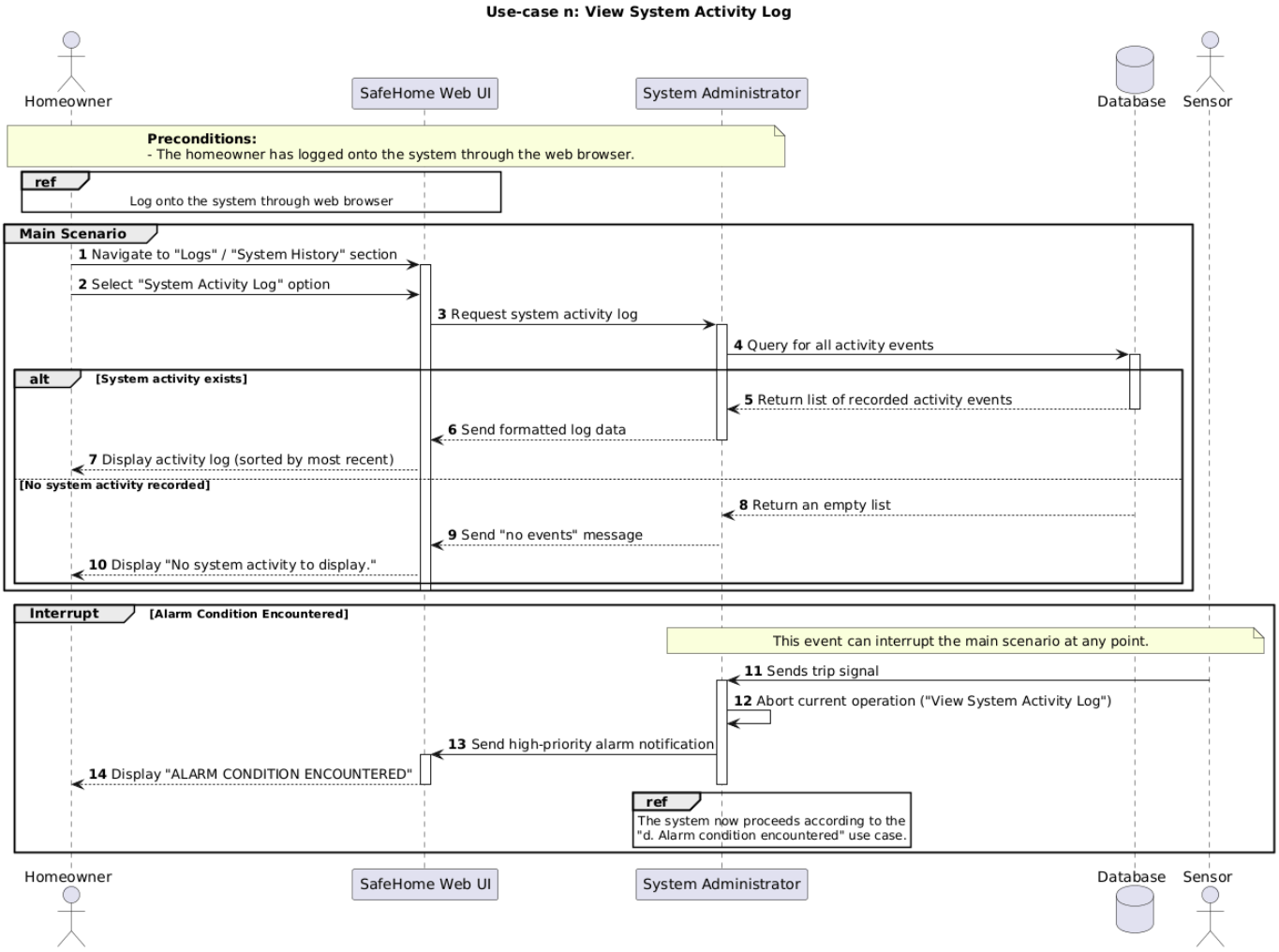

Figure 31. View System Activity Log Sequence Diagram

o. Add intrusion log

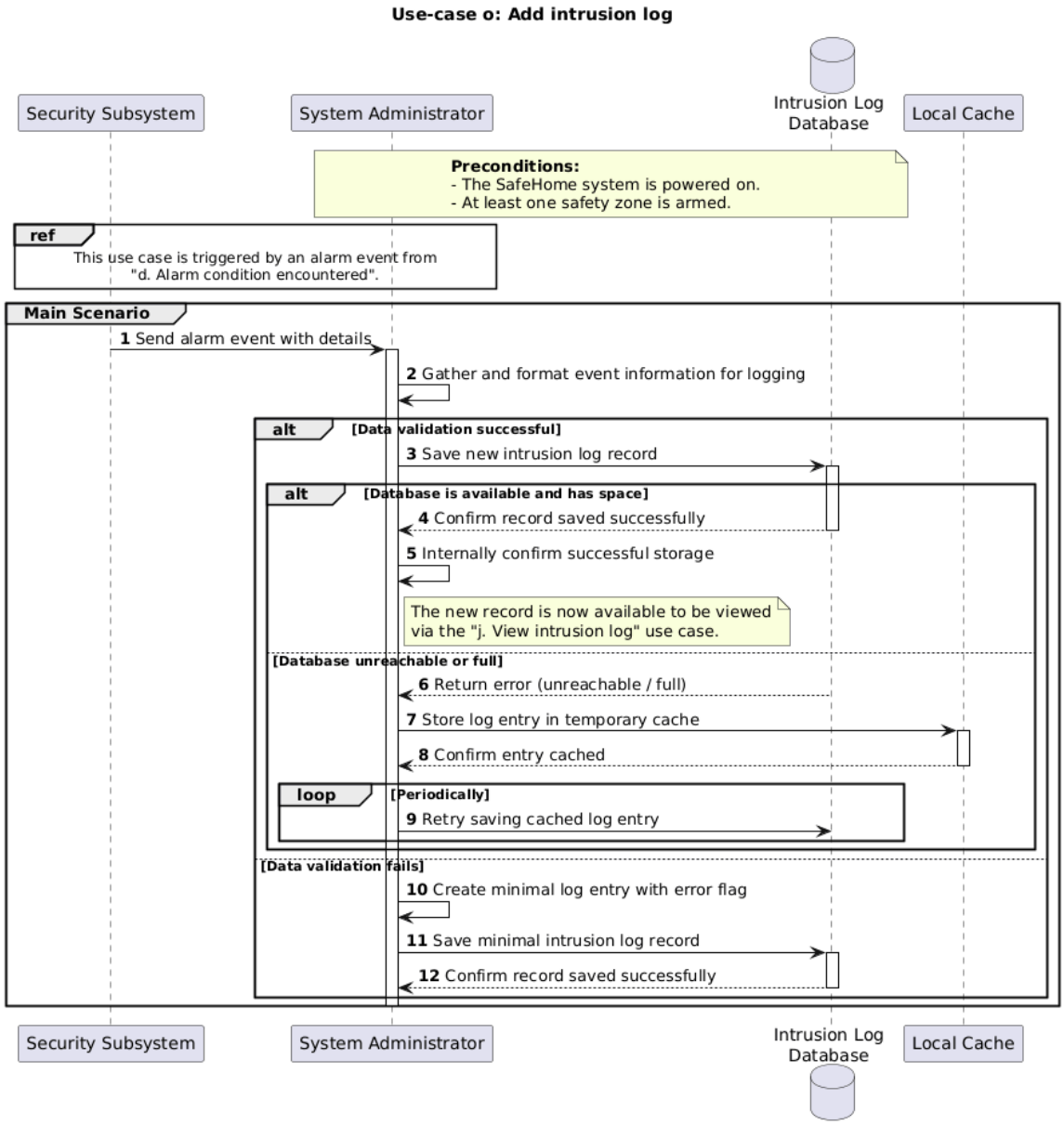

Figure 32. Add intrusion log Sequence Diagram

3. Surveillance Sequence Diagram

a. Display Specific camera view

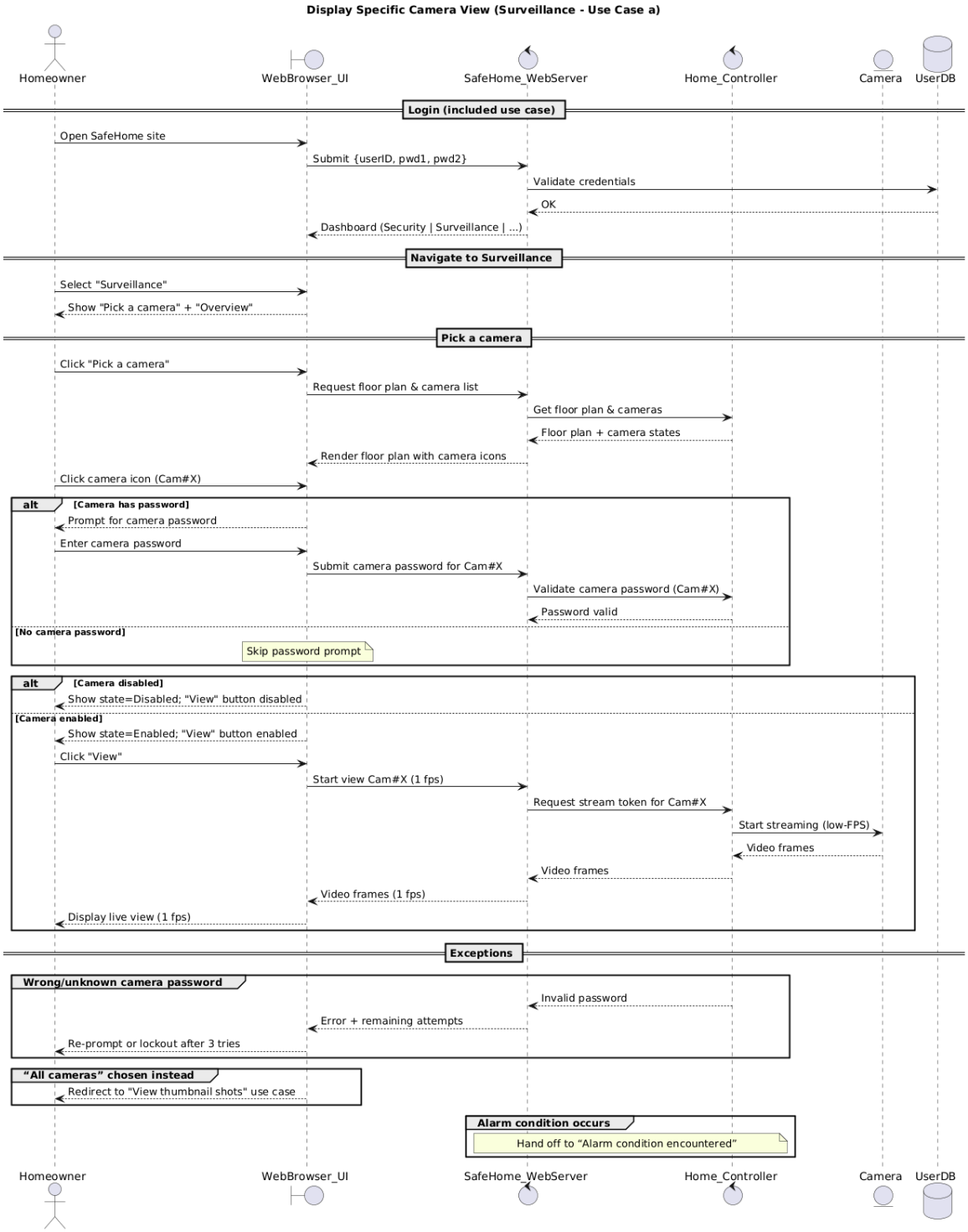

Figure 33. Display Specific camera view Sequence Diagram

b. Pan/Zoom specific camera view

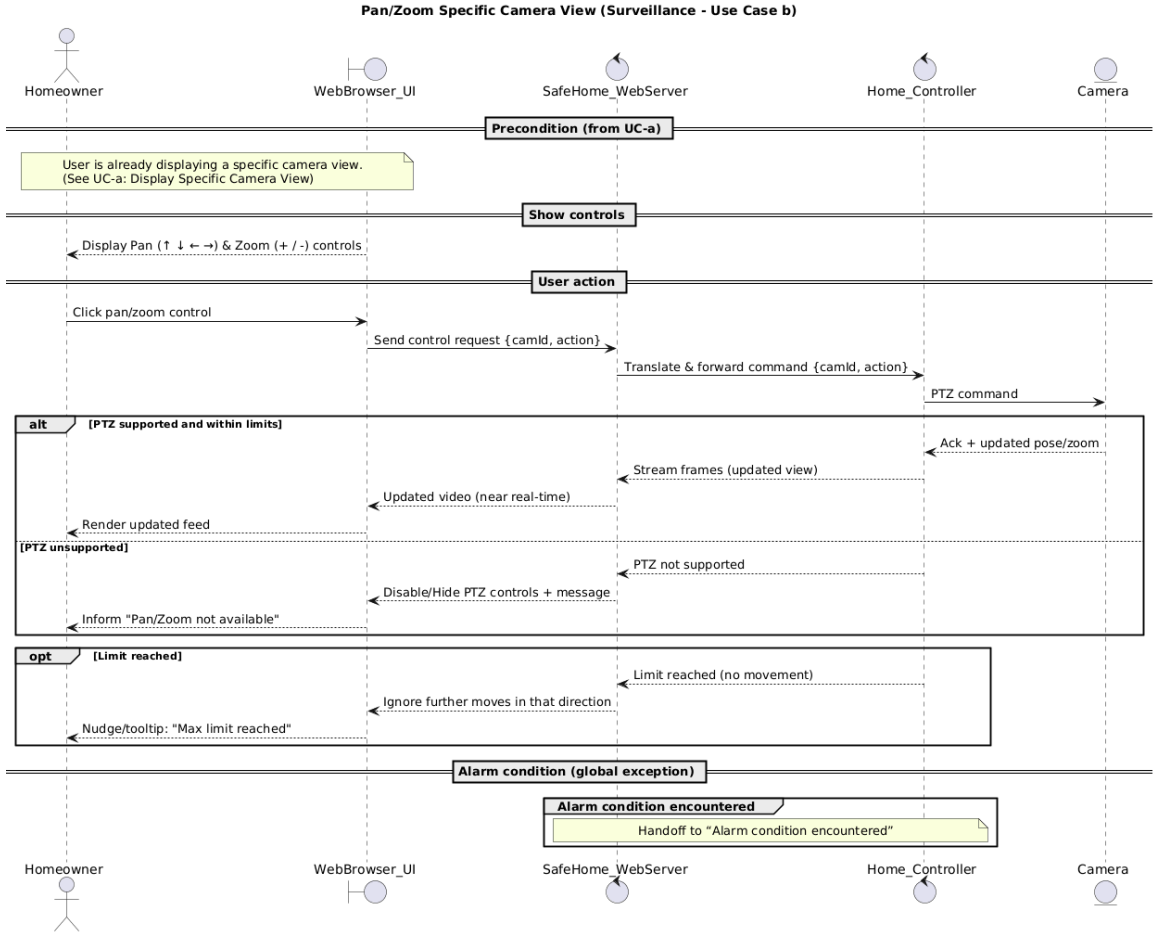

Figure 34. Pan/Zoom specific camera view Sequence Diagram

c. Begin camera recording

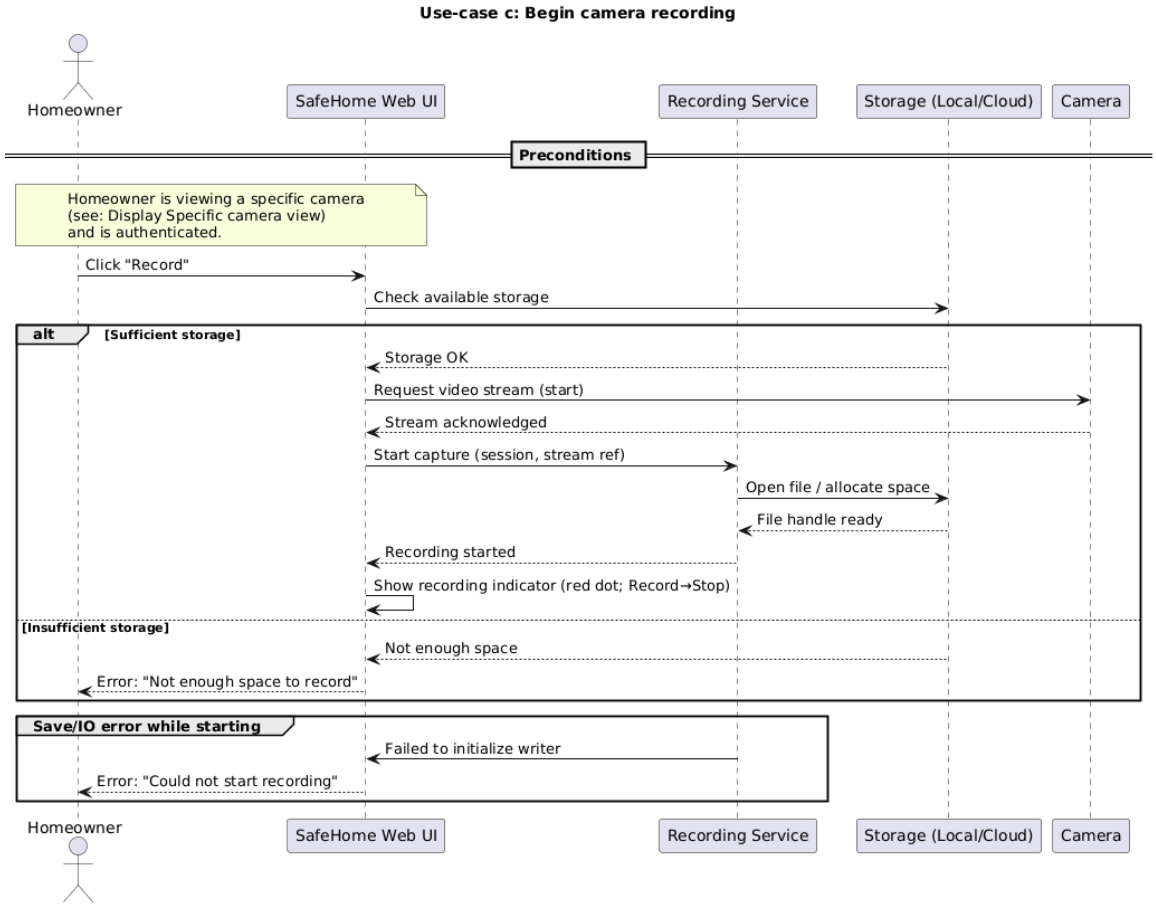

Figure 35. Begin camera recording Sequence Diagram

d. Stop camera recording

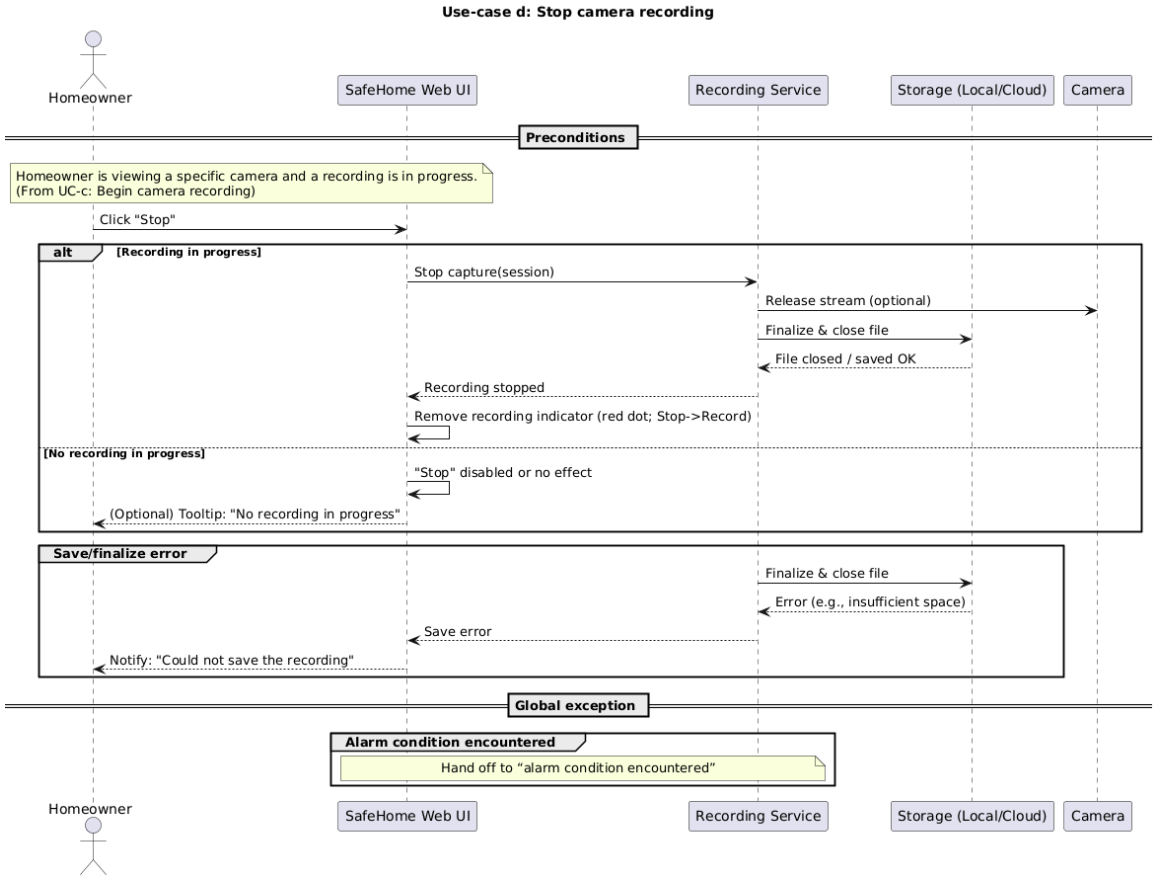

Figure 36. Stop camera recording Sequence Diagram

e. Replay camera recording

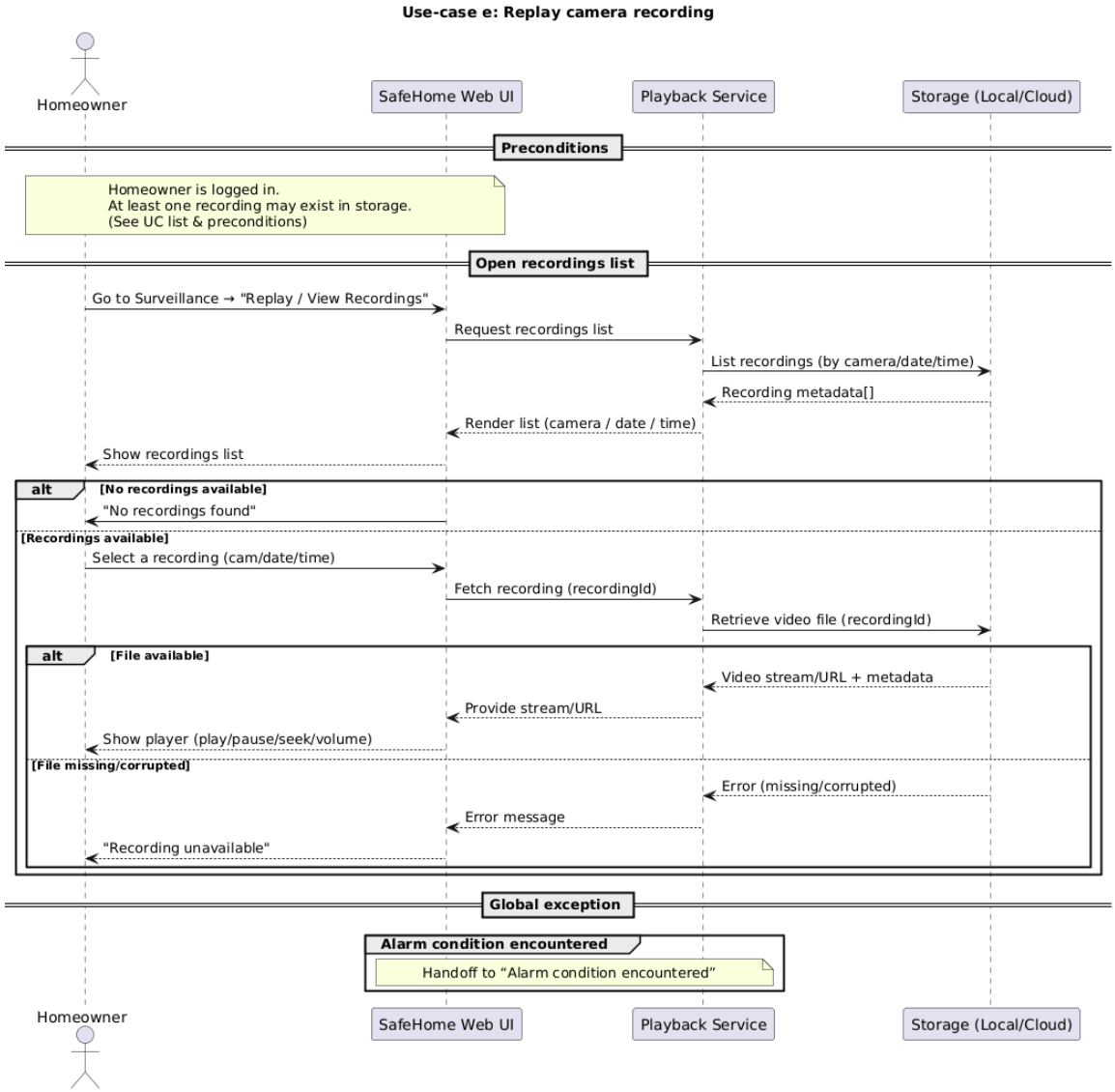

Figure 37. Replay camera recording Sequence Diagram

f. Set camera password

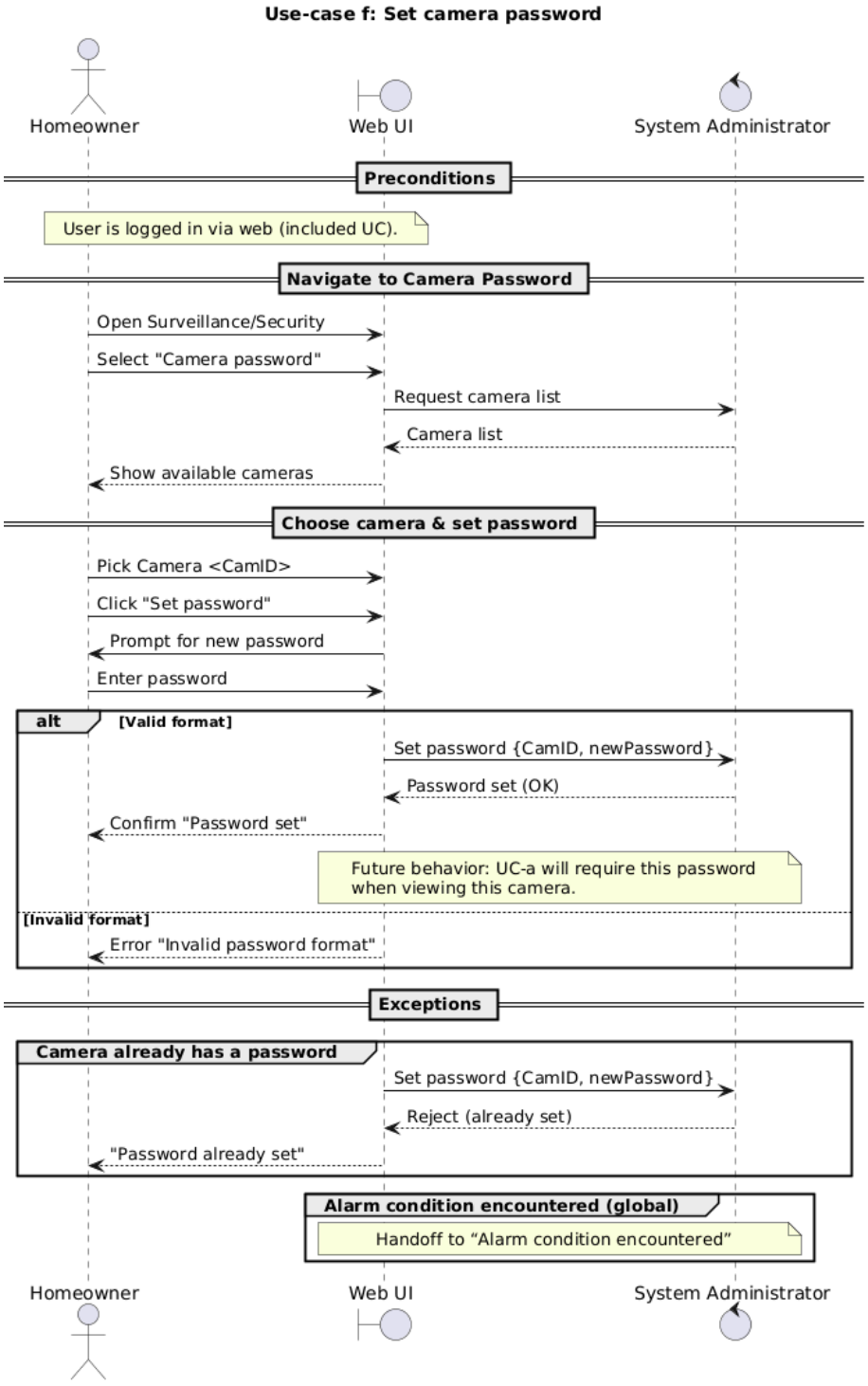

Figure 38. Set camera password Sequence Diagram

g. Delete camera password

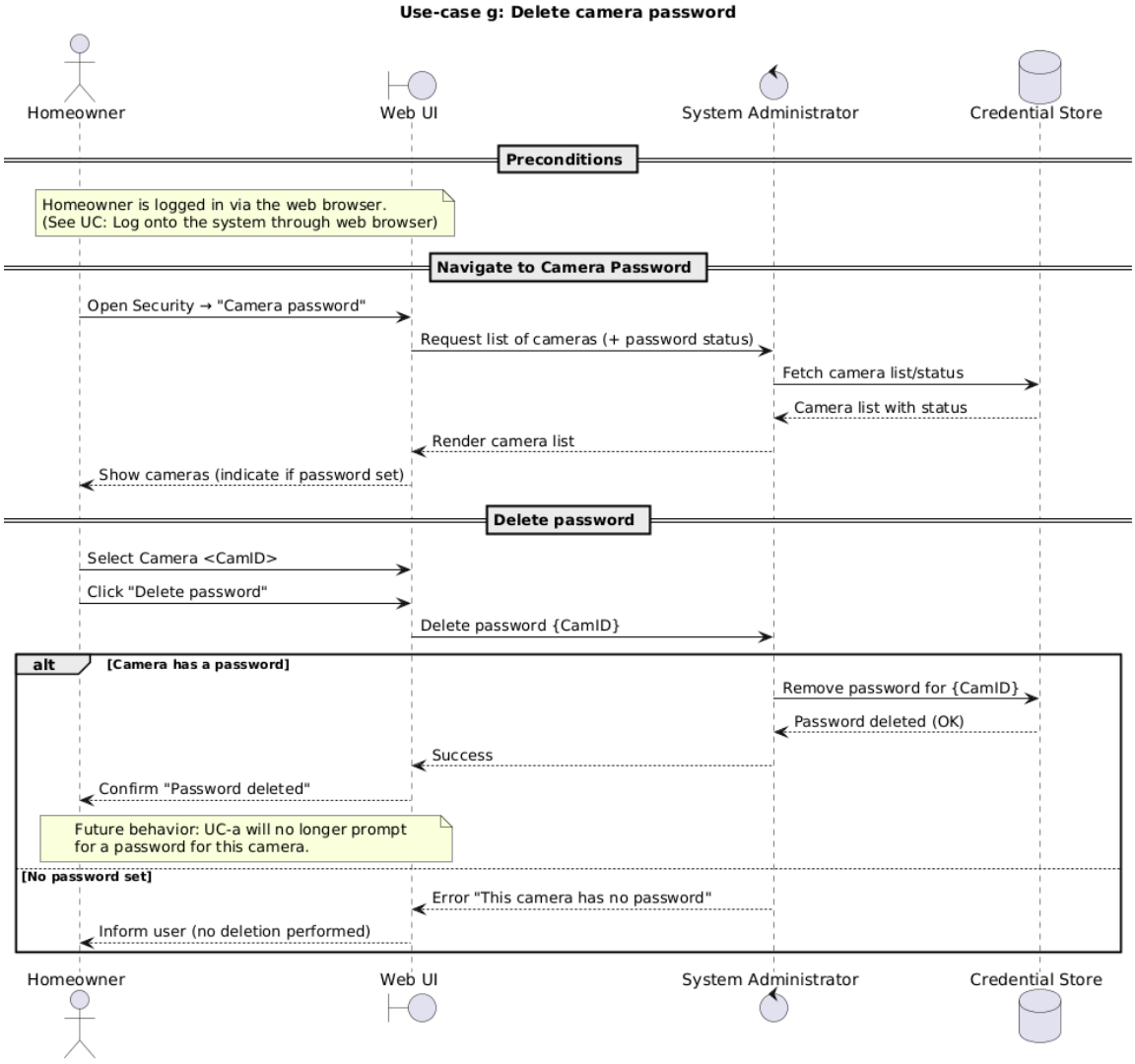

Figure 39. Delete camera password Sequence Diagram

h. View thumbnail Shots

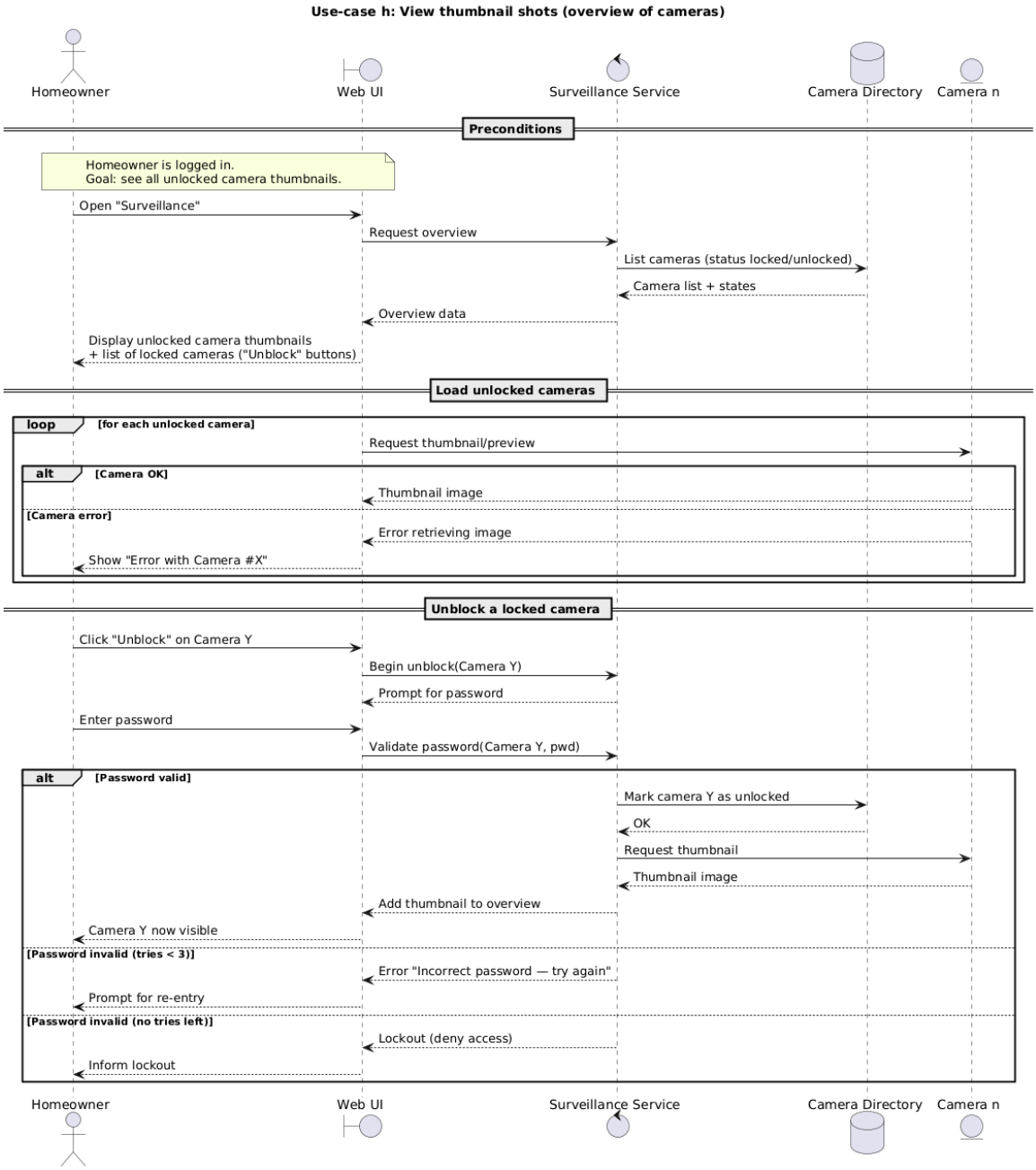

Figure 40. View thumbnail Shots Sequence Diagram

i. Enable camera

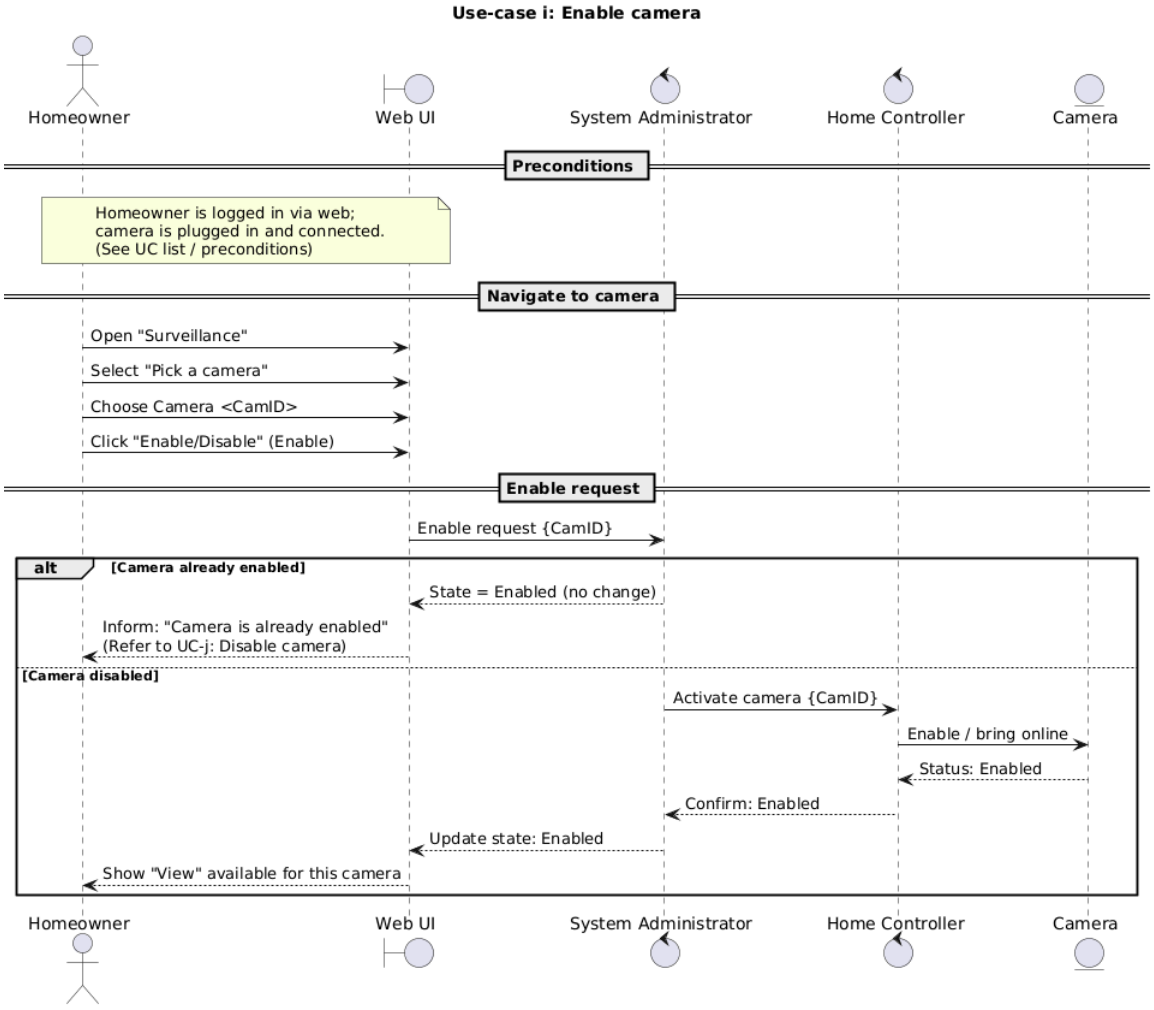

Figure 41. Enable camera Sequence Diagram

j. Disable camera

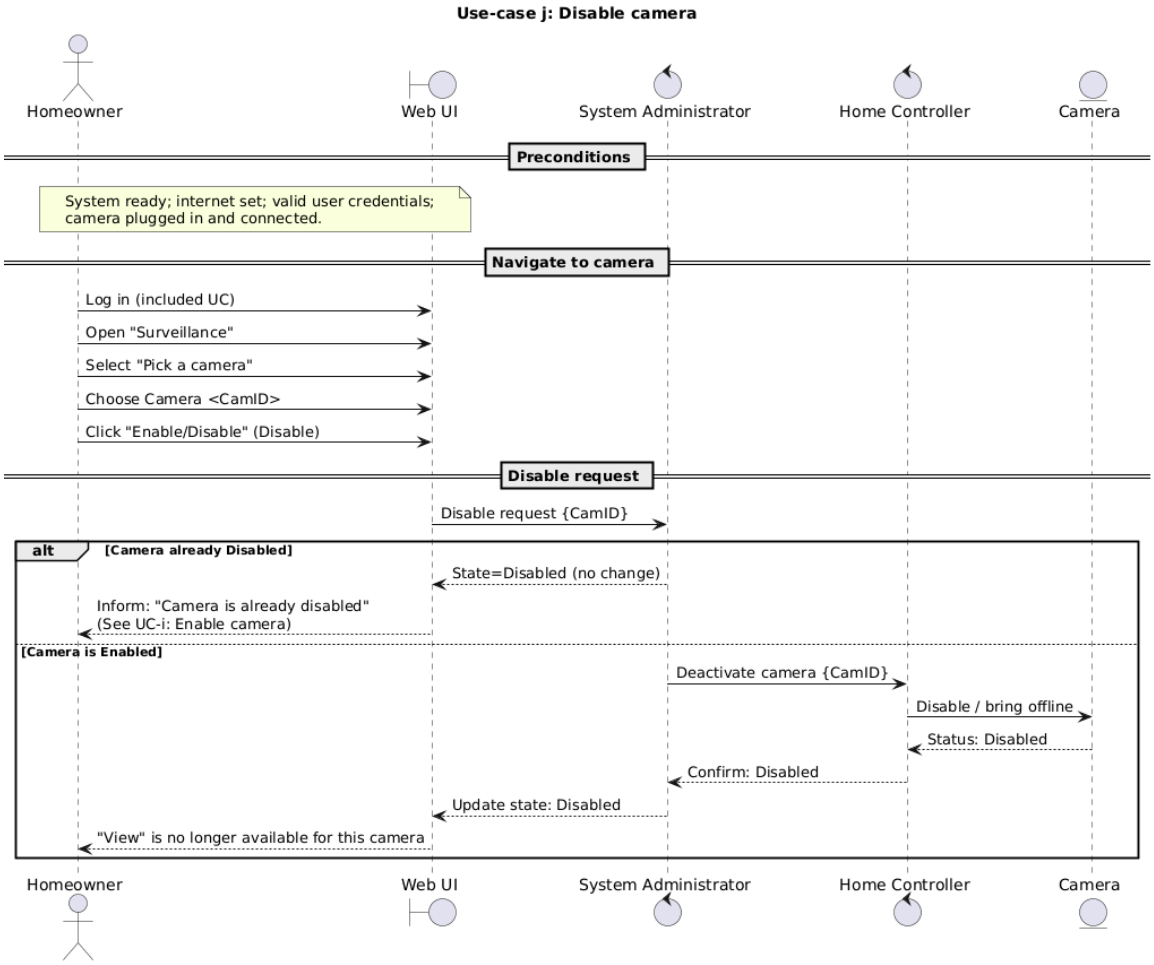

Figure 42. Enable camera Sequence Diagram

VIII. Who did what

Jamal Alibalayev
Common Use Cases b. Log onto the system through web browser 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

Security Use Cases

b. Arm/disarm system through web browser

c. Arm/disarm safety zone selectively

Work on the consistency of team's written use cases

Glossary

Meeting logs

Edit of Assumptions

Yonas Alexander Grossard Amin

Surveillance Use Cases

f. Set camera password

g. Delete camera password

h. View thumbnail Shots

i. Enable camera

j. Disable camera

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

Section about future features

Alan Pak To Cheung

Surveillance Use Cases

a. Display Specific camera view

b. Pan/Zoom specific camera view

c. Begin camera recording

d. Stop camera recording

e. Replay camera recording

Common Sequence Diagram

a. Log onto the system through control panel

b. Log onto the system through web browser

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

Use Case Diagram

Security Functions

Configure Safety Zone Functions

Surveillance Functions

Jongyoon Baek

Use Cases

d. Alarm condition encountered

e. Configure safety zone

f. Create new safety zone

g. Delete safety zone

h. Update an exist safety zone

i. Configure Safehome modes

j. View intrusion log

k. Call monitoring service through control panel

l. Manage User Accounts and Permissions

m. Send Security Alert to Homeowner

n. View System Activity Log

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. Alarm condition encountered

e. Configure safety zone

f. Create new safety zone

g. Delete safety zone

h. Update an exist safety zone

i. Configure Safehome modes

j. View intrusion log

k. Call monitoring service through control panel

l. Manage User Accounts and Permissions

m. Send Security Alert to Homeowner

n. View System Activity Log

o. Add Intrusion Log

IX. Meeting logs

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

Meeting 1 — October 24, 2025, 3pm

Where:
Student lounge, Second floor, MirHall dormitory

Who (Participants):

- Jamal Alibalayev
- Yonas Alexander Grossard Amin
- Alan Pak To Cheung
- Jongyoon Baek

What:
The team divided responsibilities for creating **use case diagrams** for the SRS.

Why:
To ensure parallel progress and prepare for integrating the use cases in the next meeting.

How:
Tasks were distributed according to complexity and prior progress:

- **Jamal** — Use cases of *Common Functionalities* (since they're fewer and already diagrammed) + use cases *(a, b, c)* of *Security Functions*.
- **Jongyoon** — Remaining use cases of *Security Functions*.
- **Alan** — The first half of *Surveillance Functions* use cases.
- **Yonas** — The other half of *Surveillance Functions* use cases.

When:
All members complete their assigned parts **by the next meeting on October 27, 2025, 4pm**.

Summary of Outcome:
It was decided that at the next meeting the group would **link the individual use cases** and **eliminate inconsistencies** between them.

Meeting 2 — October 27, 2025, 4pm

Where:
Second floor, MirHall dormitory

Who (Participants):

- Jamal Alibalayev
- Yonas Alexander Grossard Amin
- Alan Pak To Cheung
- Jongyoon Baek

What:
Reviewed progress on use cases and reassigned new tasks focusing on **sequence diagrams** and consistency of the use cases.

Why:
Because project deadlines were approaching and the team needed to accelerate the work on the software requirement specification.

How:

- **Jamal** — Responsible for:
    - Writing *Glossary*
    - *Eliminating inconsistencies* in use cases
    - *Making meeting logs*
    - *Adding cross-references* to SRS
    - *Notifying team* about any changes to use cases
- **Alan, Jongyoon, Yonas** — need to do the main bulk of the software requirement specification. Each will design *10 sequence diagrams* and synchronously update them based on the changes on the use cases by Jamal side or reject his changes through communication
- **Jongyoon** suggested adding additional functionalities beyond the ones described in the template(Security use cases l, m, n, o).
- **Alan** additionally proposed to add scheduling functionality for the camera recordings.

- **Jamal** expressed concerns about the need to integrate these new functionalities in a consistent way to the project's documentation and the need to spend more time during the implementation.
- **Yonas** suggested to keep the additional features, and drop/add even more features in the future steps of the project depending on our schedules.
- Team agreed to Yonas;s suggestion.

When:

Assigned tasks need to be done until the next meeting on October 29, 2025, 10pm

Summary of Outcome:

The team acknowledged the time constraints and decided to proceed with parallel work: Jamal handling consistency and cross reference, while others produce the main bulk of the remaining work with the sequence diagrams.

Appendix A. Glossary

1. Control panel: a small gadget to display basic information and receive your commands
   See Fig. 1 in page 6, use case “Log onto the system through control panel” in page 11, and …
2. Exit delay time - The period after arming the system during which the alarm doesn’t yet monitor sensors — giving the homeowner time to leave and close doors. If the exit delay is 60 s, you can arm the system, leave the house, and close the door before the system starts detecting motion.
3. Exit delay time - The period after arming the system during which the alarm doesn’t yet monitor sensors — giving the homeowner time to leave and close doors. If the exit delay is 60 s, you can arm the system, leave the house, and close the door before the system starts detecting motion.
4. “Turn the system on” and “Turn the system off” is **powering on/off the SafeHome system administrator** — cameras, sensors, communication modules, etc.
   See use cases “Turn the system on” and “Turn the system off”
5. “Arm/disarm system through control panel” and “Arm/disarm system through web browser” - The system is **already powered ON**, but you tell it whether to **start or stop monitoring** sensors for intrusions.
   See use cases “Arm/disarm system through control panel” and “Arm/disarm system through web browser”
6. **System Administrator:** Represents the SafeHome system acting internally to manage functions (not a human).
   1. See Assumptions section for clarification.
7. **Homeowner:** The primary user of the SafeHome system with full administrative privileges, including configuring system settings, managing safety zones, and changing passwords. The homeowner can access the system through both the control panel and the web interface.
8. **Guest:**
   A limited-access user of the SafeHome system who can log onto the system only through the control panel to enter the house. Guests cannot arm or disarm the system, configure settings.

Future additions:

This is a section for future improvements/additions we plan to add, but have not yet implemented, due to time constraint.

- Implement other account types, as for now we only have Master and Guest, we are planning on adding intermediary accounts, which the Master account can give more or less access to. (eg. Children account, where the children have the authorisation to disable/enable their room cameras)
  → This will also imply an extra verification in many use-cases, as we have to check if the user has authorization.