Software Requirement Specification

for

SAFE HOME

Version 0.1

Team 5
Sihun Chae (20190642)
Wooyoung Choi (20190659)
Donggeun Kim (20190074)

Revision History

Name	Date	Version	Reason for Changes
Phase I, Draft 1	2025-10-31	0.1	Initial SRS

Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose

The purpose of this Software Requirements Specification (SRS) document is to describe the functional and nonfunctional requirements of the **SafeHome System**—a smart home security and surveillance solution designed to help homeowners monitor and control their residential environments. This document defines the intended functions, performance goals, and operational constraints for both the hardware control panel and the web-based interface. It serves as a communication bridge among stakeholders, including customers, developers, testers, and project managers, ensuring that all parties share a common understanding of system capabilities and limitations.

1.2 Scope & Goals

The **SafeHome System** enables homeowners to remotely monitor their homes, configure security zones, and view real-time video from cameras or sensors through a unified interface. The scope of this project includes three major functional areas:

- **Security Functions** – Arm/disarm system, detect intrusion, and notify users of alarm events.
- **Surveillance Functions** – Provide real-time video streaming, playback, and camera configuration.
- **System Management** – Support user authentication, and device configuration.

Key project goals include:

- Develop a reliable and user-friendly home monitoring solution accessible from both physical and web interfaces.
- Provide configurable safety zones and single-user support.
- Deliver real-time alerts with high availability and data integrity.
- Ensure system security, scalability, and compliance with privacy standards.

The system's boundary includes the control panel, sensors, cameras, and the SafeHome web application. External systems such as third-party cloud services or mobile notification servers are assumed to be integrated but maintained outside of SafeHome's direct control.

2 Overall Description

2.1 Product Perspective

The **SafeHome System** is a distributed smart home solution composed of hardware devices and a centralized software platform. The system integrates motion sensors, cameras, and a control panel with an intelligent web application that allows homeowners to monitor and control their home environment from any location.

SafeHome replaces manual home security practices with an automated, connected environment. It serves as a part of a larger Internet of Things (IoT) ecosystem but is designed to operate independently from other smart devices.

System Boundary:

- **Inside the System:** Control panel, sensors, cameras, communication module, database server, and SafeHome web application.
- **Outside the System:** External cloud storage, third-party notification servers, and mobile SMS gateways.

External Interfaces:

- **User Interface:** Touchscreen panel and responsive web interface.
- **Hardware Interface:** Sensor and camera connections through standard I/O or wireless modules.
- **Network Interface:** Wi-Fi or Ethernet communication for control and alerts.

2.2 Major Functionalities

SafeHome provides integrated security, surveillance, and system management features.

1. **Security Monitoring** – Users can arm or disarm the system, define safety zones, and receive instant alerts when intrusion or abnormal events occur.
2. **Surveillance Management** – Supports real-time video monitoring, recording, and playback through both web and panel interfaces.
3. **User Control & Notifications** – Provides authenticated access, user configuration, and instant notifications via web and mobile interfaces.

Each functionality contributes to improving the safety, convenience, and control of the home environment.

2.3 User and Stakeholder Classes & Characteristics

The system is designed for several classes of users, each with specific roles and privileges:

- **Homeowner**
  1. Operates the system daily via control panel or web interface.
  2. Can arm/disarm the system, monitor live feeds, and manage notifications.
  3. Requires minimal technical knowledge.
- **Administrator**
  1. Configures the system, manages user accounts, updates settings.
  2. Requires intermediate technical knowledge.

2.4 Assumptions

2.4.1 Common

- We ensure that the SafeHome system has an active Internet connection; any malfunction of SafeHome features due to network disconnection is outside our scope.
- We assumed that web pages for visually impaired users are out of scope.
- System Administrator accounts exist and can perform all homeowner functions. Separate admin use cases are not modeled.
- E-commerce (product purchase, subscription renewal, etc.) via SafeHome web is not considered.
- Mobile access to SafeHome features is out of scope. Only desktop web and control panel interfaces are supported.
- We assumed that if credential authentication fails, the user can contact the SafeHome administrator to log in.
- Hardware deployment is complete and out of the scope of our project.
- Credential management (creation, recovery) is handled outside this increment; if authentication fails, the user must contact the administrator to regain access.
- SafeHome assumes that user passwords and two-factor credentials are managed securely by users; any breach due to password exposure is outside project responsibility.
- "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.

2.4.2 Security

- All physical sensors (door, window, motion, smoke detectors) and control hardware have been installed, tested, and verified before this software increment.
- The floor plan and sensor mapping (location and type of each sensor) are already configured in the SafeHome database; users cannot modify these in the current increment.
- SafeHome security features comply with corporate data protection and user privacy policies, but legal enforcement mechanisms (e.g., third-party liability) are not handled by this increment.
- Any sensor hardware malfunction (e.g., physical damage or battery depletion) is treated as an exceptional condition and not addressed by this software increment.
- SafeHome assumes sufficient power backup (UPS) for control panels and sensors; loss of electrical power is considered a physical infrastructure issue, not a system defect.
- The monitoring service infrastructure (call center, emergency dispatch) is pre-established and tested; SafeHome software only initiates the call and transmits event data.
- All communication between system components (control panel, sensors, admin console) uses a secure internal wireless network compliant with company standards.
- Network disconnections or packet loss between control panel and sensors are treated as exceptional events; automated recovery or redundancy is not included in this increment.
- The SafeHome server and database infrastructure are maintained by corporate IT; this increment does not include database schema migration or server-side deployment automation.

2.4.3 Surveillance

- Camera hardware installation and network configuration are completed prior to the operation of the system.
- Each camera is uniquely registered in the SafeHome system with an ID, status and optional password.
- All camera communications use wireless connectivity, and streaming bandwidth is assumed to be sufficient for at least 1 frame per second.
- Network disconnections or device malfunctions are treated as exceptional events and not handled in the first increment.

3 Prototype GUI

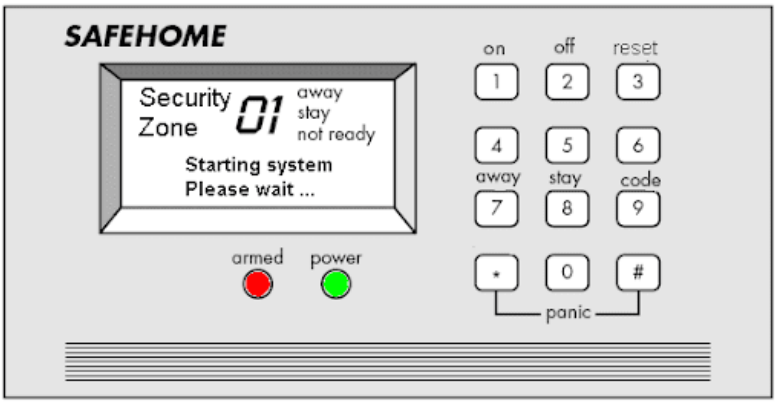

Figure 3.1: Control Panel

Figure 3.2: Login Screen

Figure 3.3: Main Functions

Figure 3.4: Security Function - Safety Zone

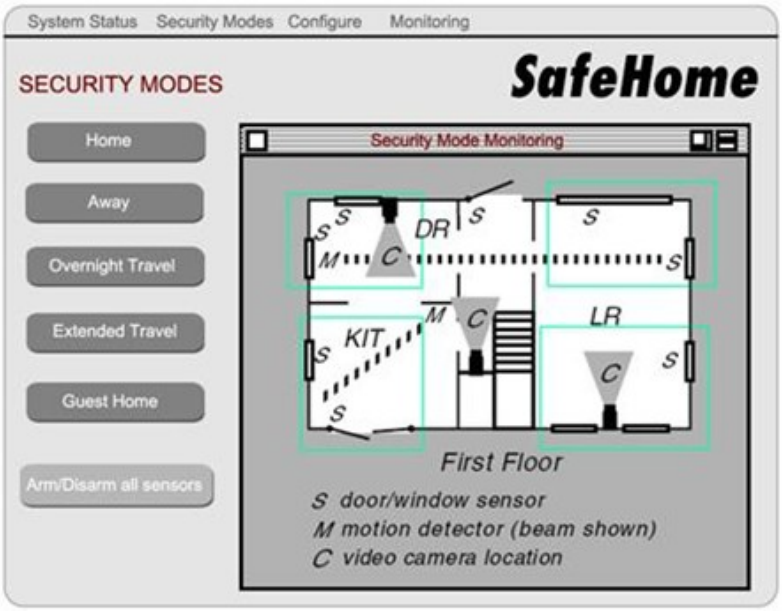

Figure 3.5: Security Function - Security Mode

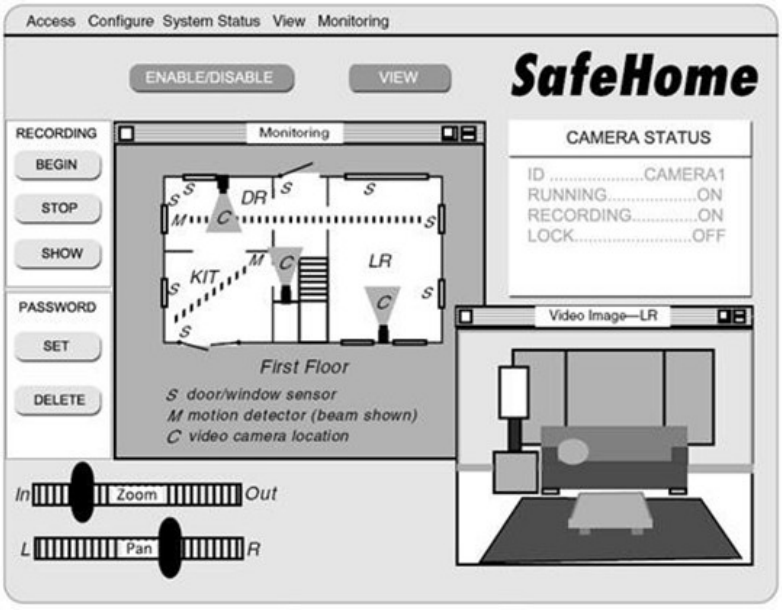

Figure 3.6: Surveillance Function

4 Functional Requirements

4.1 Overview

This chapter lists all functional requirements derived from the use cases in Chapters 6.1 and 10. Each FR is uniquely identified (e.g., FR-1) and described with its statement, rationale, verification method, category, and source use cases.

4.2 Functional Requirements

Table 4.1: Functional Requirement — FR-1

Requirement ID	FR-1
Statement	System shall authenticate users via the control panel before granting access to any protected function.
Rationale	Prevents unauthorized physical access to system controls.
Verification	Test with valid/invalid passwords; verify lockout after N failed attempts.
Category	Authentication
Source Use Cases	UC1
Priority	High

Table 4.2: Functional Requirement — FR-2

Requirement ID	FR-2
Statement	System shall authenticate users via the web interface and display the dashboard upon success.
Rationale	Prevents unauthorized remote access.
Verification	Attempt login with valid/invalid credentials and (if enabled) 2FA; verify redirect.
Category	Authentication
Source Use Cases	UC2
Priority	High

Table 4.3: Functional Requirement — FR-3

Requirement ID	FR-3
Statement	System shall arm and disarm the security system via the control panel.
Rationale	Allows local control of security state.

Verification	Change state on panel; verify controller state and indicator synchronization.
Category	Security Management
Source Use Cases	UC8
Priority	High

Table 4.4: Functional Requirement — FR-4

Requirement ID	FR-4
Statement	System shall arm and disarm the security system via the web interface.
Rationale	Allows remote control of security state.
Verification	Change state on web; verify controller confirmation and UI consistency.
Category	Security Management
Source Use Cases	UC9
Priority	High

Table 4.5: Functional Requirement — FR-5

Requirement ID	FR-5
Statement	System shall allow selective arming and disarming of configured safety zones.
Rationale	Supports partial security coverage per user needs.
Verification	Toggle target zones; verify active sensors, bypass handling, and audit trail.
Category	Security Management
Source Use Cases	UC10
Priority	High

Table 4.6: Functional Requirement — FR-6

Requirement ID	FR-6
Statement	System shall trigger an alarm when an intrusion event meets configured thresholds.
Rationale	Ensures timely detection and response to threats.
Verification	Simulate sensor events across thresholds; verify alarm, logging, and notifications.
Category	Security Events
Source Use Cases	UC11
Priority	High

Table 4.7: Functional Requirement — FR-7

Requirement ID	FR-7

Statement	System shall display a chronological intrusion log with timestamps and zones.
Rationale	Enables incident review and auditability.
Verification	Create events; verify listing, filtering, and export options.
Category	Security Audit
Source Use Cases	UC17
Priority	Medium

Table 4.8: Functional Requirement — FR-8

Requirement ID	FR-8
Statement	System shall notify the external monitoring service according to escalation policy during an active alarm.
Rationale	Supports professional response escalation.
Verification	Emulate alarm; verify payload delivery, ack/retry behavior, and status recording.
Category	Integration
Source Use Cases	UC18
Priority	High

Table 4.9: Functional Requirement — FR-9

Requirement ID	FR-9
Statement	System shall display a real-time live view for a selected registered camera.
Rationale	Provides situational awareness.
Verification	Open camera view; verify FPS ≥ 1, password prompt (if protected), and offline handling.
Category	Surveillance
Source Use Cases	UC19
Priority	High

Table 4.10: Functional Requirement — FR-10

Requirement ID	FR-10
Statement	System shall start recording for a selected camera when requested by an authorized user.
Rationale	Supports evidence capture.
Verification	Start recording; verify storage quota check, recording indicator, and clip creation.
Category	Surveillance
Source Use Cases	UC21
Priority	High

Table 4.11: Functional Requirement — FR-11

Requirement ID	FR-11
Statement	System shall stop an ongoing recording and safely finalize the video clip.
Rationale	Prevents data loss and ensures clip integrity.
Verification	Stop recording; verify finalized clip, metadata, and list update.
Category	Surveillance
Source Use Cases	UC22
Priority	High

Table 4.12: Functional Requirement — FR-12

Requirement ID	FR-12
Statement	System shall replay a stored recording with basic transport controls.
Rationale	Supports incident review.
Verification	Select clip; verify playback, seek, and error on unsupported codec.
Category	Surveillance
Source Use Cases	UC23
Priority	Medium

Table 4.13: Functional Requirement — FR-13

Requirement ID	FR-13
Statement	System shall configure operational modes (e.g., Home, Away, Vacation) and apply associated policies.
Rationale	Simplifies consistent behavior across contexts.
Verification	Change mode; verify policy effects, schedule conflicts, and UI/controller sync.
Category	Configuration
Source Use Cases	UC16
Priority	High

Table 4.14: Functional Requirement — FR-14

Requirement ID	FR-14
Statement	System shall allow creation and configuration of safety zones, including thresholds and sensor assignments.
Rationale	Enables tailored security coverage.
Verification	Create/update zone; verify validation, persistence, and audit logs.
Category	Configuration
Source Use Cases	UC12

Priority	Medium

5 Non-Functional Requirements

5.1 Overview

This chapter defines system-wide quality attributes and constraints that complement the functional requirements. Each NFR is uniquely identified (NFR-1, NFR-2, ...) and specifies: *Statement*, *Rationale*, and *Measurement/Verification (MoV)*.

5.2 Non-Functional Requirements

Table 5.1: Non-Functional Requirement — NFR-1

Requirement ID	NFR-1
Statement	All communications between client, controller, sensors, and cameras shall be encrypted via TLS or equivalent secure channels.
Rationale	Protect confidentiality and integrity of data in transit.
MoV	Traffic inspection for TLS versions/ciphers; penetration tests; config audit.
Category	Security/Privacy
Priority	High

Table 5.2: Non-Functional Requirement — NFR-2

Requirement ID	NFR-2
Statement	Sensitive data at rest (e.g., credentials, keys, personal info) shall be protected via encryption or compensating controls (e.g., HSM/OS hardening).
Rationale	Reduce risk of data exposure on storage compromise.
MoV	Key management review; at-rest encryption checks; file-system and DB policy audits.
Category	Security/Privacy
Priority	High

Table 5.3: Non-Functional Requirement — NFR-3

Requirement ID	NFR-3
Statement	The service shall achieve availability of at least 99.5% during normal operation.
Rationale	Ensure continuous access for security-critical features.

MoV	SLA monitoring; monthly availability report; incident tracking and postmortems.
Category	Reliability/Availability
Priority	High

Table 5.4: Non-Functional Requirement — NFR-4

Requirement ID	NFR-4
Statement	On component failure (sensor/camera/controller), the system shall degrade gracefully without corrupting state or losing committed data.
Rationale	Maintain safety and data integrity during partial outages.
MoV	Fault-injection tests; recovery drills; verification of idempotent writes and rollbacks.
Category	Reliability
Priority	High

Table 5.5: Non-Functional Requirement — NFR-5

Requirement ID	NFR-5
Statement	Average user-facing response time shall be $\leq$ 2 seconds for typical flows with 10 concurrent users.
Rationale	Maintain responsive interactions for common operations.
MoV	Load tests with p50/p95 latency metrics; acceptance threshold per scenario.
Category	Performance
Priority	Medium

Table 5.6: Non-Functional Requirement — NFR-6

Requirement ID	NFR-6
Statement	The system shall scale to 50 concurrent users while keeping p95 response time $\leq$ 3 seconds for common actions.
Rationale	Support growth without major redesign.
MoV	Scalability tests with step-load; resource utilization and latency SLO checks.
Category	Performance/Scalability
Priority	Medium

Table 5.7: Non-Functional Requirement — NFR-7

Requirement ID	NFR-7
Statement	The web interface shall follow applicable accessibility guidelines for in-scope features (e.g., keyboard navigation, labels, contrast).

Rationale	Improve usability and reduce user errors.
MoV	Accessibility audit checklist; heuristic evaluation; sample user testing.
Category	Usability/Accessibility
Priority	Medium

Table 5.8: Non-Functional Requirement — NFR-8

Requirement ID	NFR-8
Statement	Components shall be modular and documented to enable mean time to repair (MTTR) $\leq$ 2 hours for standard, documented faults.
Rationale	Reduce downtime and maintenance effort.
MoV	Ops playbooks; repair drills; measure time-to-recover across fault catalog.
Category	Maintainability/Modularity
Priority	Medium

Table 5.9: Non-Functional Requirement — NFR-9

Requirement ID	NFR-9
Statement	The system shall interoperate with third-party devices using open protocols (e.g., RTSP for video, MQTT/ONVIF for telemetry/control).
Rationale	Avoid vendor lock-in and ease integration.
MoV	Integration tests with reference devices; protocol compliance checks.
Category	Interoperability/Compliance
Priority	Medium

Table 5.10: Non-Functional Requirement — NFR-10

Requirement ID	NFR-10
Statement	The system shall expose structured logs, metrics, and (where feasible) traces sufficient for automated monitoring and alerting.
Rationale	Enable observability, incident detection, and continuous validation.
MoV	Log schema validation; metrics scraping; synthetic alert tests for critical paths.
Category	Testability/Monitoring
Priority	High

Table 5.11: Non-Functional Requirement — NFR-11

Requirement ID	NFR-11

Statement	Configuration and event data shall be backed up and restorable within documented RTO/RPO targets.
Rationale	Support business continuity and forensic analysis.
MoV	Backup job verification; periodic restore drills; RTO/RPO evidence.
Category	Reliability/Continuity
Priority	High

Table 5.12: Non-Functional Requirement — NFR-12

Requirement ID	NFR-12
Statement	Authentication controls shall enforce lockout/throttling for repeated failed attempts and provide audit trails.
Rationale	Mitigate brute-force and credential-stuffing risks.
MoV	Security tests for rate limits; lockout policy verification; audit-log review.
Category	Security
Priority	High

6 Use Case Model

6.1 Overview

The **Use Case Model** describes the primary interactions between external actors and the SafeHome system. It provides a high-level view of how users (homeowners and administrators) utilize SafeHome to perform various security, surveillance, and configuration operations.

Each use case represents a distinct system function triggered by an actor, describing the system's response and outcome. These use cases form the foundation for defining detailed scenarios and deriving functional requirements.

6.2 Use Case Diagrams

The following diagrams illustrate SafeHome's functional categories: common use case interaction, security-related operations, and surveillance capabilities.

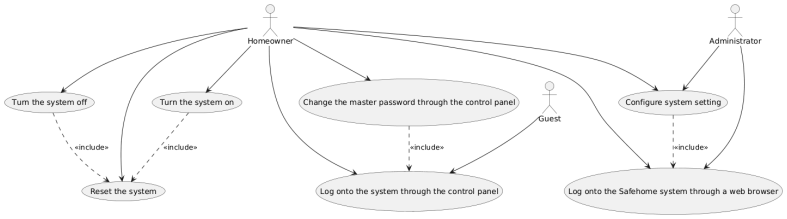

Figure 6.1: Common Use Case Diagram

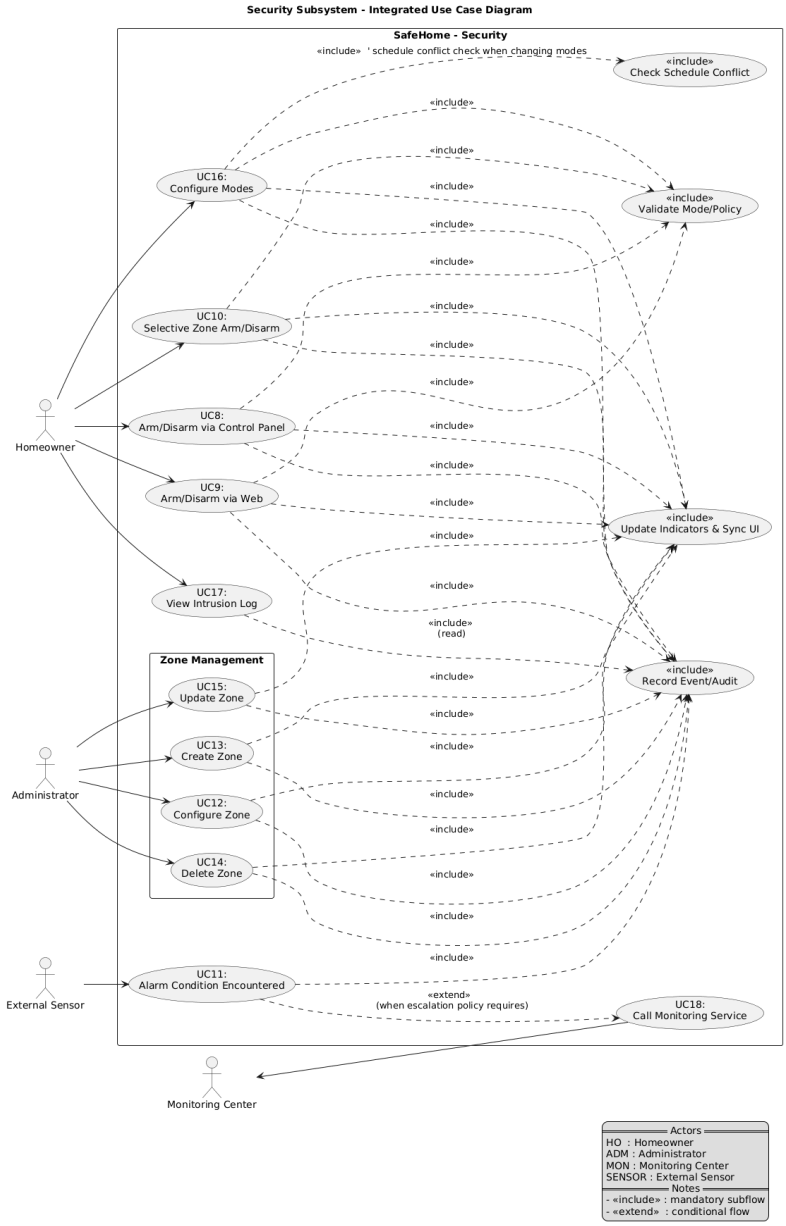

Figure 6.2: Security Use Case Diagram

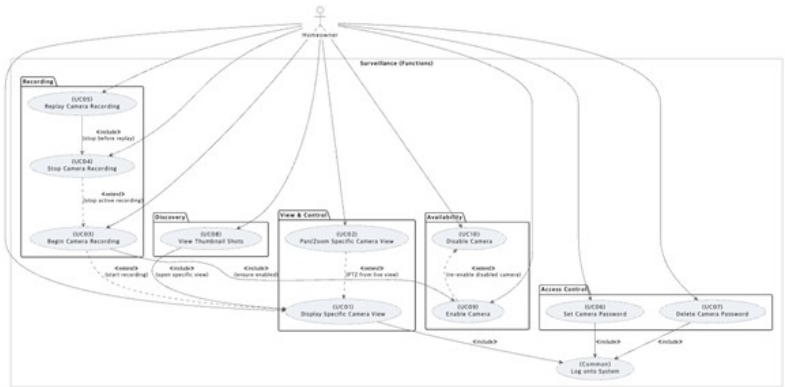

Figure 6.3: Surveillance Use Case Diagram

6.3 Use Case List

Table 6.1 summarizes all identified use cases. Each ID and name is clickable and links to the detailed scenario in Chapter 6.

Table 6.1: SafeHome Use Case Summary

ID	Name	Description	Primary Actor
Common Use Cases			
UC1	Log onto the system through control panel	Authenticate via control panel to access features.	Homeowner
UC2	Log onto the system through web browser	Authenticate via web UI to access features.	Homeowner
UC3	Configure system setting	Modify system preferences and environment parameters.	Administrator
UC4	Turn the system on	Activate system operation mode.	Homeowner
UC5	Turn the system off	Deactivate system and suspend monitoring.	Homeowner
UC6	Reset the system	Restart to restore a stable operational state.	Homeowner
UC7	Change master password through control panel	Update master password securely on panel.	Homeowner
Security Use Cases			
UC8	Arm/disarm system through control panel	Enable/disable alarm monitoring via panel.	Homeowner
UC9	Arm/disarm system through web browser	Enable/disable alarm monitoring via web UI.	Homeowner
UC10	Arm/disarm safety zone selectively	Activate only selected zones.	Homeowner
UC11	Alarm condition encountered	System detects intrusion and triggers alarm.	System
UC12	Configure safety zone	Define parameters and thresholds for a zone.	Administrator
UC13	Create new safety zone	Add a new zone and assign sensors.	Administrator
UC14	Delete safety zone	Remove an existing zone.	Administrator
UC15	Update an existing safety zone	Modify zone configuration and sensors.	Administrator
UC16	Configure SafeHome modes	Define/modify modes (Home/-Away/etc.).	Homeowner
UC17	View intrusion log	Display historical alarm events.	Homeowner
UC18	Call monitoring service through control panel	Contact external monitoring center on emergency.	System
Surveillance Use Cases			
UC19	Display specific camera view	Show live feed from a selected camera.	Homeowner

ID	Name	Description	Primary Actor
UC20	Pan/Zoom specific camera view	Adjust camera orientation or zoom.	Homeowner
UC21	Begin camera recording	Start recording from a camera feed.	Homeowner
UC22	Stop camera recording	Stop recording and finalize clip.	Homeowner
UC23	Replay camera recording	Playback previously stored video.	Homeowner
UC24	Set camera password	Protect a camera with a password.	Administrator
UC25	Delete camera password	Remove camera password.	Administrator
UC26	View thumbnail shots	Show thumbnails for all cameras.	Homeowner
UC27	Enable camera	Activate a disabled camera.	Administrator
UC28	Disable camera	Temporarily deactivate a camera.	Administrator

7 Detailed Use Cases

7.1 Overview

This chapter presents detailed, actor-oriented scenarios for each use case. Each entry is auto-numbered in order of appearance (UC1, UC2, ...) and labeled as `uc:<slug>` for cross-references from Chapter 5 and elsewhere. All use cases share the same structure: **Preconditions**, **Trigger**, **Main Scenario**, **Alternate Flows**, and **Postconditions**.

7.2 Common Use Cases

Table 7.1: Use Case — UC1: Log onto the system through control panel

Use Case ID	UC1
Name	Log onto the system through control panel
Priority	High
Actors	Homeowner
Preconditions	System configured and powered; control panel reachable; user has valid password
Trigger	User selects “Login” on the control panel
Main Scenario	1. System prompts for master/guest password. 2. User enters a valid 4-digit password. 3. System validates credentials against local store. 4. System displays the main menu with permitted functions.
Alternate Flows	2a. Invalid password: show error; allow retry; lock out after 3 failures (policy).
Postconditions	User authenticated on panel; permitted menu visible

Table 7.2: Use Case — UC2: Log onto the system through web browser

Use Case ID	UC2
Name	Log onto the system through web browser
Priority	High
Actors	Homeowner
Preconditions	System operational; web server reachable; user has valid credentials; network available

Trigger	User opens the SafeHome website and chooses “Login”
Main Scenario	1. System serves the login page. 2. User submits username and password. 3. System validates credentials against user database. 4. (Optional) System requests one-time verification (2FA) if enabled. 5. System redirects the user to the dashboard.
Alternate Flows	3a. Invalid credentials: show error; throttle after repeated failures. 4a. Invalid or expired code: allow resend; lock out after 3 failures. 1a. Web unreachable: show outage page; advise contacting administrator.
Postconditions	User authenticated on web; dashboard visible

Table 7.3: Use Case — UC3: Configure system setting

Use Case ID	UC3
Name	Configure system setting
Priority	High
Actors	Administrator
Preconditions	Admin authenticated; configuration privileges granted
Trigger	Admin opens “Settings/Configuration”
Main Scenario	1. System loads configurable parameters (time zone, notifications, policies). 2. Admin edits fields and selects *Save*. 3. System validates inputs and applies changes. 4. System confirms update and logs the event.
Alternate Flows	3a. Invalid value: highlight field; show validation message; keep previous value.
Postconditions	Settings stored

Table 7.4: Use Case — UC4: Turn the system on

Use Case ID	UC4
Name	Turn the system on
Priority	Medium
Actors	Homeowner
Preconditions	System installed; power available; user authenticated or physical access granted

Trigger	User selects “Power On / Start”
Main Scenario	1. System performs startup checks (sensors, network). 2. System initializes services and sets status to *Ready*.
Alternate Flows	1a. Critical check failed: show error.
Postconditions	System in operational state; ready for arming or monitoring

Table 7.5: Use Case — UC5: Turn the system off

Use Case ID	UC5
Name	Turn the system off
Priority	Medium
Actors	Homeowner
Preconditions	User authenticated on panel or web; system in operational state
Trigger	User selects “Power Off / Stop”
Main Scenario	1. System gracefully stops services. 2. System sets status to *Stopped* and logs action.
Alternate Flows	1a. Pending alarm: require confirmation; notify user about consequences.
Postconditions	System safely stopped; no active monitoring

Table 7.6: Use Case — UC6: Reset the system

Use Case ID	UC6
Name	Reset the system
Priority	Medium
Actors	Homeowner
Preconditions	System responsive; user has access to reset command
Trigger	User selects “Reset / Reboot”
Main Scenario	1. System confirms intent and schedules reboot. 2. System restarts and reloads last known configuration.
Alternate Flows	1a. Critical update in progress: defer reset; show warning.
Postconditions	System rebooted; services restored to normal

Table 7.7: Use Case — UC7: Change master password through control panel

Use Case ID	UC7
Name	Change master password through control panel
Priority	High
Actors	Homeowner
Preconditions	User authenticated as master; control panel available
Trigger	User selects “Change Master Password”
Main Scenario	1. System prompts for current password, then new password twice. 2. System validates complexity and confirms change. 3. System updates secure store and logs the event.
Alternate Flows	1a. Current password incorrect: show error; allow retry.
Postconditions	Master password updated; subsequent logins require new password

7.3 Security Use Cases

Table 7.8: Use Case — UC8: Arm/disarm system through control panel

Use Case ID	UC8
Name	Arm/disarm system through control panel
Priority	High
Actors	Homeowner
Preconditions	User authenticated on panel; sensors healthy per last self-test
Trigger	User presses Arm/Disarm on the panel
Main Scenario	1. System validates mode change (e.g., Home/Away). 2. System activates/deactivates sensors accordingly. 3. Panel indicators update to Armed/Disarmed.
Alternate Flows	2a. Sensor fault: notify user; allow arm with bypass if policy permits.
Postconditions	House status updated; indicators and logs synchronized

Table 7.9: Use Case — UC9: Arm/disarm system through web browser

Use Case ID	UC9
Name	Arm/disarm system through web browser
Priority	High
Actors	Homeowner
Preconditions	User authenticated on web; network connectivity available
Trigger	User selects Arm/Disarm on the dashboard

Main Scenario	1. System sends mode change to controller. 2. Controller applies mode and confirms. 3. Web UI reflects Armed/Disarmed status.
Alternate Flows	1a. Controller unreachable: show error; allow retry.
Postconditions	Requested mode applied; UI state consistent

Table 7.10: Use Case — UC10: Arm/disarm safety zone selectively

Use Case ID	UC10
Name	Arm/disarm safety zone selectively
Priority	High
Actors	Homeowner
Preconditions	User authenticated; zones configured and visible
Trigger	User selects zones and chooses Arm/Disarm
Main Scenario	1. System displays all zones with status. 2. User toggles specific zones. 3. System applies zone arming policy and confirms.
Alternate Flows	3a. Zone contains faulty sensor: offer bypass; log condition.
Postconditions	Selected zones armed or disarmed; audit trail recorded

Table 7.11: Use Case — UC11: Alarm condition encountered

Use Case ID	UC11
Name	Alarm condition encountered
Priority	High
Actors	System
Preconditions	System armed; sensor reports intrusion or hazard
Trigger	Sensor event exceeds configured threshold
Main Scenario	1. System validates event and triggers alarm. 2. System records event, time, and zone. 3. System notifies user(s) and (optionally) monitoring service.
Alternate Flows	1a. False positive suspected: apply debounce or secondary check.
Postconditions	Alarm active; downstream actions initiated per policy

Table 7.12: Use Case — UC12: Configure safety zone

Use Case ID	UC12
Name	Configure safety zone
Priority	Medium
Actors	Administrator
Preconditions	Admin authenticated; sensors registered
Trigger	Admin opens “Zones” and chooses a zone
Main Scenario	1. System shows zone parameters (name, sensors, thresholds). 2. Admin edits parameters and saves. 3. System validates and applies changes.
Alternate Flows	2a. Invalid threshold: show guidance; refuse save.
Postconditions	Zone configuration updated; change logged

Table 7.13: Use Case — UC13: Create new safety zone

Use Case ID	UC13
Name	Create new safety zone
Priority	Medium
Actors	Administrator
Preconditions	Admin authenticated; available sensors detected
Trigger	Admin selects “Create Zone”
Main Scenario	1. System prompts for zone name and assigns sensors. 2. Admin reviews and confirms. 3. System persists the new zone and refreshes the list.
Alternate Flows	1a. Duplicate name: suggest alternative; block creation.
Postconditions	New zone created; visible in configuration

Table 7.14: Use Case — UC14: Delete safety zone

Use Case ID	UC14
Name	Delete safety zone
Priority	Medium
Actors	Administrator
Preconditions	Admin authenticated; target zone exists; not locked by policy
Trigger	Admin selects “Delete Zone”

Main Scenario	1. System asks for confirmation. 2. Admin confirms deletion. 3. System removes zone and updates references.
Alternate Flows	3a. Zone in use (armed or recording): refuse; advise disarming first.
Postconditions	Zone removed; configuration consistent

Table 7.15: Use Case — UC15: Update an existing safety zone

Use Case ID	UC15
Name	Update an existing safety zone
Priority	Medium
Actors	Administrator
Preconditions	Admin authenticated; target zone exists
Trigger	Admin opens an existing zone for edit
Main Scenario	1. System loads current parameters and assigned sensors. 2. Admin modifies details (name, sensors, thresholds). 3. System validates and saves changes.
Alternate Flows	2a. Removing last critical sensor: warn and require override.
Postconditions	Zone updated; audit entry recorded

Table 7.16: Use Case — UC16: Configure SafeHome modes

Use Case ID	UC16
Name	Configure SafeHome modes
Priority	High
Actors	Homeowner
Preconditions	User authenticated; supported modes available (Home/Away/-Vacation)
Trigger	User opens “Modes” and changes selection
Main Scenario	1. System shows existing modes and rules. 2. User selects or edits a mode. 3. System applies mode policy and updates UI and controller.
Alternate Flows	2a. Mode conflicts with current schedule: show conflict; allow override.

Postconditions	Mode updated; status consistent across panel and web

Table 7.17: Use Case — UC17: View intrusion log

Use Case ID	UC17
Name	View intrusion log
Priority	Medium
Actors	Homeowner
Preconditions	User authenticated; historical events stored
Trigger	User opens “Intrusion Log”
Main Scenario	1. System loads events with timestamps and zones. 2. User filters or sorts entries. 3. User opens details for a specific event.
Alternate Flows	1a. No entries: show “No events recorded” message.
Postconditions	Events displayed; user can export or navigate to related actions

Table 7.18: Use Case — UC18: Call monitoring service through control panel

Use Case ID	UC18
Name	Call monitoring service through control panel
Priority	High
Actors	System
Preconditions	Alarm is active and policy requires escalation
Trigger	Escalation timer or user command triggers the call
Main Scenario	1. System dials or sends event payload to the monitoring center. 2. System awaits acknowledgment. 3. System records the transaction status.
Alternate Flows	2a. No acknowledgment: retry per backoff; log failure.
Postconditions	Monitoring center notified; status captured for audit

7.4 Surveillance Use Cases

Table 7.19: Use Case — UC19: Display specific camera view

Use Case ID	UC19
Name	Display specific camera view
Priority	High
Actors	Homeowner

Preconditions	Camera registered and reachable; user authorized; (optional) camera password known
Trigger	User selects a camera to view
Main Scenario	1. System shows camera list or floor plan. 2. User selects a target camera. 3. If password-protected, system prompts and validates. 4. Live view is displayed at frame rate ≥ 1 FPS.
Alternate Flows	3a. Wrong camera password: allow limited retries; then temporarily block. 4a. Camera offline: show placeholder and guidance.
Postconditions	Live view displayed; user may proceed to PTZ or recording

Table 7.20: Use Case — UC20: Pan/Zoom specific camera view

Use Case ID	UC20
Name	Pan/Zoom specific camera view
Priority	Medium
Actors	Homeowner
Preconditions	Camera supports PTZ; user has PTZ permission
Trigger	User opens PTZ controls
Main Scenario	1. System displays PTZ controls. 2. User sends pan/tilt/zoom commands. 3. System relays commands; camera updates view.
Alternate Flows	2a. Rate limit exceeded: throttle and notify.
Postconditions	View adjusted; PTZ actions logged

Table 7.21: Use Case — UC21: Begin camera recording

Use Case ID	UC21
Name	Begin camera recording
Priority	High
Actors	Homeowner
Preconditions	Camera reachable; storage available; user authorized
Trigger	User clicks “Record”
Main Scenario	1. System checks storage quota and policies. 2. Recording starts; indicator shows active capture.
Alternate Flows	1a. Insufficient storage: deny start; advise freeing space.

Postconditions	Recording in progress; metadata created

Table 7.22: Use Case — UC22: Stop camera recording

Use Case ID	UC22
Name	Stop camera recording
Priority	High
Actors	Homeowner
Preconditions	Recording currently in progress
Trigger	User clicks “Stop Recording”
Main Scenario	1. System finalizes the clip and writes metadata. 2. System updates recording list and indicator.
Alternate Flows	1a. I/O error: attempt recovery; mark clip as partial.
Postconditions	Recording safely stopped; clip available for replay

Table 7.23: Use Case — UC23: Replay camera recording

Use Case ID	UC23
Name	Replay camera recording
Priority	Medium
Actors	Homeowner
Preconditions	Existing recordings available; user authorized
Trigger	User selects “Recordings” and chooses a clip
Main Scenario	1. System lists recordings with time and camera info. 2. User selects a clip to play. 3. Player opens with transport controls.
Alternate Flows	3a. Unsupported codec: show error and fallback guidance.
Postconditions	Clip playback active; user may pause, seek, or export

Table 7.24: Use Case — UC24: Set camera password

Use Case ID	UC24
Name	Set camera password
Priority	Medium
Actors	Administrator
Preconditions	Admin authenticated; camera registered
Trigger	Admin chooses “Set Camera Password”

Main Scenario	1. System prompts for new password (twice) and policy checks. 2. System saves the password securely to camera/system. 3. System confirms and logs the change.
Alternate Flows	1a. Weak password: reject; show policy.
Postconditions	Camera password set; future access requires the new password

Table 7.25: Use Case — UC25: Delete camera password

Use Case ID	UC25
Name	Delete camera password
Priority	Medium
Actors	Administrator
Preconditions	Admin authenticated; camera currently password-protected
Trigger	Admin chooses “Delete Camera Password”
Main Scenario	1. System confirms intent and warns about security impact. 2. System removes password protection on the camera. 3. System confirms and logs the change.
Alternate Flows	2a. Policy forbids removal: refuse; require elevated approval.
Postconditions	Camera no longer requires a password; audit updated

Table 7.26: Use Case — UC26: View thumbnail shots

Use Case ID	UC26
Name	View thumbnail shots
Priority	Low
Actors	Homeowner
Preconditions	Cameras configured to produce thumbnails; user authorized
Trigger	User opens “Thumbnails”
Main Scenario	1. System displays thumbnails by camera/time. 2. User scrolls or filters the gallery. 3. User opens a thumbnail to jump to live or recording.
Alternate Flows	1a. No thumbnails available: show empty state with tips.
Postconditions	Thumbnails displayed; user can navigate to relevant views

Table 7.27: Use Case — UC27: Enable camera

Use Case ID	UC27
Name	Enable camera
Priority	Medium
Actors	Administrator
Preconditions	Camera registered but disabled; admin authenticated
Trigger	Admin selects “Enable Camera”
Main Scenario	1. System sends enable command to camera/controller. 2. Camera transitions to enabled state; system updates status.
Alternate Flows	1a. Camera unresponsive: retry with backoff; log incident.
Postconditions	Camera enabled; available for live view and recording

Table 7.28: Use Case — UC28: Disable camera

Use Case ID	UC28
Name	Disable camera
Priority	Medium
Actors	Administrator
Preconditions	Camera enabled; admin authenticated; no critical recording in progress
Trigger	Admin selects “Disable Camera”
Main Scenario	1. System warns about impacts (no live/recording). 2. Admin confirms; system disables the camera. 3. System updates status and logs action.
Alternate Flows	2a. Recording in progress: require stop or override.
Postconditions	Camera disabled; no live/recording permitted until re-enabled

8 Behavior and Sequences

8.1 Overview

This chapter illustrates the internal behavior of the SafeHome system in response to external actor interactions defined in the Use Case Model. Each sequence diagram shows message flows among system components—actors, control panels, web interfaces, sensors, cameras, and databases—over time. These diagrams complement the Use Case Model by visualizing how each use case scenario is executed by the system. All diagrams are placeholders and will later be replaced with finalized UML artifacts.

8.2 Sequence Diagrams – Common

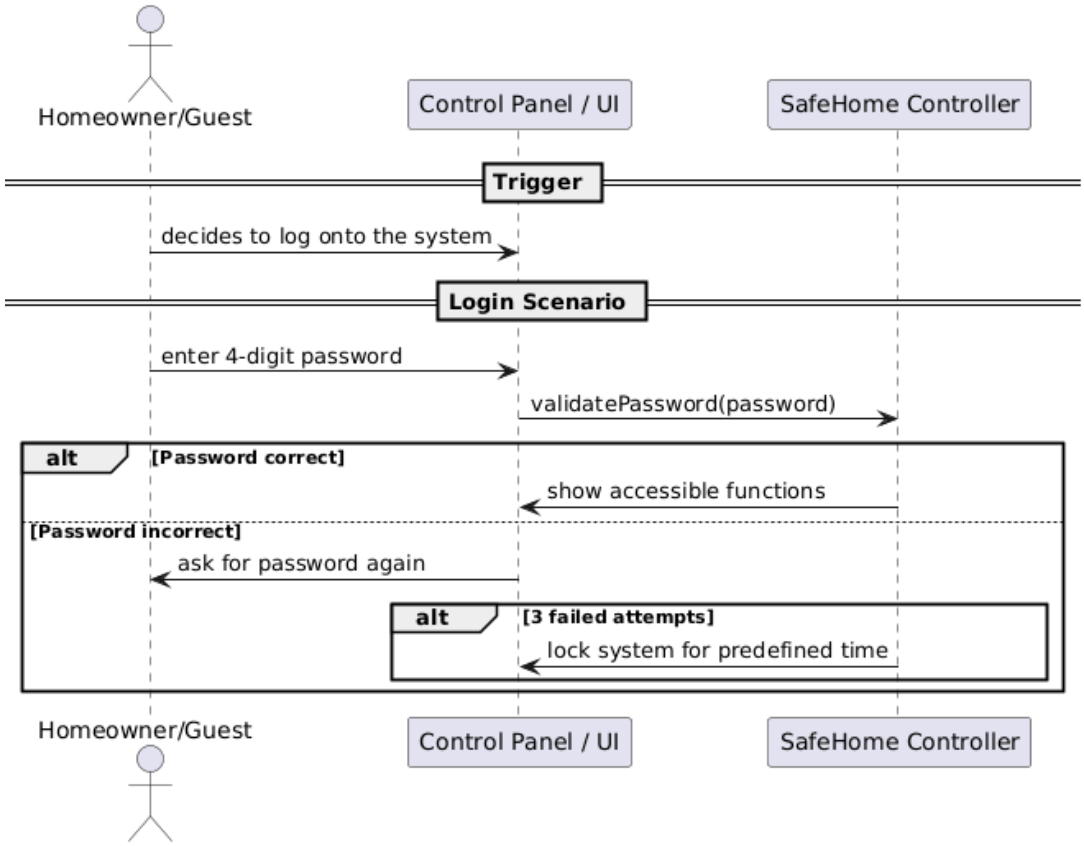

Figure 8.1: Sequence Diagram – UC1: User Login through Control Panel

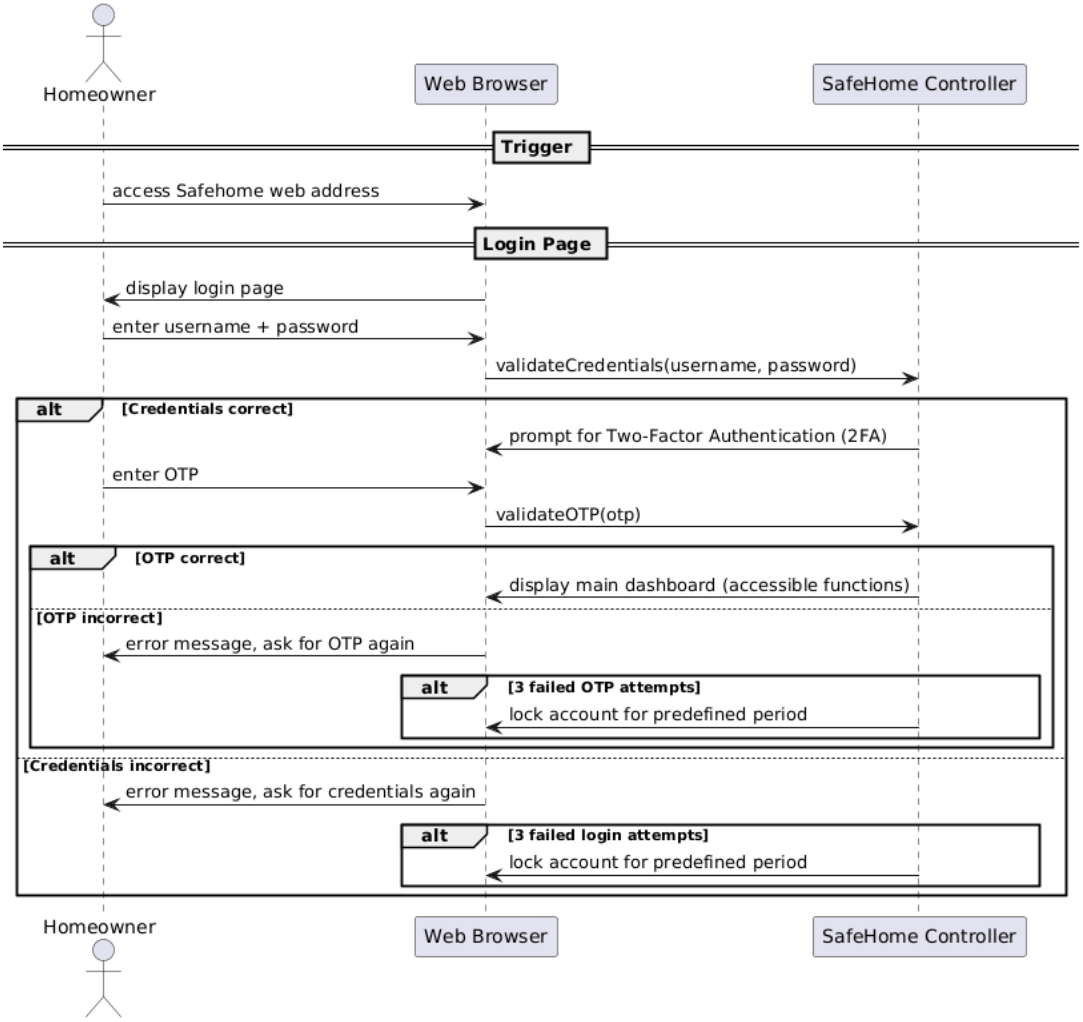

Figure 8.2: Sequence Diagram – UC2: User Login through Web Browser

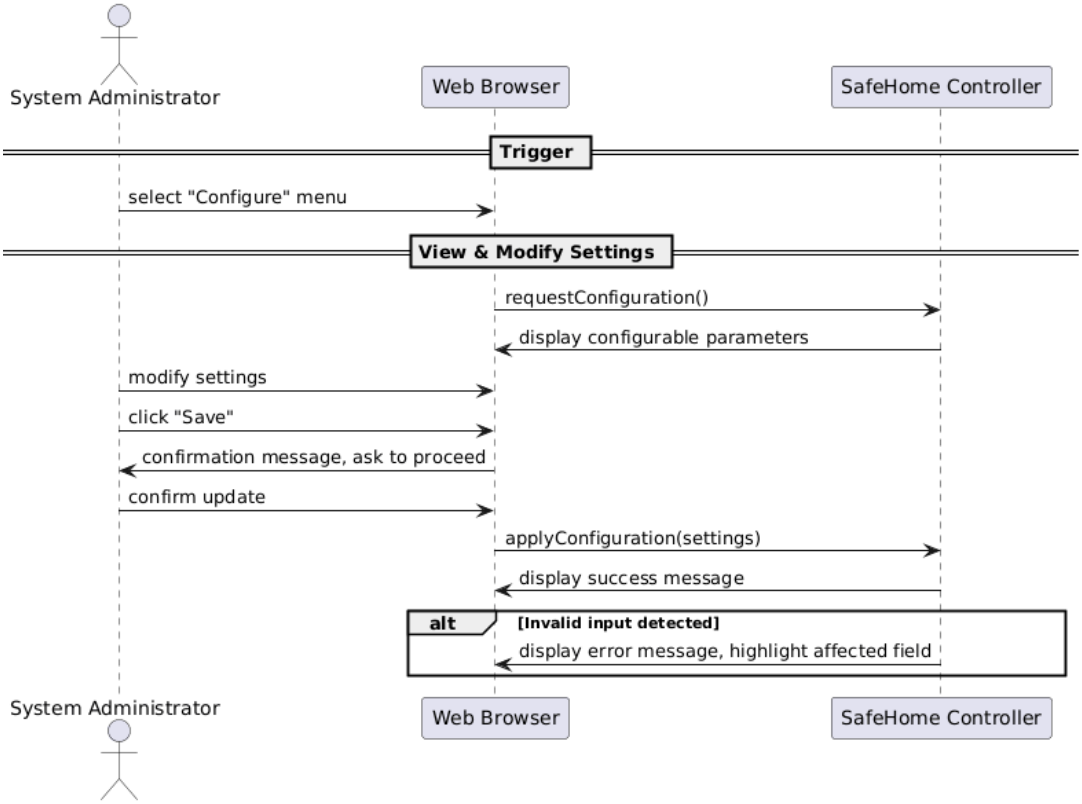

Figure 8.3: Sequence Diagram – UC3: Configure System Settings

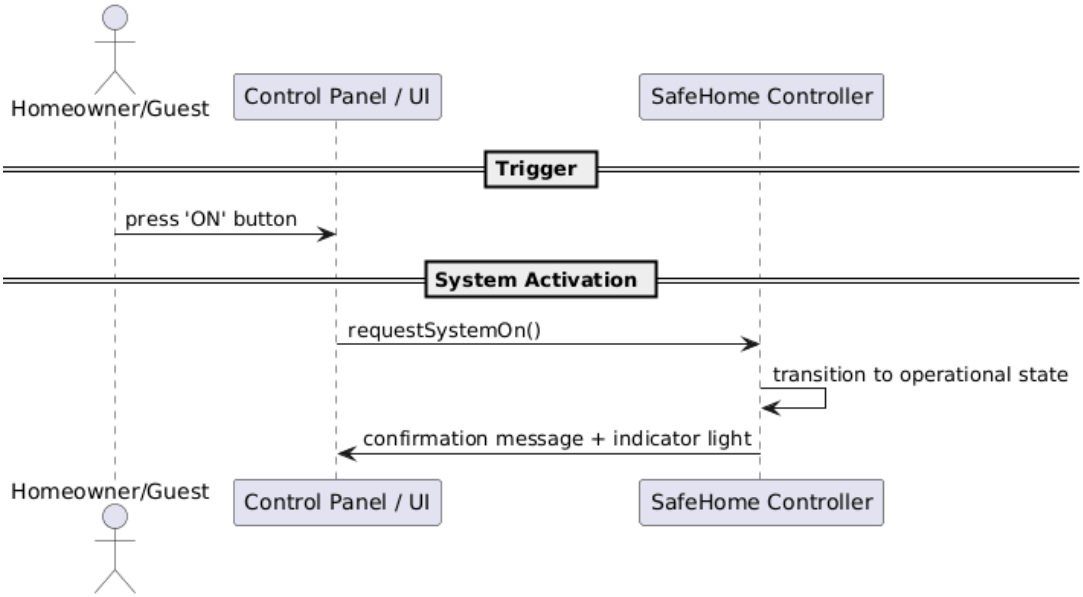

Figure 8.4: Sequence Diagram – UC4: Turn the System On

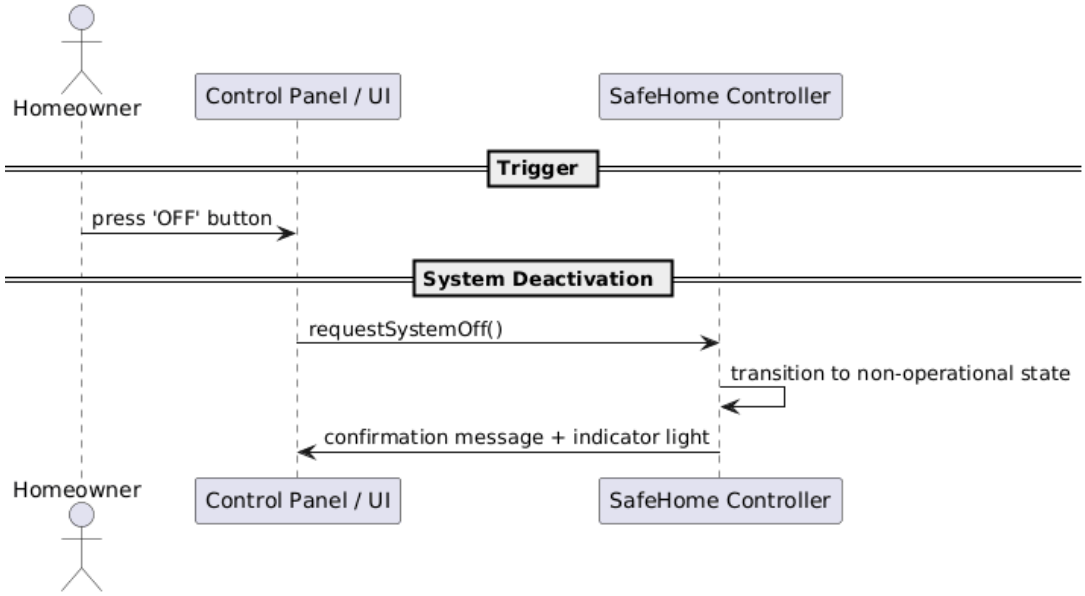

Figure 8.5: Sequence Diagram – UC5: Turn the System Off

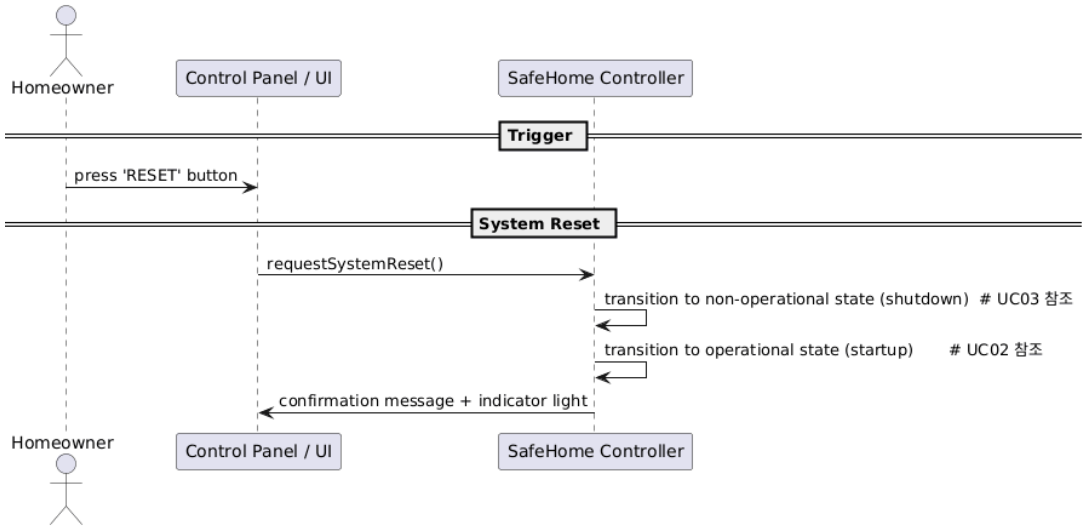

Figure 8.6: Sequence Diagram – UC6: Reset the System

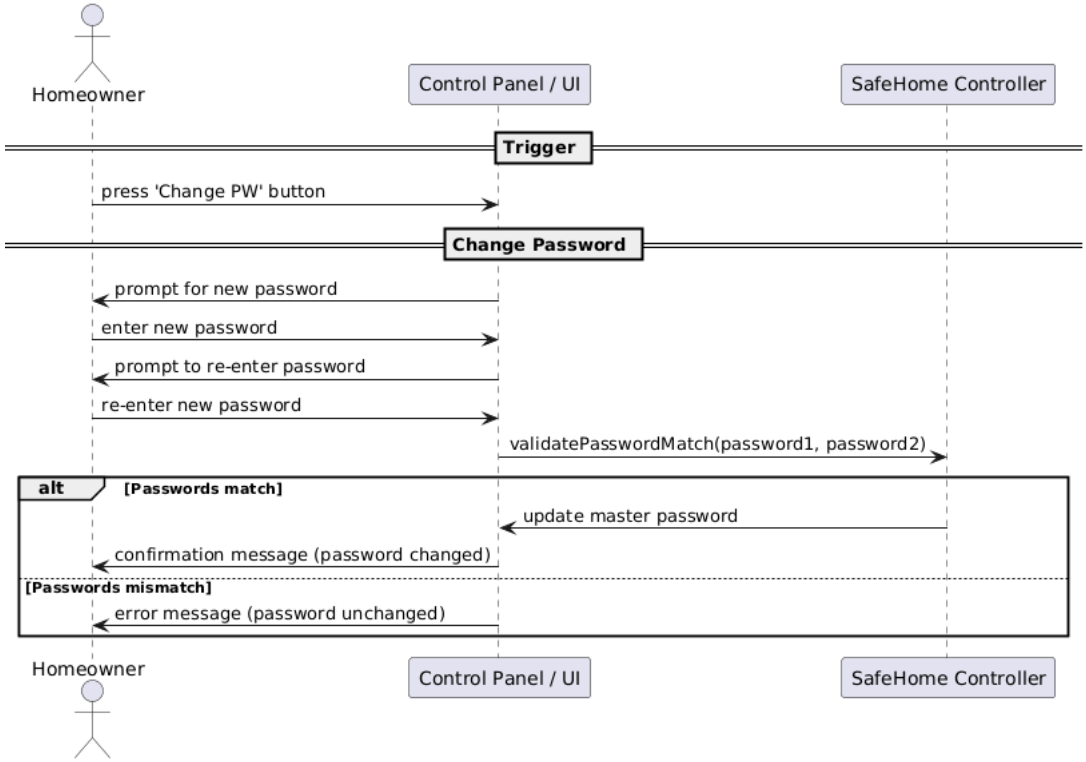

Figure 8.7: Sequence Diagram – UC7: Change Master Password

8.3 Sequence Diagrams – Security

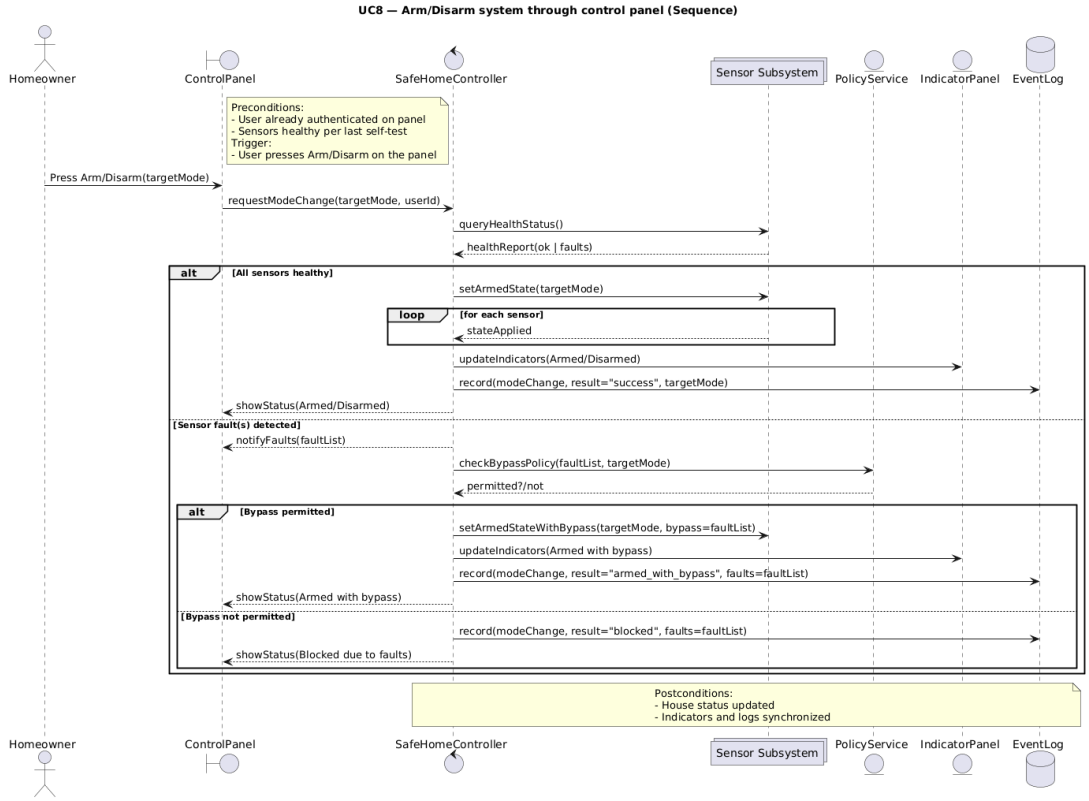

Figure 8.8: Sequence Diagram – UC8: Arm/Disarm System via Control Panel

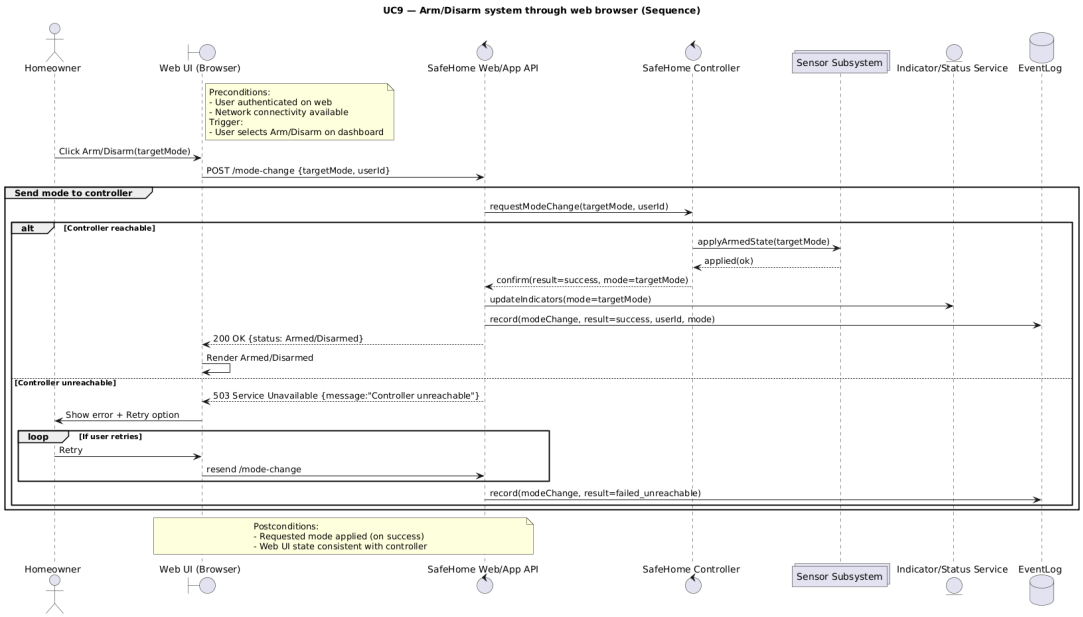

Figure 8.9: Sequence Diagram – UC9: Arm/Disarm System via Web Interface

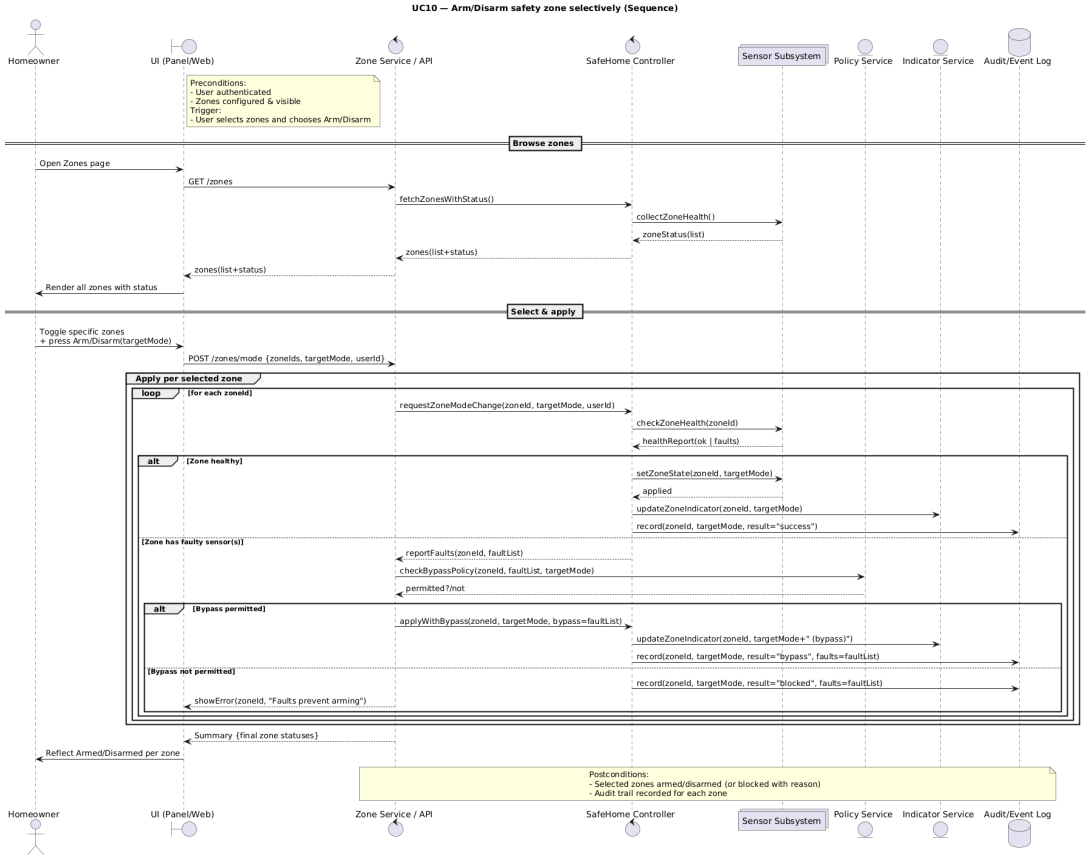

Figure 8.10: Sequence Diagram – UC10: Selective Zone Arming/Disarming

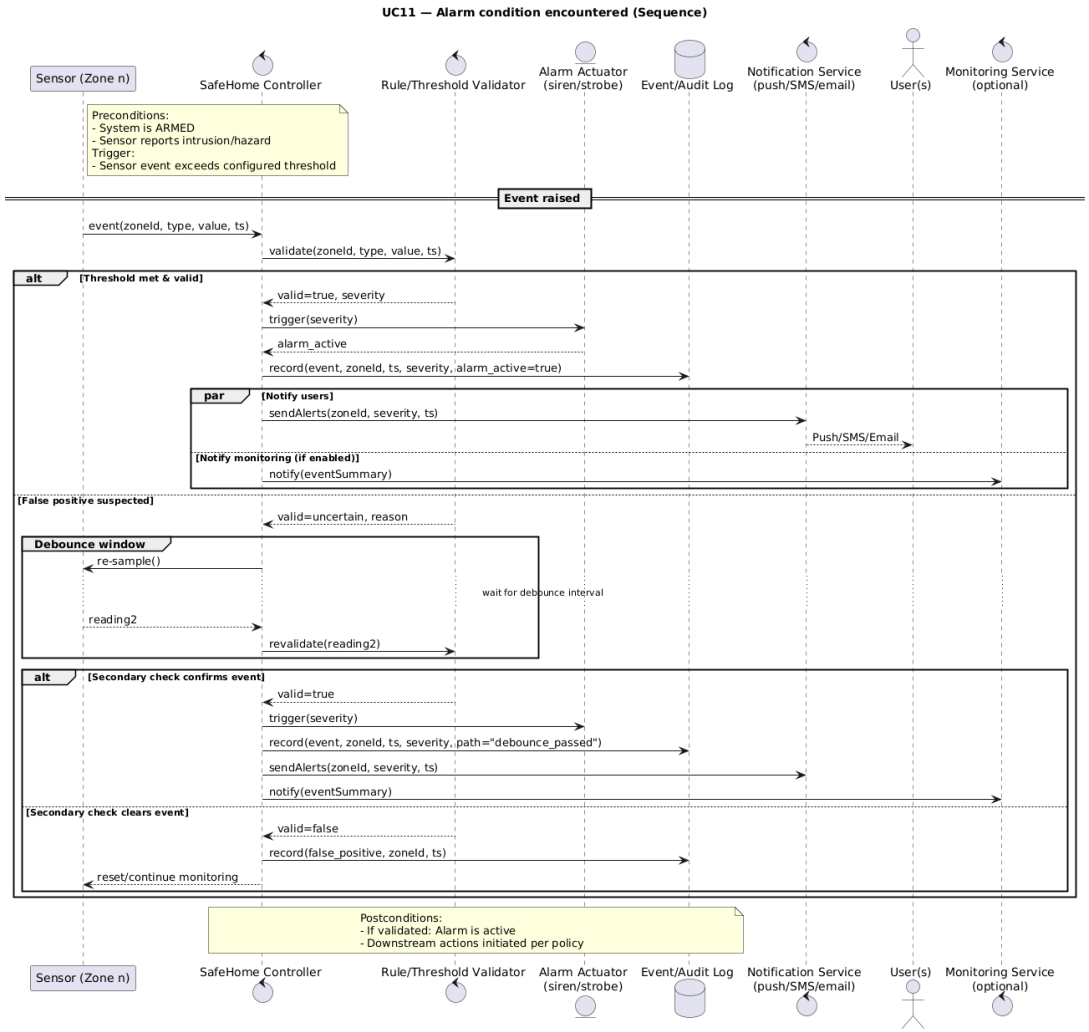

Figure 8.11: Sequence Diagram – UC11: Alarm Condition Encountered

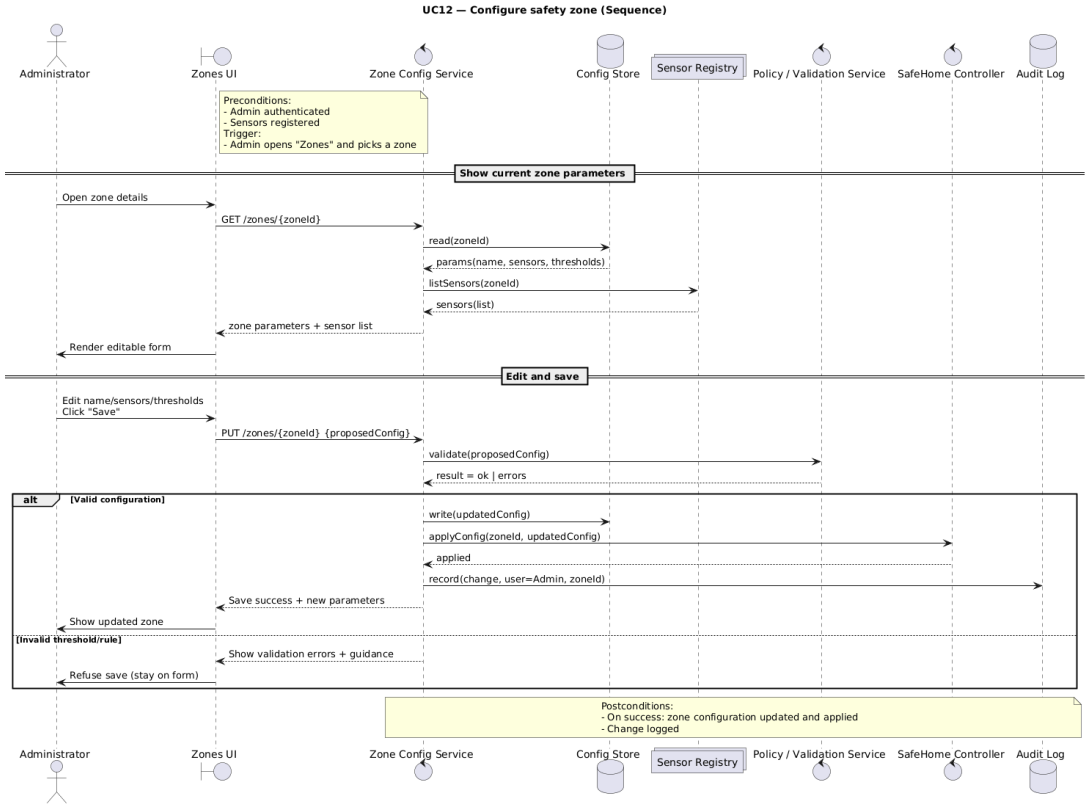

Figure 8.12: Sequence Diagram – UC12: Configure Safety Zone

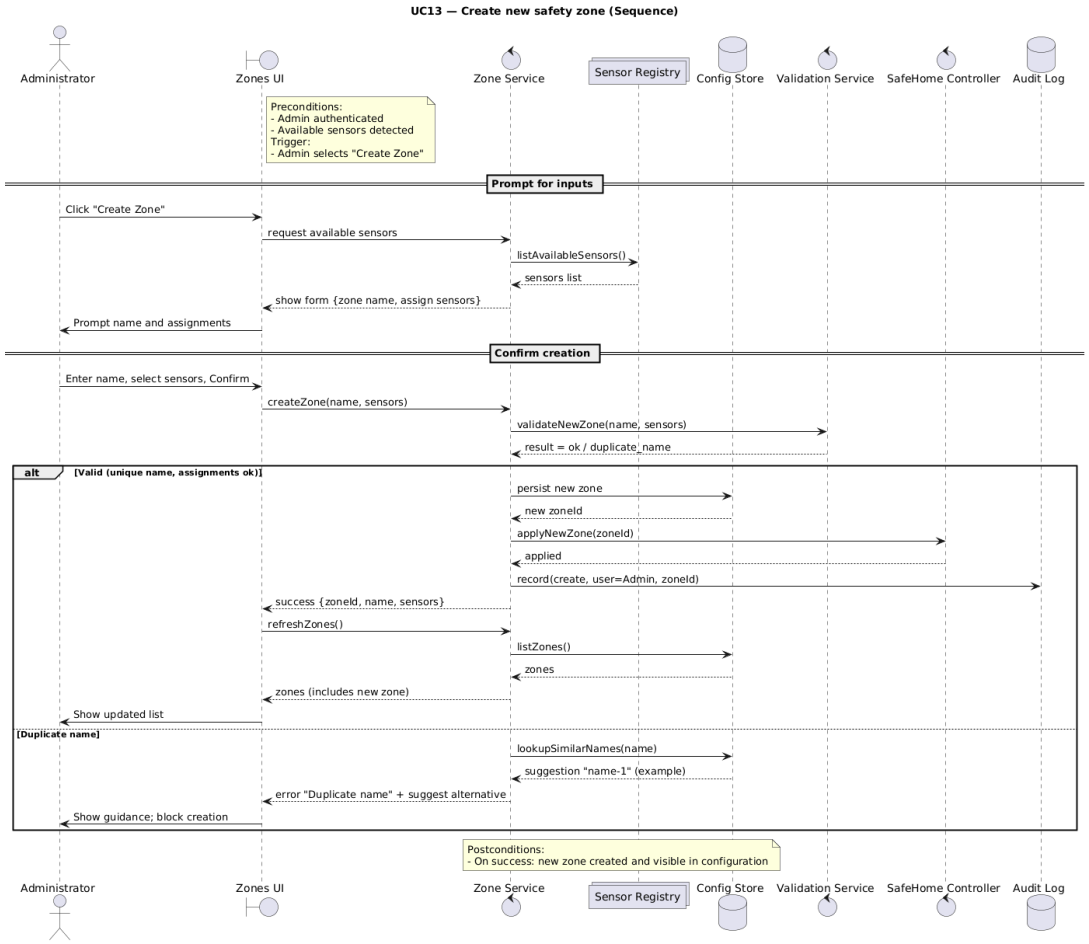

Figure 8.13: Sequence Diagram – UC13: Create New Safety Zone

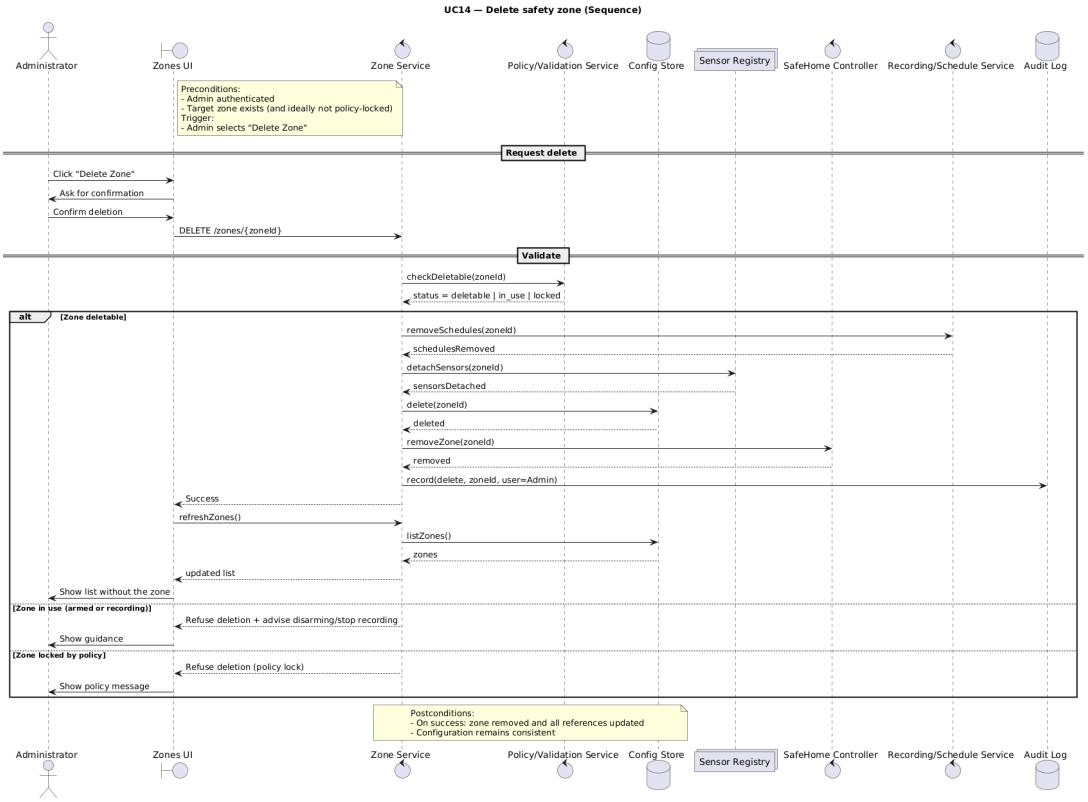

Figure 8.14: Sequence Diagram – UC14: Delete Safety Zone

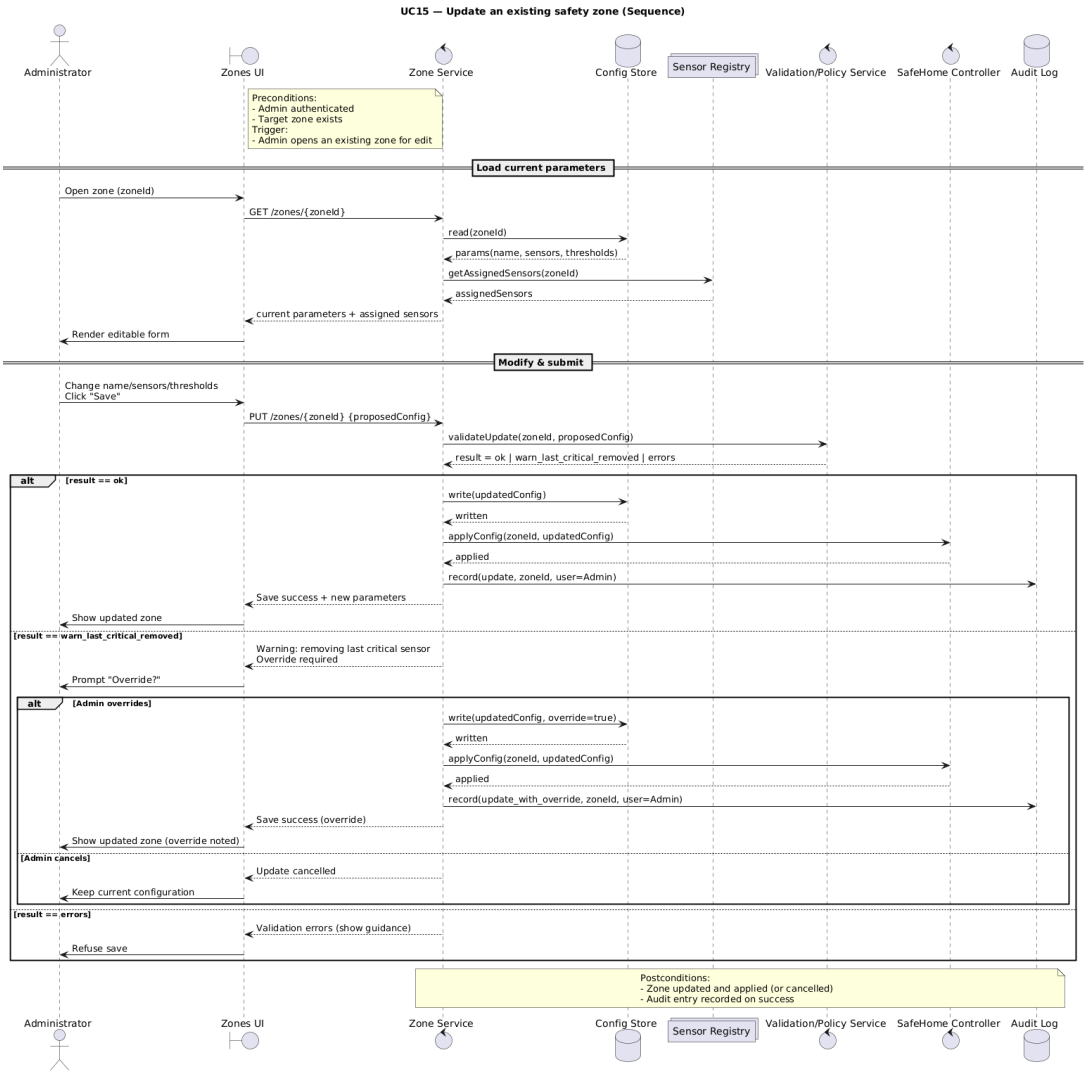

Figure 8.15: Sequence Diagram – UC15: Update Existing Safety Zone

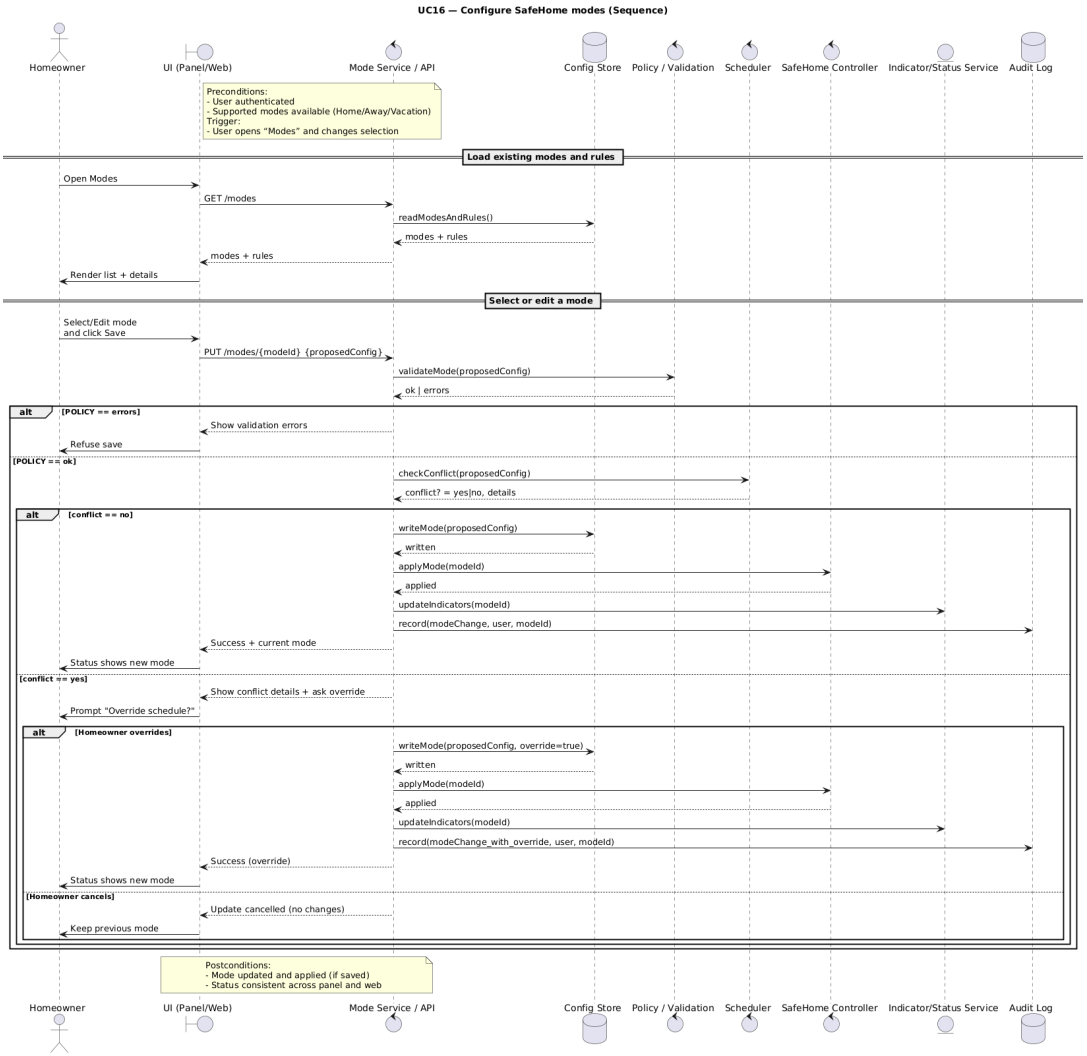

Figure 8.16: Sequence Diagram – UC16: Configure SafeHome Modes

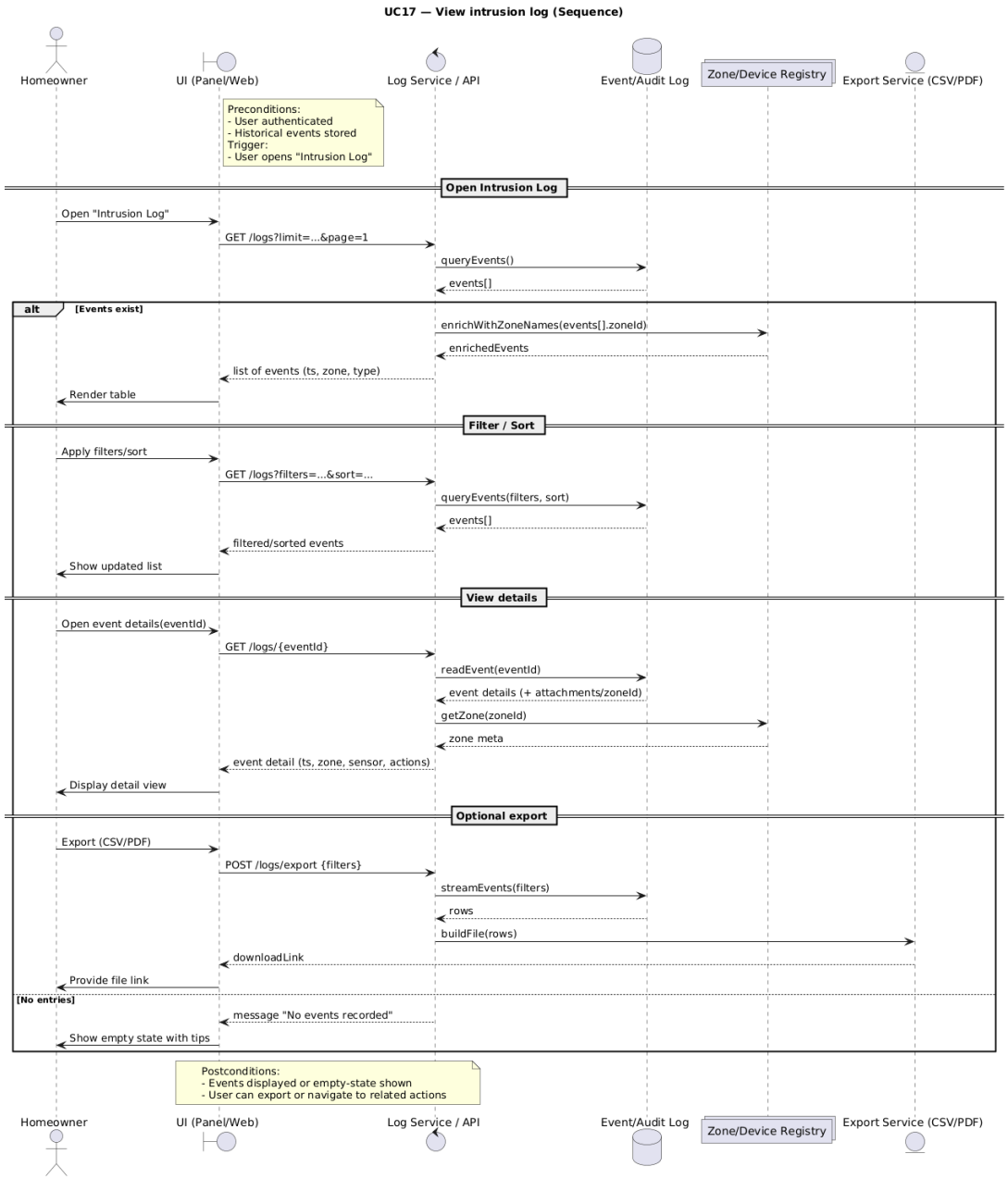

Figure 8.17: Sequence Diagram – UC17: View Intrusion Log

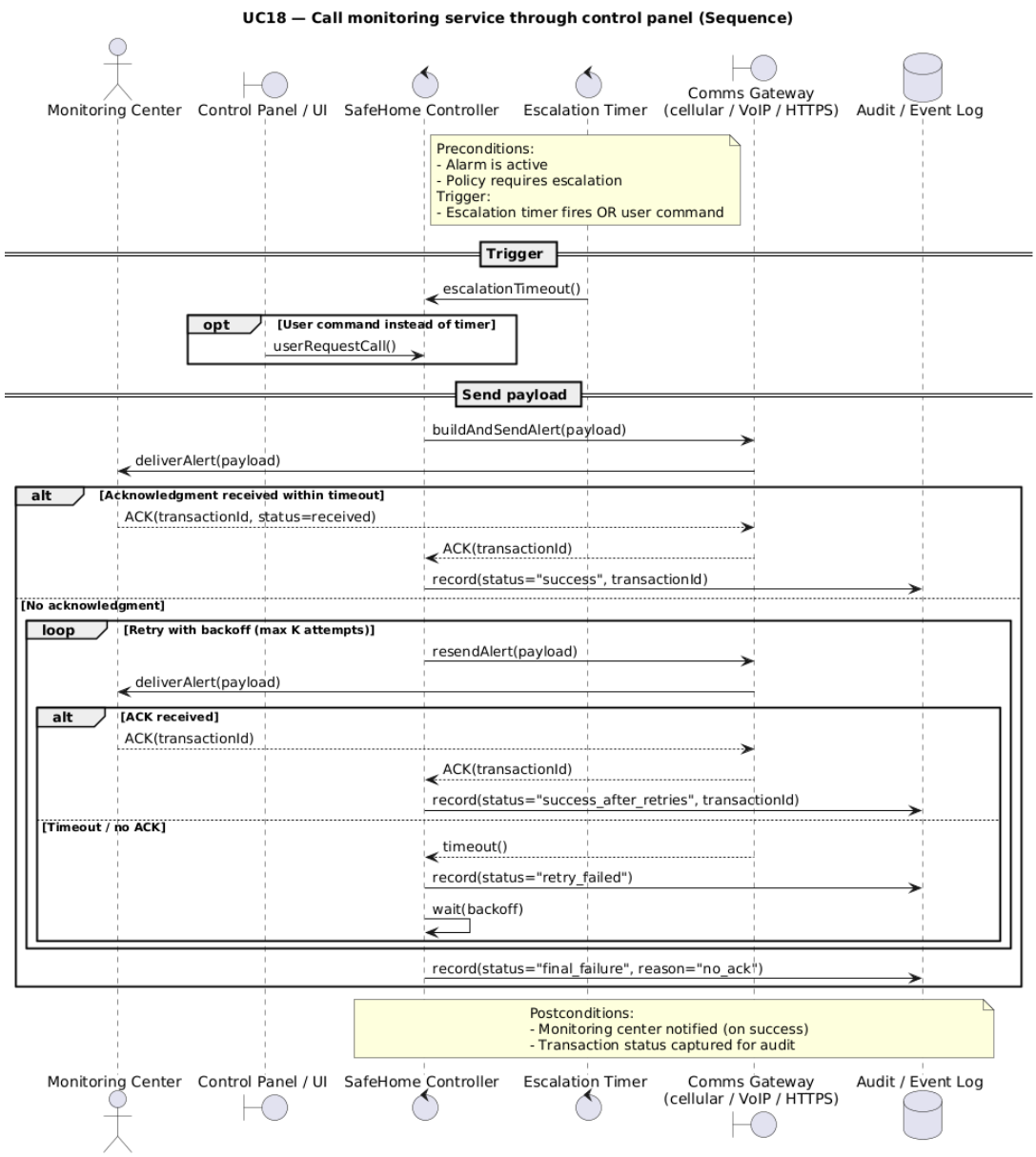

Figure 8.18: Sequence Diagram – UC18: Call Monitoring Service

8.4 Sequence Diagrams – Surveillance

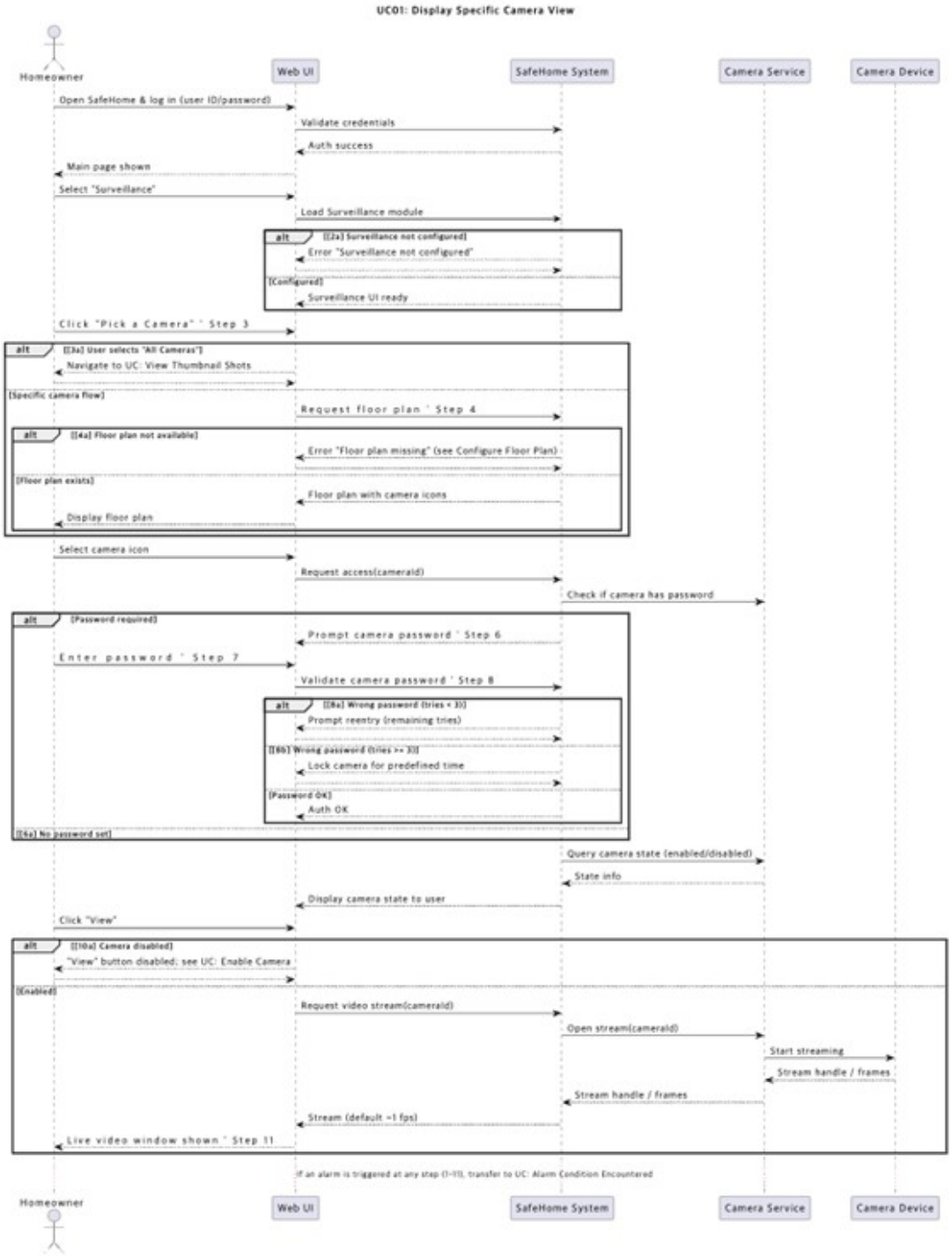

Figure 8.19: Sequence Diagram – UC19: Display Specific Camera View

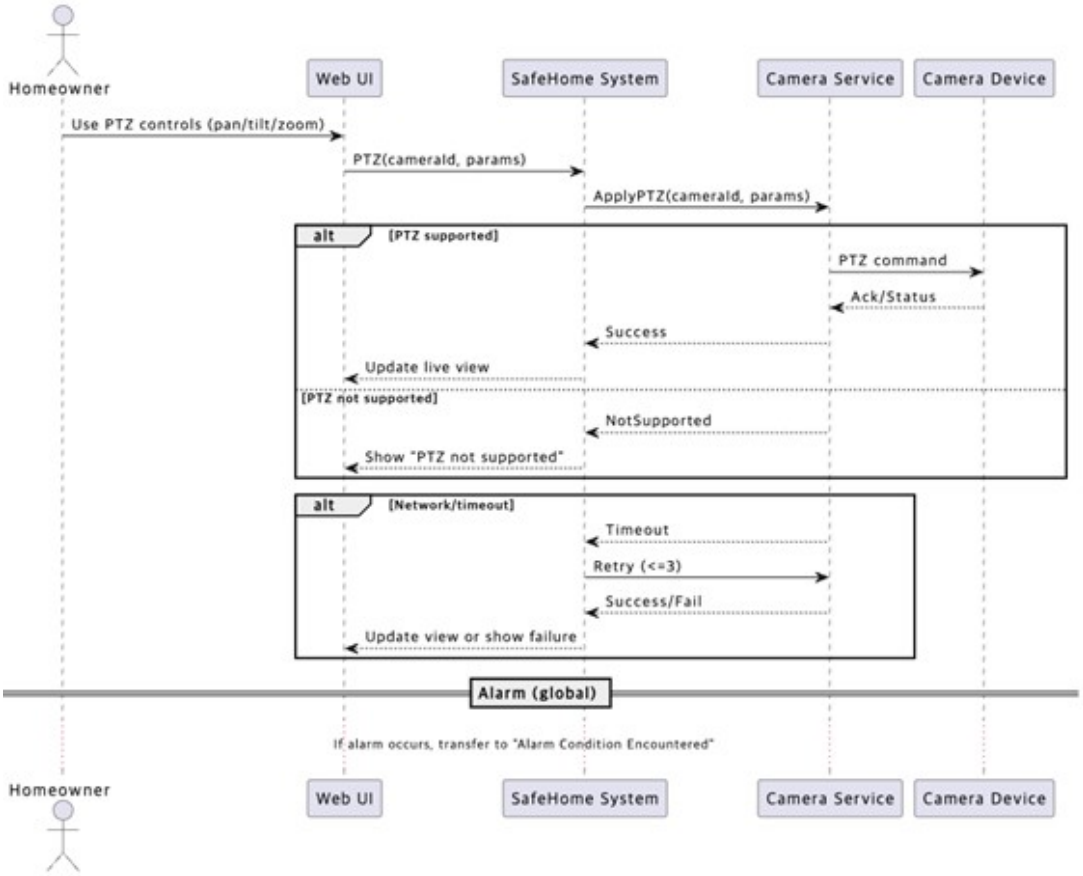

Figure 8.20: Sequence Diagram – UC20: Pan/Zoom Specific Camera View

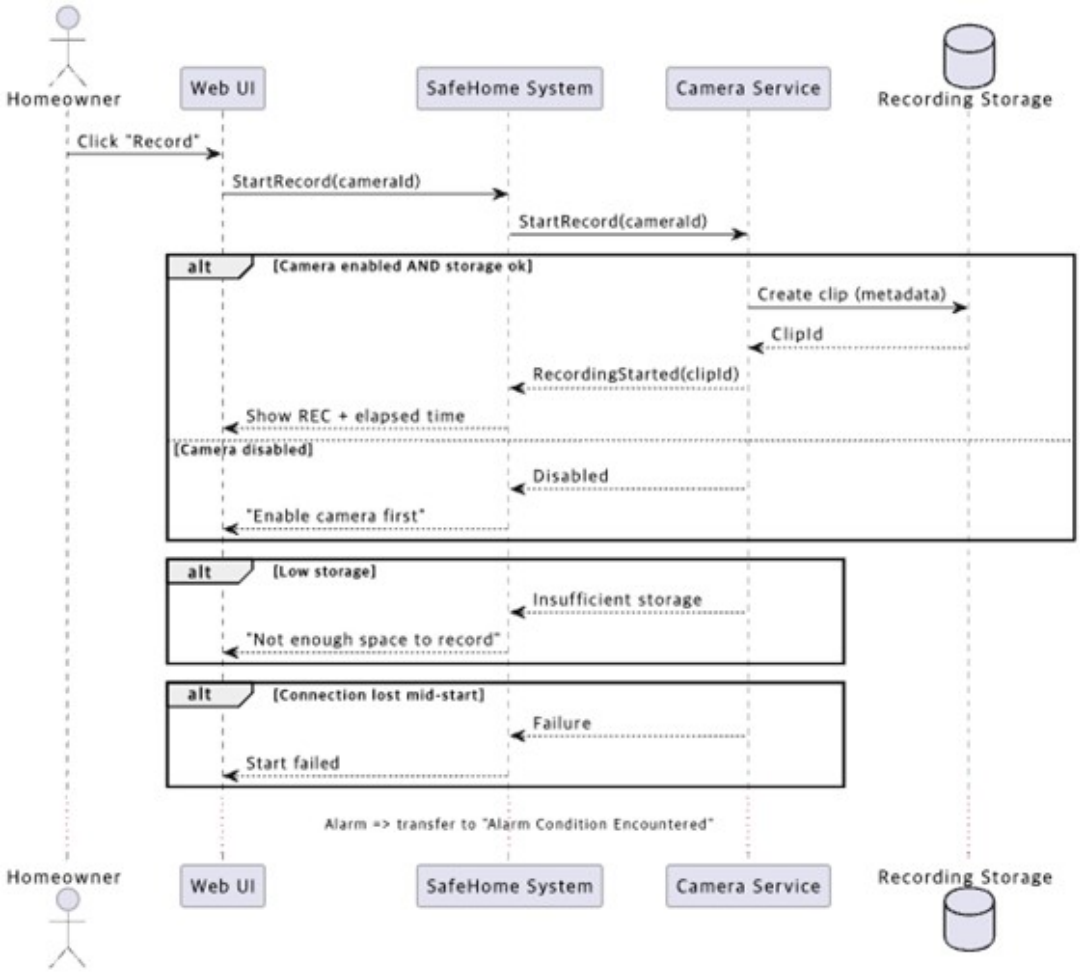

Figure 8.21: Sequence Diagram – UC21: Begin Camera Recording

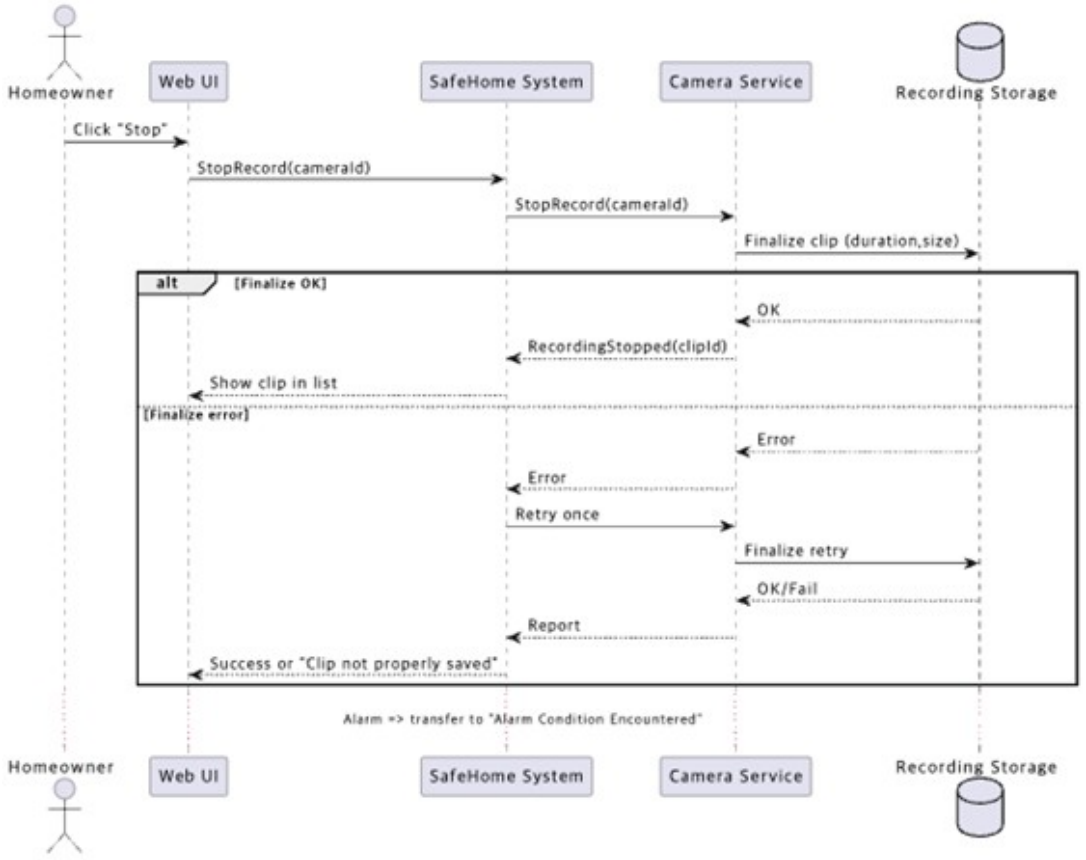

Figure 8.22: Sequence Diagram – UC22: Stop Camera Recording

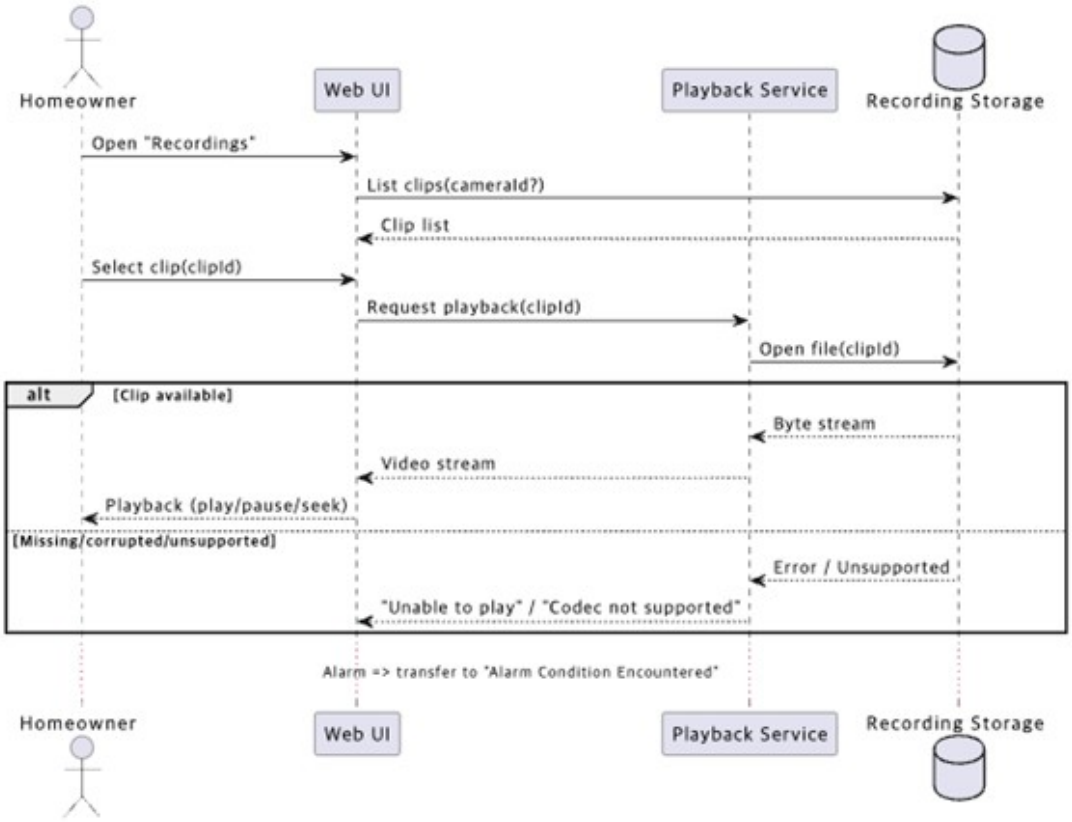

Figure 8.23: Sequence Diagram – UC23: Replay Camera Recording

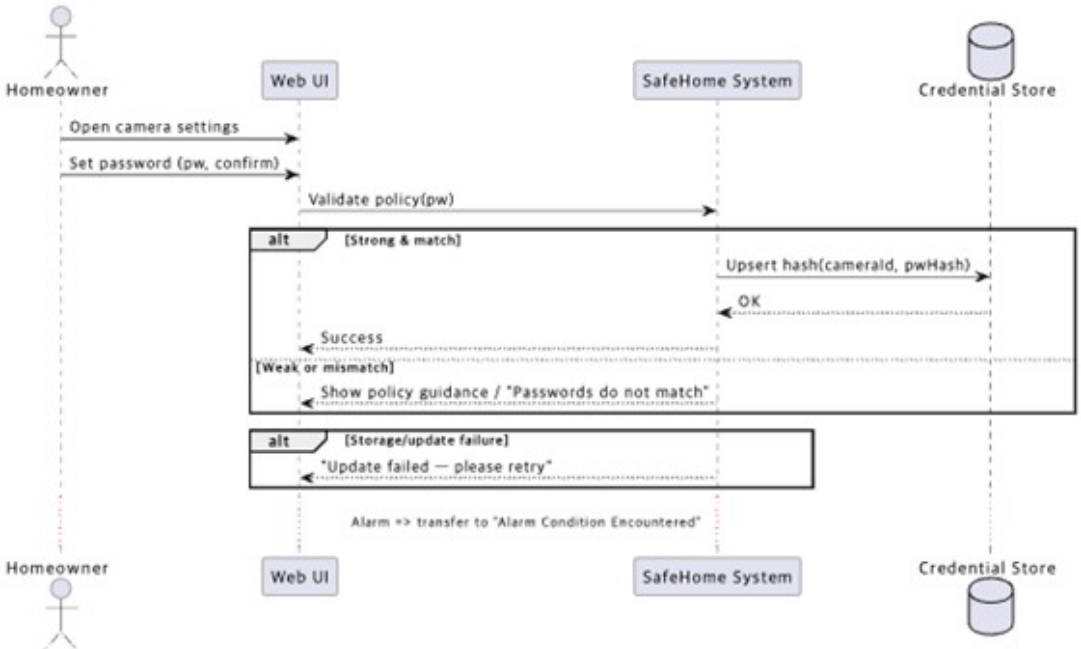

Figure 8.24: Sequence Diagram – UC24: Set Camera Password

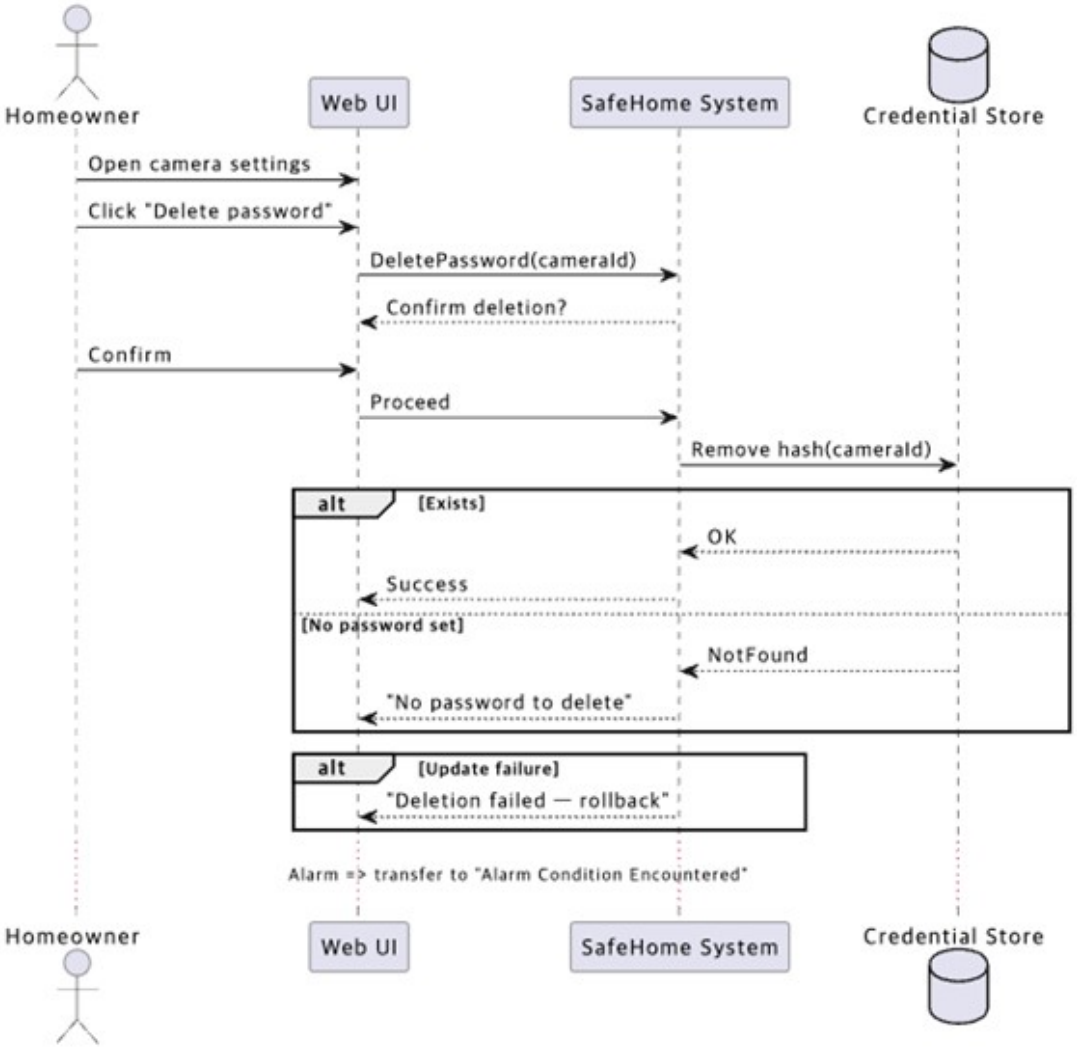

Figure 8.25: Sequence Diagram – UC25: Delete Camera Password

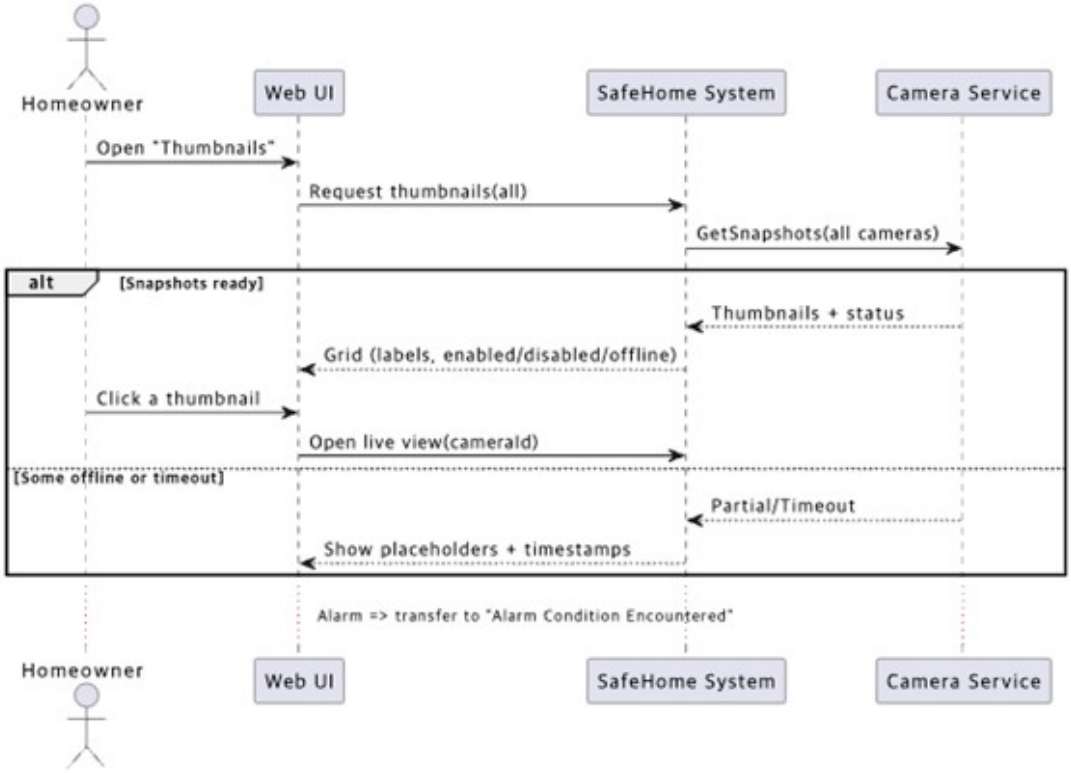

Figure 8.26: Sequence Diagram – UC26: View Thumbnail Shots

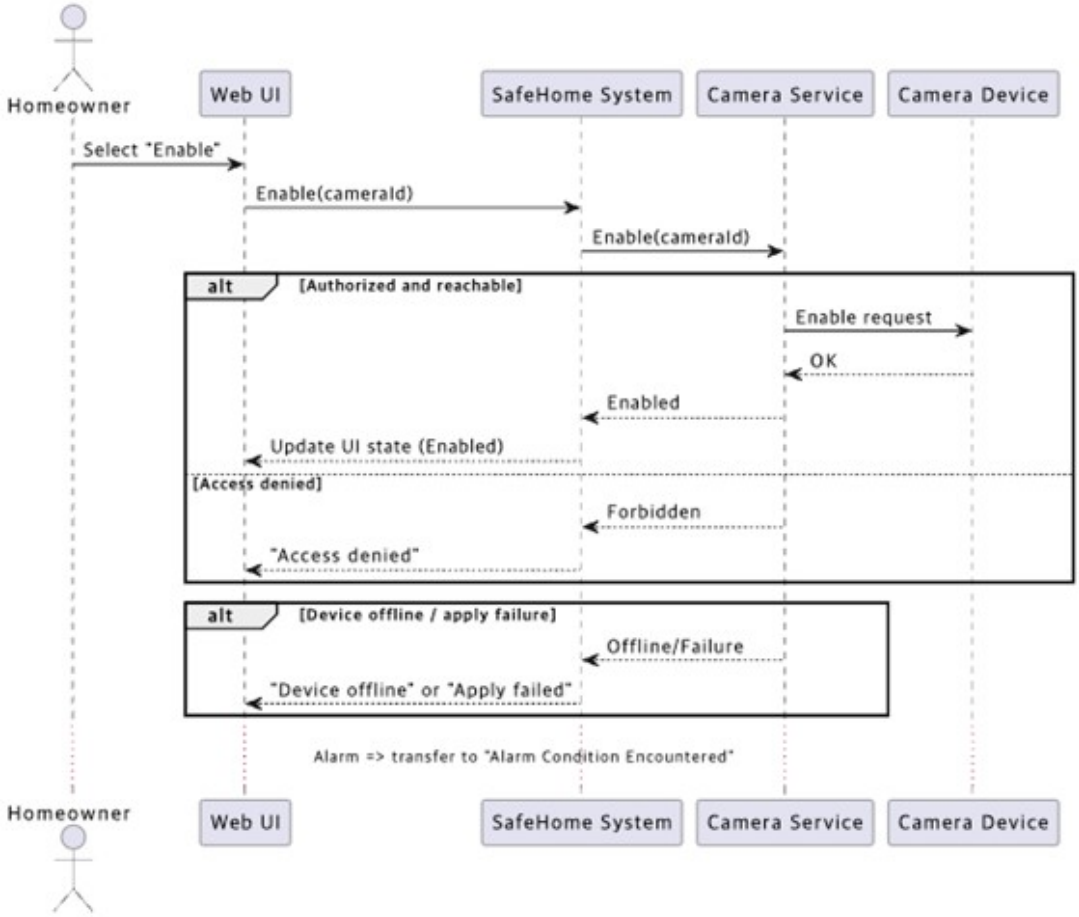

Figure 8.27: Sequence Diagram – UC27: Enable Camera

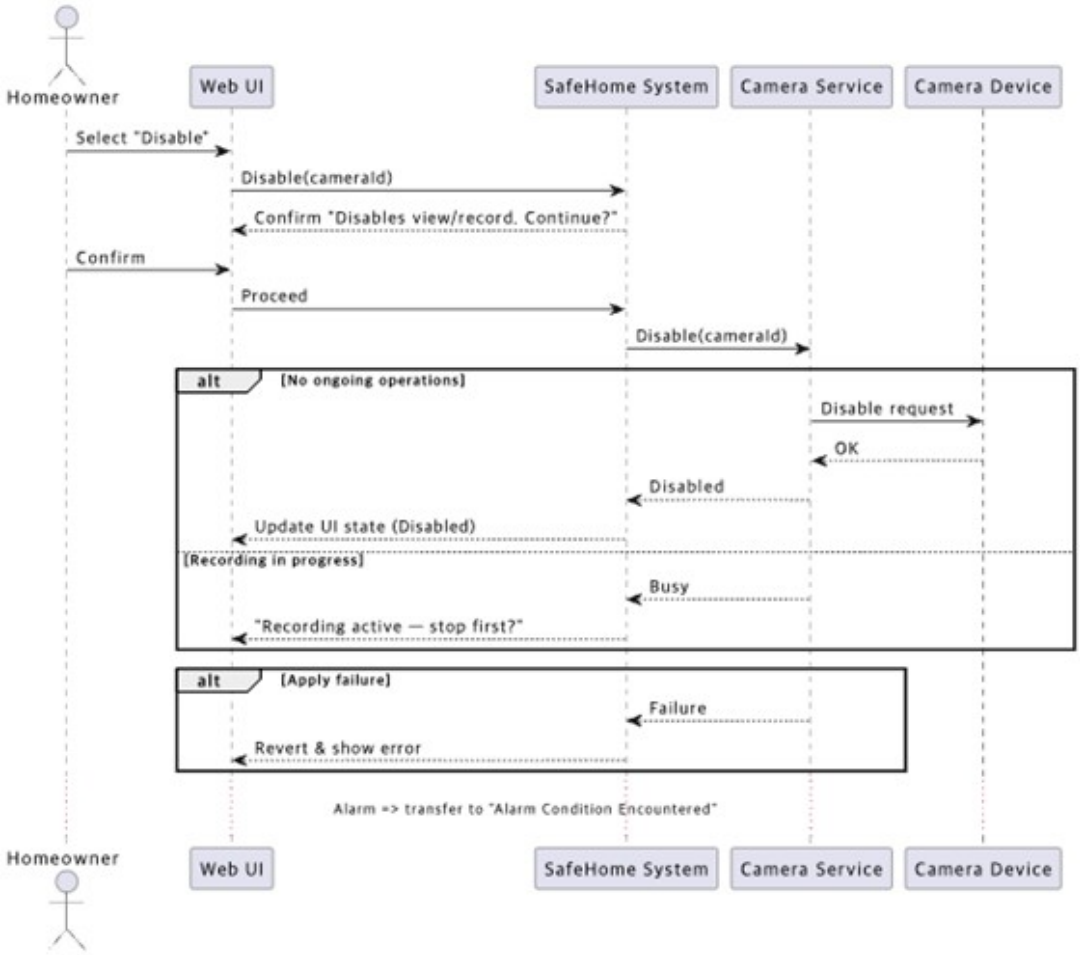

Figure 8.28: Sequence Diagram – UC28: Disable Camera

9 Project Records

9.1 Overview

This chapter documents the team's work contributions and responsibilities, summarizing who did what for each part of the project. It also records meeting notes, discussions, and key project decisions to ensure traceability and accountability throughout the project lifecycle.

9.2 Who Did What

Table 9.1: Team Member Responsibilities

Student ID	Name	Responsibilities
20190642	Sihun Chae	Use case scenario for common functions Use case diagram for common functions Sequence diagram for common functions Summarize meeting logs
20190659	Wooyoung Choi	Use case scenario for security functions Use case diagram for security functions Sequence diagram for security functions Organize the SRS template
20190074	Donggeun Kim	Use case scenario for surveillance functions Use case diagram for surveillance functions Sequence diagram for surveillance functions

9.3 Meeting Logs

9.3.1 1st Meeting

Time: Oct. 25th, 2025, 11:00AM–11:30AM
Location: Zoom meeting
Attendees: Sihun Chae, Wooyoung Choi, Donggeun Kim
Goal: Role assignment and schedule coordination

Discussion

- How to distribute roles and conduct the requirement analysis?

- By when will the requirement analysis be completed?
- By when will the draft SRS be completed?

Conclusion Each member was assigned specific roles and functions. The requirement analysis will be completed by Oct. 27, and the draft SRS will be completed by Oct. 29.

9.3.2 2nd Meeting

Time: Oct. 27th, 2025, 4:00PM–5:30PM
Location: E3-1
Attendees: Sihun Chae, Wooyoung Choi, Donggeun Kim
Goal: Define the functional and non-functional requirements.

Discussion

- How should we define the functional and non-functional requirements?

Conclusion We defined the functional and non-functional requirements by first reviewing the SafeHome project goals and key user needs such as safety, convenience, and remote access. We then analyzed use cases to identify essential system actions like arming/disarming, alarm handling, and authentication for the functional requirements. Finally, we defined non-functional requirements by focusing on system qualities such as security, performance, and reliability that ensure stable and efficient operation.

9.3.3 3rd Meeting

Time: Oct. 28th, 2025, 4:00PM–5:00PM
Location: E3-1
Attendees: Sihun Chae, Wooyoung Choi, Donggeun Kim
Goal: Define assumptions for SRS.

Discussion

- What assumptions should we make?

Conclusion We defined the SafeHome project assumptions by reviewing system scope, dependencies, and excluded features. Hardware setup, network connectivity, and monitoring infrastructure were considered pre-established. Mobile access, e-commerce, and credential management were set as out of scope. Security assumptions include proper credential handling, reliable internal communication, and compliant data protection. For surveillance, we assumed all camera hardware and network configurations were already verified. These assumptions clarify project boundaries and ensure focus on core SafeHome functionality.

9.3.4 4th Meeting

Time: Oct. 30th, 2025, 7:00PM–8:00PM
Location: E3-1
Attendees: Sihun Chae, Wooyoung Choi, Donggeun Kim
Goal: Review the SRS document and provide feedback for improvement.

Discussion

- Reviewed the completeness and clarity of functional and non-functional requirements.
- Checked consistency between use cases and system requirements.
- Identified minor ambiguities in requirement wording and suggested clearer phrasing.

Conclusion We agreed that the SRS is generally well-structured and comprehensive. Minor revisions will be made to improve clarity and consistency. Final review and formatting adjustments will be completed before submission.

10 Glossary

10.1 Terminology Table

Term	Description
Actor	Any external user or subsystem that interacts with SafeHome.
Administrator	The person who sets up the SafeHome system, configures system settings, lays out the floor plan, and places the cameras.
Camera View	The live or recorded visual field captured by a specific surveillance camera.
Control Panel	A small gadget to display basic information and receive commands.
Floor Plan	A map showing the homeowner's security and surveillance layout.
FR	Functional Requirement, specifying what the system must do.
GUI	Graphical User Interface of the control panel or web application.
Guest	A person who temporarily enters the home, such as a housekeeper or repair worker.
Homeowner	The primary user who installs and manages SafeHome security and surveillance features in their home.
NFR	Non-Functional Requirement, defining quality attributes of the system.
SafeHome	Target home security and surveillance system described in this SRS.
Safety Zone	A designated area within or around the home that is continuously monitored for security and safety purposes.
Two-Factor Authentication	A security mechanism that requires the user to provide two forms of verification before gaining access to the system.