CS350 Safehome Project
Software Requirement Specification (SRS)

Project Group #7 Members:

StudentID	**20230943**
StudentID	**20230970**
StudentID	**20230988**
StudentID	**20231008**

Korea Advanced Institute of Science and Technology

Table of Contents

I. Overview

1. Introduction

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

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

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

2. Goal

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

Functional goal is to provide the followings:

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

Plan for first increment

Beginning of the project	Oct 29, 2025
Initial requirement gathering	Oct 29 - Nov 4, 2025
Planning and creating analysis model	Oct 29 – Nov 20, 2025
Creating design model	Nov 21 - Dec 5, 2025
Construction & testing	Dec 6 – Dec 19, 2025
Testing & bug fixing	Dec 20 – Dec 26, 2025
First deployment	Dec 26, 2025 –

id	Name of Process	Begins	Ends	Working Period	10 2025	11 2025		12 2025		
					29-4	4-20	21-5	6-19	20-26	26+
1	Initial requirement gathering	2025-10-29	2025-11-4	5d						
2	Planning and creating analysis model	2025-10-29	2025-11-20	16d						
3	Creating design model	2025-11-21	2025-12-5	12d						
4	Construction & testing	2025-12-06	2025-12-19	10d						
5	Testing & bug fixing	2025-12-20	2025-12-26	5d						
6	First deployment	2025-12-26	2025-12-26	1d						

III. Prototype GUI

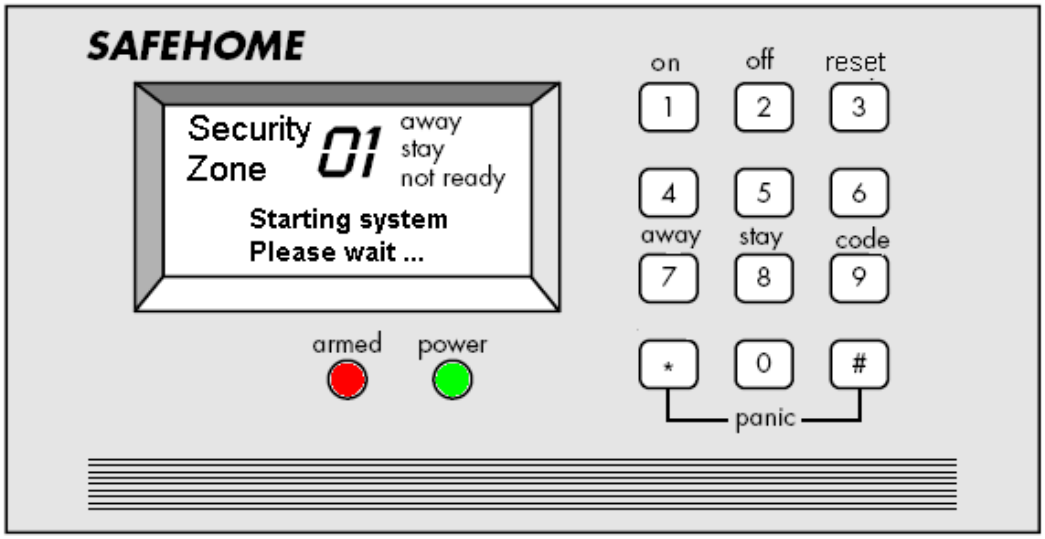


Fig 1. Control Panel

Fig 2. Login Screen

Fig 3. MainFunctions

Fig. 4 Security Function – Safety zone

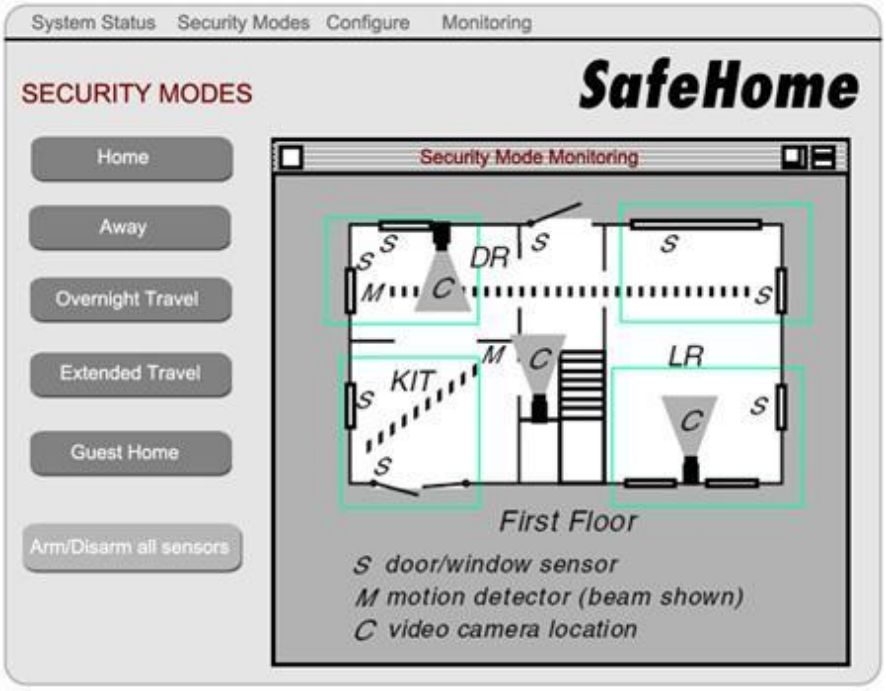


Fig. 5 Security Function – Security Mode

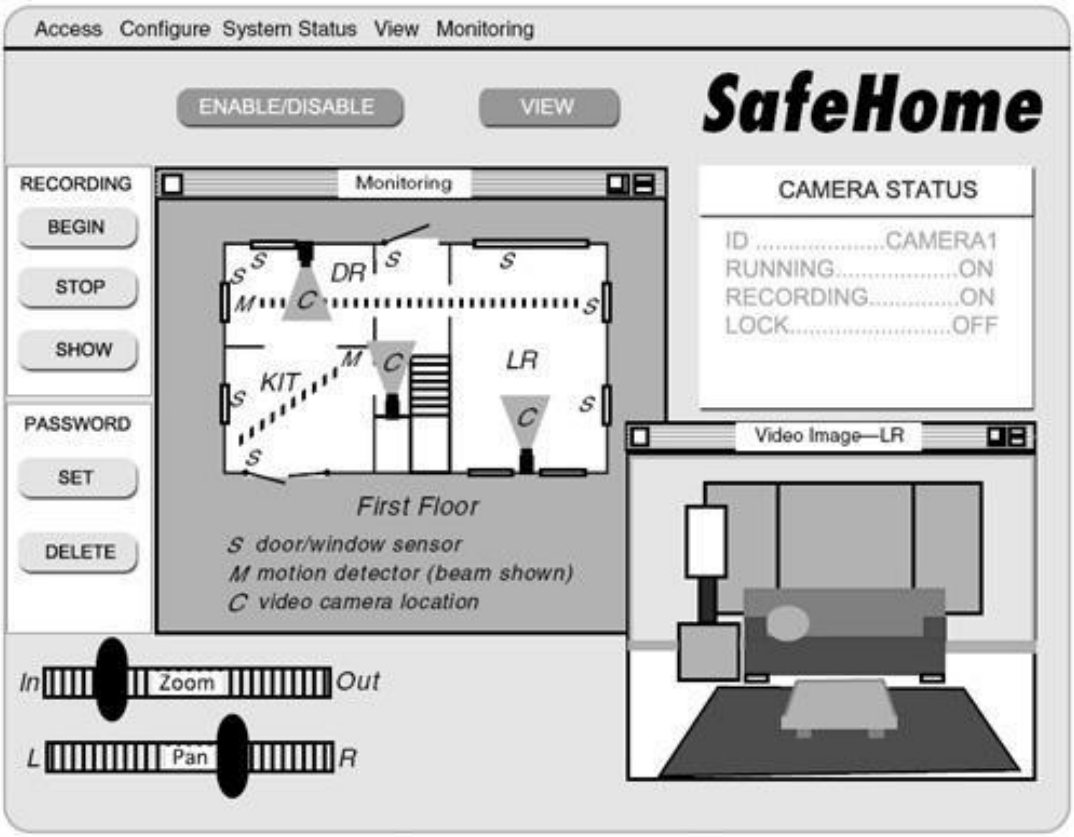


Fig. 6 Surveillance Function.

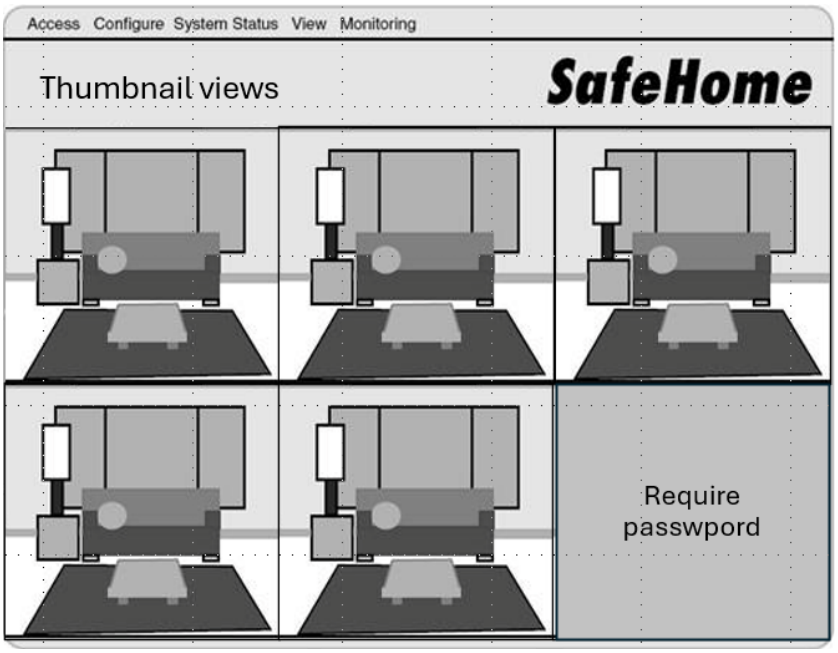


Fig. 7 Thumbnail view.

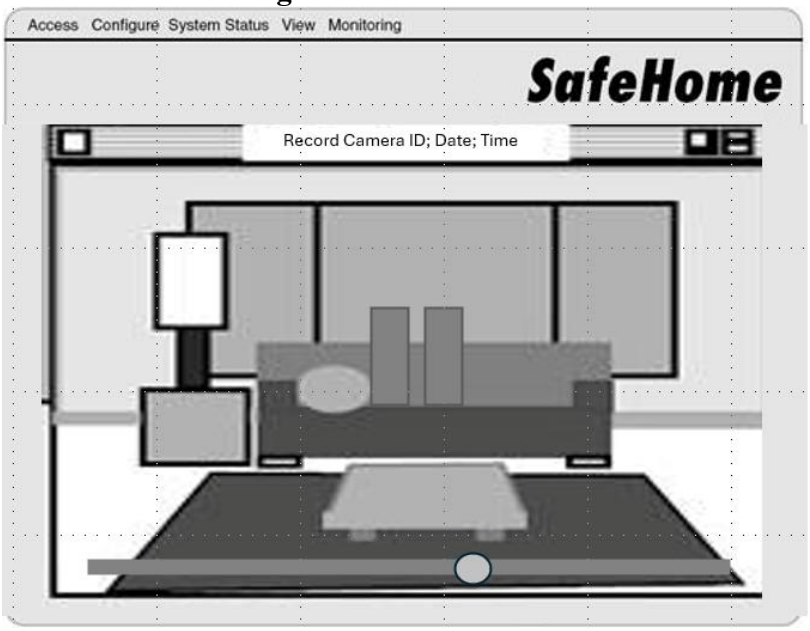


Fig. 8 Replay Record view.

IV. Assumptions

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

1. Camera monitoring zone in page X is defined as camera pan/zoom control

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

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

4. “set alarm” on slide Y is setting delay time defined in the use case “configure system setting”

5. “configure Safehome system parameters” on page w is defined as “configure system setting”

6. “encounters an error condition” on slide z is not defined as an use case but is described in exceptions of each use cases

7. reconfigure sensors on page q is considered as setting floor plan which is not in the scope of our project.

8. “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.

9. Doggie angst sensor on page z is considered to be implemented in the next increment

10. Enable/test/read/disable sensors on page y is for test cases. We only control sensors through changing house safety situation or by arming/disarming safety zones.

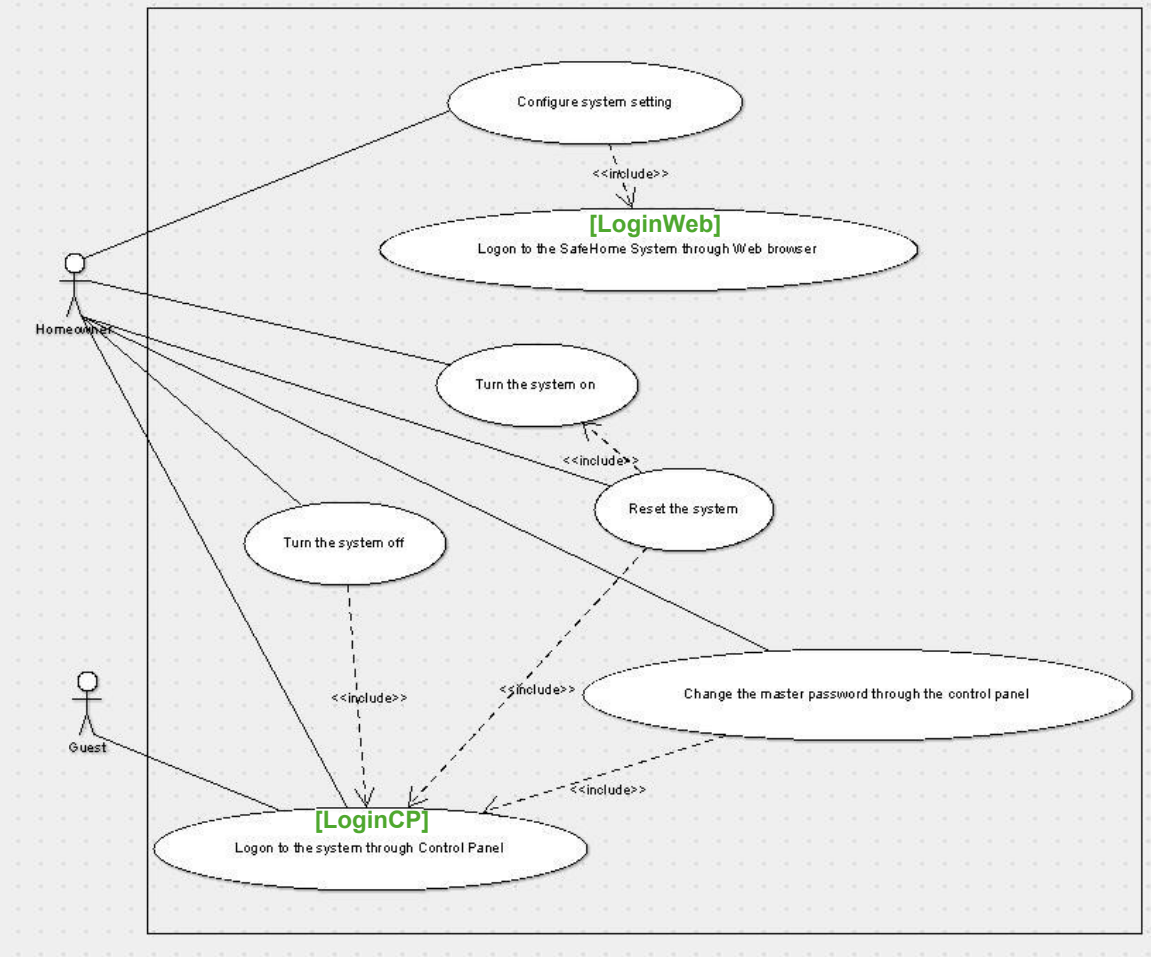
11. We do not consider web pages selling product on page k

12. We added function to view intrusion log on the web page

13. We added enabling and disabling all the cameras

V. Use Case Diagrams

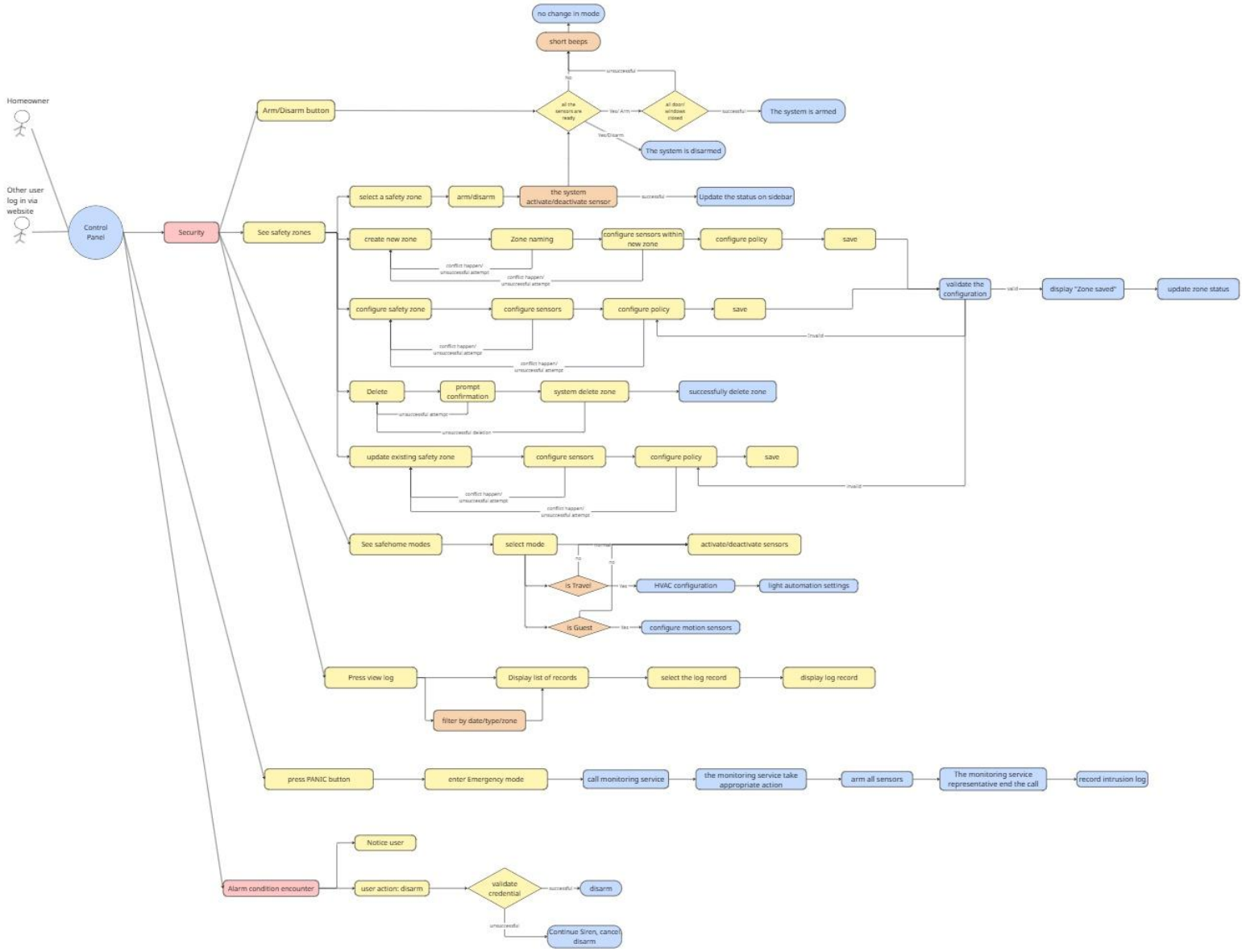
1. Common Functions



< Figure 9. Common Functions [CM]>

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

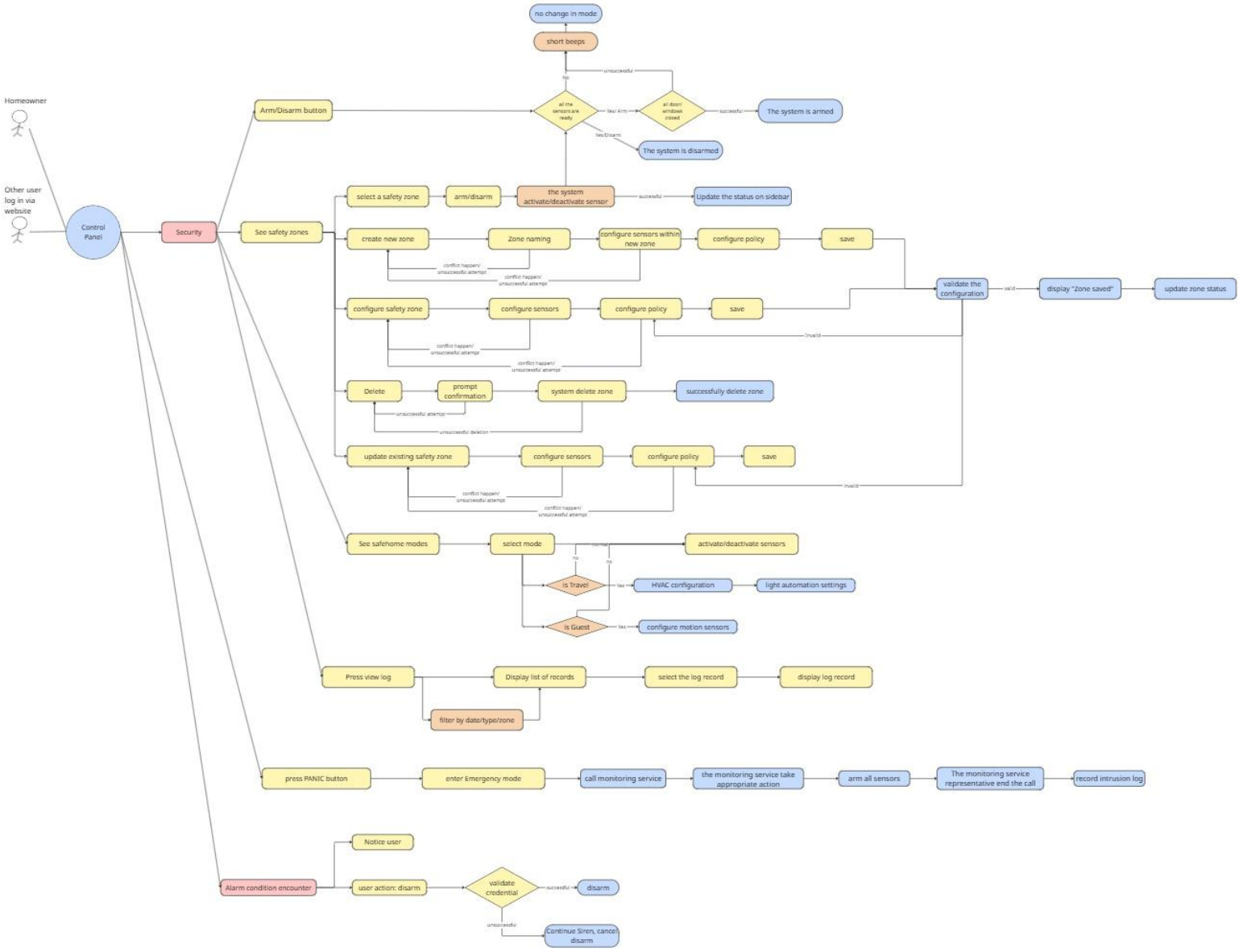
2. Security Functions



< Figure. 10 Security Functions >

Reference in meeting log 2025.10.27

4. Configure Safety Zone Functions

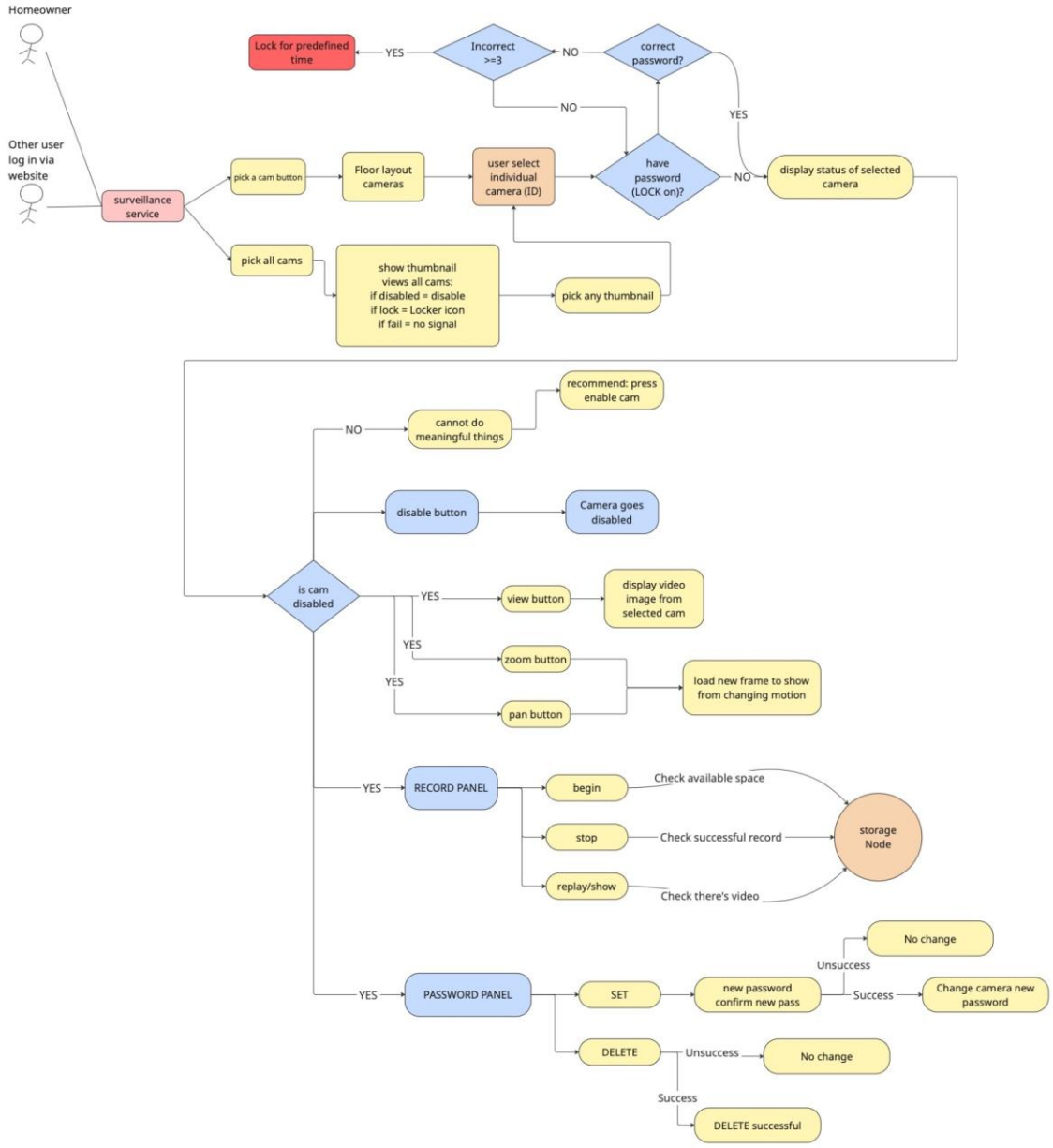


5.

< Figure. 11 Security Functions >

Reference in meeting log 2025.10.27

4. Surveillance Functions



< Figure 12 Surveillance Functions>

Reference in meeting log 2025.10.27

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 system through control panel
Preconditions: The system has been configured, powered on and connected. A 4-digit number master password must be obtained. The control panel must be operational.
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 password.
3. The system validates the password.
4. The control panel screen shows accessible functions on the control panel.

Exception:

1a. Password incorrect
.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 a set amount of time.
2a. 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?
2. What mechanisms alert the homeowner about the failed login attempts?
3. What mechanisms allow the user to recover the password if the user forgets it?

Reference in meeting log 2025.10.28

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 log onto the system through web browser
Preconditions: The system has been configured, powered on and connected. A registered user ID, password and email must be obtained. Web browser system must be operational
Trigger: The homeowner/guest decides to log onto the system.
Scenario:

1. The homeowner/guest opens the system's website via web browser.
2. The homeowner/guest enters the user ID and password.
3. The system validates the user ID, password and sends an authentication code to the respective email
4. The homeowner/guest enters the authentication code within a set amount of time
5. The web browser shows accessible functions on the web browser.

Exception:

3a. User ID not registered or password incorrect.
.1: The system asks for user ID and password again.
.2: If the homeowner/guest enters unregistered user ID or incorrect password three times in a row the system locks itself for a set amount of time.
4a. The homeowner/guest doesn't receive the authentication code in the email
.1: The system offers to send the authentication code to the email again
5a. Authentication code incorrect.
.1: The system asks for the authentication code again
.2: If the homeowner/guest doesn't enter the correct authentication code within the given, the system returns to the login page
6a. 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: Web browser
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?
2. What mechanisms alert the homeowner about the failed login attempts?
3. What mechanisms allow the user to recover the user ID or password if the user forgets it?
4. What mechanisms allow the user to complete the 2-factor authentication without the use of email?

Reference in meeting log 2025.10.28

c. Configure system setting

Use case: Adjust the system's setting
Primary actor: Homeowner
Goal in context: To adjust the system's setting through the web browser
Preconditions: The homeowner has successfully logged into the system — see use case: "Log onto the system through the web browser."
Trigger: The homeowner decides to adjust the system's setting.
Scenario:

1. The homeowner successfully accesses the system on the web browser
2. The homeowner clicks on the button "Configure" on the website
3. The system shows accessible configuration functions on the web browser
4. Homeowner selects a number of settings to adjust.
5. Homeowner modifies the desired configuration values.
6. System validates the new configuration input.
7. System updates configuration and stores changes.
8. System confirms successful update to the homeowner.

Exception:

7a. Invalid configuration inputs
.1: System asks for valid configuration inputs again
8a. System fails to update configuration
.1: System returns an error message and suggest contacting administrator

Priority: High priority, basic functions.
When available: Later increment
Frequency of use: Occasional to frequent
Channel to actor: web browser
Secondary actors: System administrator
Channel to secondary actors:

1. System administrator: PC-based system

Open issues:

1. Should some configuration options require additional authentication?
2. What types of configuration settings will be available in early vs. later releases?
3. Should there be a rollback or "reset to default" option for configuration?
4. What mechanism allows the owner to grant permission to change configuration to guests?

Reference in meeting log 2025.10.28

d. Turn the system on

Use case: Turn the system on through control panel
Primary actor: Homeowner, Guest
Goal in context: To turn the Safehome system on through the control panel
Preconditions: The homeowner has successfully logged into the system — see use case: "Log onto the system through the control panel." The system is currently turned off
Trigger: The homeowner/guest decides to turn on the system.
Scenario:

1. The homeowner/guest presses the "1" button on the control panel
2. Armed indicator light turns on.
3. System transitions turn on and activate fully armed mode.
4. System displays a confirmation message indicating success.

Exception:

9a. A window/door or sensor is triggered/open during arming process

.1: Control panel alerts user of zones preventing arming and system waits for user action:

Priority: High priority, basic functions.
When available: Later 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. Should confirmation be required for bypassed sensors before arming?
2. Should an alert be sent when a guest arms the system?
3. Should a countdown delay be shown before the system fully arms?

Reference in meeting log 2025.10.28

e. Turn the system off

Use case: Turn the system off through control panel
Primary actor: Homeowner, Guest
Goal in context: To turn the Safehome system off through the control panel
Preconditions: The homeowner has successfully logged into the system — see use case: "Log onto the system through the control panel." The system is turned on.
Trigger: The homeowner/guest decides to turn off the system.
Scenario:

1. The homeowner/guest presses the "2" button on the control panel
2. Armed indicator light turns off.
3. System transitions turn on and deactivate fully armed mode.
4. System displays a confirmation message indicating success.

Exception:
10a. A window/door or sensor is triggered/closed during disarming process
.1: Control panel alerts user of zones preventing disarming and system waits for user action

Priority: High priority, basic functions.
When available: Later 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. Should confirmation be required for bypassed sensors before disarming?
2. Should an alert be sent when a guest disarms the system?
3. Should a countdown delay be shown before the system fully disarms?

Reference in meeting log 2025.10.28

f. Reset the system

Use case: Reset the system through control panel
Primary actor: Homeowner, Guest
Goal in context: To reset the Safehome system through the control panel
Preconditions: The homeowner has successfully logged into the system — see use case: "Log onto the system through the control panel." The control panel malfunctions.
Trigger: The homeowner/guest decides to perform a reset of the system.
Scenario:

1. The homeowner/guest presses the "3" button on the control panel
2. System aborts current process and reboots the original interface
3. System resumes normal operation and alerts administrator about error

Exception:
11a. Reset button input not recognized due to severe malfunction
.1: User must contact system administration for advice
Priority: Low priority, basic functions.
When available: Later increment
Frequency of use: Rare
Channel to actor: Control panel
Secondary actors: System administrator
Channel to secondary actors:

1. System administrator: PC-based system

Open issues:

1. Should the system notify the administrator if reset happens repeatedly in a short time?
2. Should reset affect the arming state or continue previous mode?

Reference in meeting log 2025.10.28

g. Change master password through control panel

Use case: Change master password through control panel
Primary actor: Homeowner
Goal in context: To change the Safehome system's master password through the control panel
Preconditions: The homeowner has successfully logged into the system — see use case: "Log onto the system through the control panel." The system is not in the alarm state
Trigger: The homeowner/guest decides to change the master password.
Scenario:

1. The homeowner presses the "9" button on the control panel
2. The control panel screen loads a reset master password screen
3. The homeowner enters a new master password
4. The system validates the new password and returns to the original interface
5. The new master password is updated

Exception:

12a. New password invalid or similar to old password
.1: The system asks for a new password again.
13a. An alarm condition is encountered – see use case: "alarm condition encountered"
Priority: Medium priority, basic functions.
When available: Later increment
Frequency of use: Infrequent
Channel to actor: Control panel
Secondary actors: System administrator
Channel to secondary actors:

1. System administrator: PC-based system

Open issues:

1. Should the system send a notification or log entry each time the master password is changed?
2. Should a timeout cancel the password change if inactive too long?

Reference in meeting log 2025.10.28

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 Armed or Disarmed using physical control panel
Precondition:	- The SafeHome system is powered on and operational.The homeowner has successfully logged into the system — see use case: "Log onto the system through the control panel." The control panel is connected to the sensors (door, window, motion) via wireless network.
Trigger:	The homeowner decides to arm or disarm the system using the control panel buttons

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 presses the Home/Away button on the control panel.
3. The system checks that all required sensors are ready.
4. If all doors and windows are closed, the system changes its state accordingly: Arm: activates sensors and sets system status to Armed. Disarm: deactivates sensors and sets system status to Disarmed.
5. The control panel updates its indicator light under armed:
   Red light ON means the system is *Armed*.Green light ON means the system is *Disarmed*.
6. The system records the event (user ID, time, and action) in the intrusion log — see use case: "View intrusion log."

Exception:

2a. The homeowner presses Arm, but one or more doors or windows are open.
??So??the??control??panel??emits??a??short??beep sound and keeps the previous state (no change).

3a. If a sensor fault or tamper condition is detected, the system notifies the user with a beep pattern and does not arm the system.

1-6. 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:

3. Should the system provide an additional audible confirmation (e.g., a long beep) after successful arming/disarming?

4. What security mechanism prevents unauthorized physical access to the control panel?

5. Should the system record failed arming attempts (e.g., due to open doors)?

Reference in meeting log 2025.10.31

b. Arm/disarm system through web browser

Use case:	Arm/disarm system through web browser
Primary Actor:	Homeowner
Goal in context:	To arm or disarm the SafeHome security system remotely via a PC web browser.
Precondition:	- The system is running. Proper master password must be obtained - The homeowner has valid user ID and passwords and an active, authenticated web session — see use case: "Log onto the system through web browser." - Required security configuration is complete (zones/sensors defined).
Trigger:	The homeowner decides to change the house safety status from web interface.

Scenario:

1. The homeowner logs onto the system through a web browser – see use case: "Log onto the system through web browser."
2. The homeowner selects Security from the major function buttons.
3. The homeowner presses the button to change the safety status.
4. The system checks current sensor/zone readiness (e.g., door/window closed, sensor health).
5. The system activates/deactivates sensors according to Arm/Disarm condition.
6. The web page updates the System Status to "Armed" or "Disarmed" and shows a confirmation message.
7. The system records the event (user ID, mode, timestamp, client IP) in the intrusion/audit log — see use case: "View intrusion log."

Exception:

2a. Security function not configured for this account → display error and guide user to configuration (out of scope here).

4a. The homeowner presses Arm, but one or more doors or windows are open.

??So??the??system??emits??a??message??and??keeps??the??previous??state?? no??change??

4b. Sensor fault/tamper/low-battery/offline , display alert; block arming or allow with limitations depending on policy.

1–7. Alarm condition encountered at any point ,see use case: "Alarm condition encountered." Auth. errors (expired session, invalid credentials) , *see use case:* "Log onto the system through web browser."

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. Should remote arm/disarm require multi-factor authentication (MFA)?
2. Define session timeout and lockout policy for web logins.
3. Should a push notification be sent upon remote arming/disarming?

Reference in meeting log 2025.10.31

c. Arm/disarm safety zone selectively

Use case:	Arm/disarm safety zone selectively
Primary Actor:	Homeowner
Goal in context:	To change the armed status of a specified safety zone
Precondition:	- The system is running and fully configured (zones and sensors defined). - The homeowner has an authenticated session via web browser — see use case: "Log onto the system through web browser."
Trigger:	The homeowner decides to change the armed status of specified safety zone

Scenario:

1. The homeowner logs onto the system through the control panel – see use case: "Log onto the system through control panel" or through web browser – see use case "Log onto the system through web browser".
2. The homeowner presses the security button to enter security service.
3. Entering the security service, the homeowner selects a specific safety zone.
4. The system checks the zone readiness (all doors/windows in that zone closed; sensors healthy).
5. The homeowner presses the Arm/Disarm button of a specified safety zone.
6. The system activates/deactivates sensors according to home/away conditions.
7. The homeowner observes the sidebar where Safety zone status are shown, the text is shown as activated/deactivated for each zone.
8. The system records the action (user ID, zone, action, timestamp, client IP) in the intrusion/audit log — see use case: "View intrusion log."

Exception:

2a. Zone not configured / unknown zone, display error; guide user to "Configure safety zone".

5a. Open devices in the selected zone (door/window open):

- Display a list of open points within the zone; users may Cancel or Bypass those points if policy allows — see use case: "Configure safety zone."
- If bypass is not permitted, block arming and keep prior state.

5b. Sensor fault/tamper/low battery/offline in zone → display alert; block arming or allow with limitations per policy; log the condition.

1–8. Alarm condition encountered at any time, see use case: "Alarm condition encountered." Auth/session errors, see use case: "Log onto the system through web browser."

Priority:	Essential
Frequency of use:	frequent
Channel to actor:	web browser
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. Bypass policy: Are per-sensor bypasses within a zone allowed by end-users, and should bypass auto-restore when the device closes?
2. Authorization: Should guest users be allowed to arm/disarm specific zones?
3. Notifications: Send push/email when a zone is armed/disarmed or when a zone is armed with bypassed points?

Reference in meeting log 2025.10.31

d. Alarm condition encountered

Use case:	Alarm condition encountered
Primary Actor:	Homeowner
Goal in context:	Detect and handle an alarm condition (e.g., breaching a protected point or motion while armed), notify the homeowner, and transition the system to a safe, auditable state.
Precondition:	-System is Armed (Away/Stay) — see use case: "Arm/Disarm system through control panel" or "Arm/Disarm system through web browser." - Relevant safety zones and sensors are configured — see use case: "Configure safety zone."
Trigger:	A protected sensor (door/window/motion) reports an intrusion while armed. A tamper event is detected on a sensor or the control panel.

Scenario:

1. The homeowner logs onto the system through the control panel – see use case: "Log onto the system through control panel."
2. The system enters Alarm state:
   a. Activates siren/buzzer.
   b. Keeps the control panel RED light ON (Armed indicator).
   c. Logs the alarm event (sensor ID, zone, timestamp) — see use case: "View intrusion log."
3. The system issues notifications according to configuration (e.g., call/SMS/push/email).
4. The homeowner attempts to Disarm the system — see use case: "Arm/Disarm system through control panel" or "…through web browser."
5. The system validates credentials and processes the disarm command.
6. If successful, the siren stops, the control panel turns GREEN (Disarmed), and the event is marked "Acknowledged."
7. The system returns to normal monitoring mode and keeps the event record in the intrusion log.

Exception:

2a. If alarm activation fails to trigger siren (hardware fault), the system logs the event as "Siren malfunction" and continues remote notification.

3a. If network connection fails during notification, system retries three times and stores the event for later transmission.

4a. If authentication fails during disarm (wrong password), the system denies disarm and continues the alarm; the homeowner may retry.

5a. If the disarm command times out, repeat Step 4.

6a. If power outage occurs after Step 2, follow fail-safe policy (battery backup if available).

7a. If multiple alarms occur simultaneously, the system handles them sequentially; each logged separately.

Priority:	Essential

Frequency of use:	Occasional
Channel to actor:	control panel/ web browser
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. Should entry delay and alarm duration be configurable per zone?
2. Should notifications be limited to specific channels (call/SMS/push)?
3. Should repeated tamper events trigger escalation to monitoring service?
4. Should system auto-reset alarm after a defined timeout?

Reference in meeting log 2025.10.31

e. Configure safety zone

Use case:	Configure safety zone
Primary Actor:	Homeowner
Goal in context:	Create, edit, or delete a safety zone and assign sensors (door/window/motion) and policies (entry/exit delay, bypass policy) to that zone.
Precondition:	The system is running; the homeowner is authenticated on the web browser — see use case: "Log onto the system through web browser." Sensors are paired and visible to the system (discovered/registered). For editing/deleting: the target zone already exists
Trigger:	The homeowner decides to add a new zone or change the configuration of an existing zone.

Scenario:

1. The homeowner logs onto the system via web browser — see use case: "Log onto the system through web browser."
2. The homeowner navigates to Security , Safety Zones and selects Create Zone (or chooses an existing zone to Edit).
3. The homeowner specifies Zone Name and Zone Type (e.g., Perimeter, Interior, Entry/Exit).
4. The homeowner assigns sensors to the zone (select from discovered sensors list; door/window/motion).
5. The homeowner configures policies for the zone:
   5.1 Entry Delay (e.g., 0–120 s) and Exit Delay (e.g., 0–120 s) if applicable.
   5.2 Bypass Policy (Allow/Disallow per-sensor bypass when arming).
   5.3 Tamper Handling (Alarm immediately vs. mark as trouble).
6. The homeowner selects Save.
7. The system validates the configuration (name uniqueness, sensor conflicts, policy ranges).
8. If valid, the system persists the zone configuration and updates internal mappings.
9. The UI shows confirmation ("Zone saved") and updated Zone Status (e.g., Idle/Ready/Bypassed).
10. The system writes an administrative event to the audit/intrusion log (user, zone, action, timestamp) — see use case: "View intrusion log."

Exception:

2a. Zone not found when attempting to edit/delete : display error and return to Step
3a. Zone name empty/duplicate : prompt to change name and return to Step 3.
4a. No sensors selected for a zone type that requires them (e.g., Perimeter) : display warning and return to Step 4.
4b. Sensor already assigned to another mutually-exclusive zone (policy conflict) : show conflict list and let user reassign; return to Step 4.

5a. Invalid policy values (e.g., delay out of range) highlight fields; return to Step 5.

7a. Validation fails (combined constraints, e.g., Entry Delay set for a non-entry zone) show details; return to Step 5.

8a. Persistence error (storage/network): display error and allow Retry; if retried, repeat Step 6–8.

10a. Log write failure: queue the log entry and show soft warning; continue (no user re-action needed).

Priority:	Essential
Frequency of use:	Occasional
Channel to actor:	Web browser
Secondary actor:	System administrator, Sensors (door, window and motion detection)

Channels to secondary actors:

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

Open issues:

1. Authorization: Should zone configuration require an administrator role distinct from normal homeowner login?
2. Conflicts: Define rules when a sensor appears in multiple zones (priority vs. prohibition).
3. Defaults & Templates: Provide starter templates (Perimeter, Interior, Entry/Exit) to simplify setup?
4. Auto-restore: If a sensor is bypassed during arming, should it auto-restore to be active when it closes?
5. Localization: Zone names and messages — multi-language support?

Reference in meeting log 2025.10.31

f. Create new safety zone

Use case:	Create New Safety Zone
Primary Actor:	Homeowner
Goal in context:	To create a new safety zone and assign sensors to define which areas of the house will be monitored by the SafeHome system
Precondition:	The system is running., The homeowner is logged in via the web browser — see use case: "Log onto the system through web browser.". Sensors have been paired and are available for assignment.
Trigger:	The homeowner decides to create a new safety zone for part of the home

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 Security: Safety Zones and selects Create New Zone.
3. The system displays a blank zone configuration form.
4. The homeowner enters a Zone Name (e.g., "Garage Zone") and selects a Zone Type (Perimeter, Interior, Entry/Exit).
5. The homeowner assigns available sensors (door/window/motion) to this new zone.
6. The homeowner defines zone policies:
   6.1. Entry delay time (if applicable).
   6.2. Exit delay time (if applicable).
   6.3. Bypass permission (allow/disallow bypass during arming).
   6.4. Tamper handling (alarm immediately or mark as trouble).
7. The homeowner clicks Save to confirm the new zone creation.
8. The system validates the zone details (unique name, valid sensors, non-conflicting assignments).
9. If validation passes, the system stores the new zone configuration.
10. The system displays a confirmation message: "Zone created successfully."
11. The system records the event (user, timestamp, zone name) in the audit/intrusion log — see use case: "View intrusion log."

Exception:

4a. Duplicate or empty zone name detected :system displays error and prompts for correction; return to Step 4.

5a. No sensors selected : system warns "Zone must include at least one sensor" and returns to Step 5.

6a. Invalid delay/policy values (e.g., negative delay, unsupported type) : highlight invalid fields; return to Step 6.

8a. Validation failure (e.g., assigned sensor already belongs to another conflicting zone) : display list of conflicts; user may cancel or reassign sensors; return to Step 5.

9a. Database/network error during save : show retry option; repeat Step 7–9.

11a. Log write error : queue the entry for later retry (non-blocking).

Priority: Essential

Frequency of use:	Occasional
Channel to actor:	Web browser
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. Should users be allowed to clone or duplicate existing zones as templates?
2. Should the system auto-create “Default Zone” on first setup?
3. How should the interface handle partially paired sensors (offline during setup)?
4. Should newly created zones be armed automatically after saving?

Reference in meeting log 2025.10.31

g. Delete safety zone

Use case:	Delete safety zone
Primary Actor:	Homeowner
Goal in context:	To remove an existing safety zone from the SafeHome system, including its configuration and assigned sensors.
Precondition:	-The system is running. -The homeowner is logged into the system through the web browser, see use case: "Log onto the system through web browser". -The safety zone to be deleted already exists
Trigger:	The homeowner decides to delete an existing safety zone.

Scenario:

1. Homeowner logs in via web browser, see use case: "Log onto the system through web browser".
2. Navigates to Security and Safety Zones.
3. Selects a zone and clicks Delete.
4. The system asks for confirmation.
5. The homeowner confirms the change.
6. System removes the zone, unassigns sensors, updates the list, and logs the event, see use case: "View intrusion log".

Exception:

3a. Zone not found, show error and return to list.
4a. Homeowner cancels, no deletion occurs.
6a. Database/network error, show retry option.

Priority:	Essential
Frequency of use:	Occasional
Channel to actor:	Web browser
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. Prevent deletion when the zone is armed?
2. Need a recovery option (soft delete)?
3. Should confirmation email be sent?

Reference in meeting log 2025.10.31

h. Update an exist safety zone

Use case:	Update an Existing Safety Zone
Primary Actor:	Homeowner
Goal in context:	To modify the configuration of an existing safety zone, including its name, assigned sensors, or zone policies.
Precondition:	The system is running, the homeowner is logged in via the web browser, see use case: "Log onto the system through web browser", At least one safety zone already exists.
Trigger:	The homeowner decides to edit the settings of an existing safety zone.

Scenario:

1. The homeowner logs onto the system through the control panel – see use case: “Log onto the system through control panel.”
2. Navigates to Security and Safety Zones and selects a zone to edit.
3. The system displays current zone configuration.
4. Homeowners update information such as zone name, sensor assignments, or delay policies.
5. The homeowner clicks Save.
6. The system validates the changes, updates the database, and confirms with the message “Zone updated successfully.”
7. System records the update event in the audit/intrusion log, see use case: "View intrusion log".

Exception:

3a. Zone not found : show “Zone not found” and return to list.

4a. Invalid values or duplicate name : display error and return to Step 4.

6a. Database/network error : show retry option.

Priority:	Essential
Frequency of use:	Occasional
Channel to actor:	Web browser
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. Should editing be restricted while the zone is armed?
2. Should old configurations be saved for rollback?

Reference in meeting log 2025.10.31

i. Configure Safehome modes

Use case:	Configure Safehome modes
Primary Actor:	Homeowner
Goal in context:	To select and customize one of the five security modes (Home, Away, Overnight Travel, Extended Travel, or Guest Home) based on occupancy and security needs
Precondition:	The SafeHome system is powered on and operational; The homeowner has successfully logged into the system — see use case: "Log onto the system through the control panel" or "Log onto the system through web interface."; Smart lighting and HVAC systems are connected to the SafeHome system (for travel modes).
Trigger:	The homeowner decides to change the security mode to match current or planned occupancy status

Scenario:

1. The homeowner logs onto the system — see use case: "Log onto the system through control panel" or "Log onto the system through web interface."
2. The homeowner navigates to the "Security Modes" menu.
3. The system displays the five available modes with brief descriptions:
    1. Home Mode: Perimeter sensors active (doors, windows), interior motion sensors inactive
    2. Away Mode: All sensors active (perimeter and interior motion)
    3. Overnight Travel Mode: All sensors active, automated lighting simulation, HVAC control enabled
    4. Extended Travel Mode: All sensors active, automated lighting simulation, HVAC energy-saving mode, additional notifications enabled
    5. Guest Home Mode: Perimeter sensors active, selected interior motion sensors inactive, reduced alarm sensitivity
4. The homeowner selects the desired mode.
5. If Overnight Travel or Extended Travel mode is selected:
    1. The system prompts the homeowner to configure or confirm lighting automation settings (random on/off intervals between 6:00 PM - 11:00 PM).
    2. The system prompts the homeowner to set HVAC parameters (target temperature range or energy-saving settings).
6. If Guest Home mode is selected, the system prompts the homeowner to specify which interior zones should have motion sensors disabled.
7. The system validates all sensor connections and settings for the selected mode.
8. The system activates the selected mode and updates sensor states accordingly.
9. The control panel displays the current mode name and corresponding indicator light.
10. The system records the mode change event (user ID, timestamp, and mode selected) in the intrusion log — see use case: "View intrusion log."
11. If travel mode is activated, the system sends a confirmation notification to the homeowner's registered mobile device or email.

Exception:

5a. The homeowner selects a travel mode but smart lighting system is not connected or unavailable.- The system displays warning: "Lighting automation unavailable. Continue without lighting control?" and waits for confirmation.

5b. The homeowner selects a travel mode but HVAC system is not connected or unavailable.- The system displays warning: "HVAC control unavailable. Continue without climate control?" and waits for confirmation.

7a. One or more sensors required for the selected mode are offline or malfunctioning.- The system displays error: "Sensor fault detected in [zone name]. Cannot activate [mode name]." The system remains in current mode.

7b. A door or window is open when attempting to activate Away, Overnight Travel, or Extended Travel mode.- The control panel emits a beep and displays: "Secure all entry points before activating this mode." The system remains in current mode.

1-11. An alarm condition is encountered – see use case: “alarm condition encountered.”

Priority:	Essential
Frequency of use:	Frequent (Home/Away modes), Occasional (Travel and Guest modes)
Channel to actor:	control panel, web interface, mobile application
Secondary actor:	System administrator, Sensors (door, window, motion), Smart lighting system, HVAC system

Channels to secondary actors:

1. System administrator: PC-based system
2. Sensors: Wireless connectivity
3. Smart lighting system: Home automation network (Z-Wave, Zigbee, or Wi-Fi)
4. HVAC system: Home automation network or direct API connection

Open issues:

1. Should mode changes require additional authentication (e.g., PIN verification) for security-critical transitions like Away to Home?
2. Should the system support scheduling automatic mode changes (e.g., switch to Away mode every weekday at 8:00 AM)?
3. What is the maximum duration for Extended Travel mode before requiring re-authentication?
4. Should Guest Home mode allow guests to have limited control through a temporary access code?
5. How should the system handle mode conflicts when multiple users attempt to change modes simultaneously?
6. Should travel modes automatically adjust based on weather forecasts (e.g., increase HVAC usage during extreme temperatures)?

Reference in meeting log 2025.10.29

j. View intrusion log

Use case:	View intrusion log
Primary Actor:	Homeowner
Goal in context:	To review recorded security events and system activities through the control panel or web interface
Precondition:	The SafeHome system is powered on and operational; The homeowner has successfully logged into the system — see use case: "Log onto the system through the control panel" or "Log onto the system through web interface."; The intrusion log contains at least one recorded event.
Trigger:	The homeowner selects the option to view the intrusion log from the control panel menu or web interface

Scenario:

1. The homeowner logs onto the system — see use case: "Log onto the system through control panel" or "Log onto the system through web interface."
2. The homeowner navigates to the "View Log" or "Event History" option.
3. The system retrieves the intrusion log from storage.
4. The system displays a list of recorded events in reverse chronological order (most recent first), showing:
    1. Event type (arm, disarm, alarm triggered, sensor fault, etc.)
    2. Date and timestamp
    3. User ID (if applicable)
    4. Affected sensor or zone (if applicable)
    5. Event outcome (successful, failed, etc.)
5. The homeowner scrolls through the log entries to review the events.
6. The homeowner can optionally filter events by:
    1. Date range
    2. Event type
    3. Specific sensor or zone
7. The homeowner exits the log view and returns to the main menu.

Exception:

3a. The intrusion log is empty (no events recorded). - The system displays message: "No events to display" and returns to the main menu.

3b. The system cannot retrieve the log due to storage failure. - The system displays error message: "Unable to access event log" and alerts the system administrator.

4a. The log contains more entries than can be displayed on one screen. - The system provides pagination or scrolling functionality to navigate through all entries.

1-7. An alarm condition is encountered – see use case: “alarm condition encountered.”

Priority:	Essential
Frequency of use:	Moderate
Channel to actor:	control panel, web interface
Secondary actor:	System administrator

Channels to secondary actors: PC-based system

Open issues:

1. How long should event logs be retained before automatic deletion or archiving?
2. Should the system allow exporting log data to external formats (CSV, PDF) for

record-keeping?

3. What level of detail should be shown to homeowners versus system administrators?
4. Should the system send automatic notifications when certain critical events are logged (e.g., multiple failed login attempts)?

Reference in meeting log 2025.10.29

k. Call monitoring service through control panel

Use case:	Call monitoring service through control panel
Primary Actor:	Homeowner
Goal in context:	To immediately contact the monitoring service in emergency situations using the panic button on the control panel
Precondition:	- The SafeHome system is powered on and operational. - The control panel is connected to the monitoring service via phone line or internet connection. - Monitoring service contact information is configured in the System. - NO LOGIN OR PASSWORD REQUIRED - panic button works immediately for safety.
Trigger:	The homeowner presses the panic button on the control panel during an emergency situation.

Scenario:

1. The homeowner presses the panic button on the control panel (no login required - works immediately).
2. The system immediately activates emergency mode.
3. The control panel displays "EMERGENCY - Calling Monitoring Service" in red with flashing indicator.
4. The system emits a distinctive alert tone to confirm panic button activation.
5. The system establishes priority connection with the monitoring service.
6. The system transmits emergency signal along with homeowner identification, account information, and location.
7. The monitoring service receives the emergency signal and prioritizes the call.
8. The monitoring service answers the call immediately.
9. The control panel activates the speaker and microphone for two-way communication.
10. The homeowner communicates the emergency situation to the monitoring service representative.
11. The monitoring service takes appropriate action (dispatch police, fire, medical services as needed).
12. The system automatically arms all sensors and activates all cameras if not already active.
13. The homeowner or monitoring service representative ends the call when appropriate.
14. The system terminates the connection.
15. The control panel displays "Emergency Call Ended - System Remains in Alert Mode"
16. The system records the event (time, duration, call status, and emergency type) in the intrusion log — see use case: "View intrusion log."

Exception:

5a. The system fails to establish connection with the monitoring service due to network or phone line issues:

- The control panel displays "EMERGENCY CONNECTION FAILED" with continuous alarm beep.

- The system attempts to use backup communication method (cellular, alternate phone line).
- The system sends emergency SMS/text message to monitoring service and backup contacts if voice connection fails.
- The system continues retry attempts every 30 seconds until connection is established.

6a. The system's account information cannot be transmitted due to communication error.
- The monitoring service answers as emergency call with unknown caller.
- The homeowner provides verbal identification and location information.

8a. The monitoring service does not answer within 30 seconds (shorter timeout for emergency).
- The system automatically calls backup emergency contact numbers sequentially.
- The system continues attempting to reach monitoring service in parallel.
- The control panel displays "Calling Backup Contact" with contact name.

9a. Connection is lost during the emergency call due to network interruption.
- The control panel displays "CONNECTION LOST - Reconnecting" with flashing red indicator.
- The system immediately attempts to reconnect with highest priority.
- The system continues retry attempts every 15 seconds.
- The system sends emergency SMS notification about disconnection to monitoring service.

1a. The homeowner accidentally presses the panic button.
- The homeowner can press "Cancel Emergency" button within 10 seconds to abort the call.
- The system prompts for confirmation: "Cancel Emergency Call? Press OK to confirm or wait to proceed."
- If confirmed, the system cancels the emergency call and logs the cancellation.
- If not cancelled within 10 seconds, the system proceeds with emergency call to monitoring service.

13a. The homeowner is unable to speak or communicate during the call.
- The monitoring service follows silent emergency protocol (assumes emergency in progress).
- The monitoring service dispatches emergency services to the location immediately.
- The system keeps the line open for monitoring service to listen to ambient sounds.

1-16. An alarm condition is encountered – see use case: “alarm condition encountered.”

Priority:	Critical
Frequency of use:	Rare (emergency situations only)
Channel to actor:	control panel panic button
Secondary actor:	Monitoring service, Emergency services (police, fire, medical), System administrator, Communication network, Backup emergency contacts

Channels to secondary actors:

1. Monitoring service: phone line or internet connection (primary), cellular network (backup)
2. Emergency services: dispatched by monitoring service
3. System administrator: PC-based system
4. Communication network: wireless/wired connectivity
5. Backup emergency contacts: phone, SMS

Open issues:

1. Should the panic button require a specific press pattern (e.g., hold for 3 seconds) to prevent accidental activation?
2. Should there be different panic buttons for different emergency types (medical, fire, intrusion)?
3. What happens if multiple panic buttons are pressed simultaneously from different control panels?
4. Should the system automatically unlock doors for emergency responders?
5. Will the system provide visual or audio countdown during the cancellation window?
6. Should the system activate external sirens or alarms when panic button is pressed?
7. How long should the system remain in alert mode after an emergency call?
8. Should the system require explicit disarming after a panic call or remain armed?
9. Will the system capture and transmit audio/video from cameras to monitoring service during panic calls?
10. Should there be a silent panic option that doesn't emit any sounds?

Reference in meeting log 2025.10.29

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 specific 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 are 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:

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

Open Issues:

1. Will system response via the Internet be acceptable given the bandwidth required

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

b. Pan/Zoom specific camera view [Don't follow Fig 6 yet]

Use Case:	Pan/Zoom specific camera view
Primary actor:	Homeowner
Goal In Context:	To adjust the viewing angle and zoom level of a specific camera's live view
Preconditions:	System should be ready, and internet should be set; The specific camera needs to be enabled. If there is password for specific camera, correct password must be obtained from user first; User has to be able to see the default view of specific camera.
Trigger:	Homeowner decides to adjust the camera angle or zoom level while viewing live feed.

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.
12. The system displays pan control scroll bar (horizontal) for left-right movement.
13. The system displays zoom control scroll bar (vertical) for zoom in/out adjustment.
14. The homeowner adjusts the pan scroll bar to move camera view left or right.
15. The system sends pan command to the camera with the specified angle.
16. The camera adjusts its position accordingly.
17. The system updates the live view to reflect the new camera angle.
18. The homeowner adjusts the zoom scroll bar to zoom in or out.
19. The system sends zoom command to the camera with the specified zoom level.
20. The camera adjusts its zoom level accordingly.
21. The system updates the live view to reflect the new zoom level.
22. The system displays current pan position and zoom level indicators.

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 prevents the homeowner from accessing the camera.
10a. If the camera is disabled, "view" button is disabled – see use case: "Enable camera"
12a. Selected camera does not support pan functionality - pan scroll bar is disabled or hidden with message "Pan not supported"
13a. Selected camera does not support zoom functionality - zoom scroll bar is disabled or hidden with message "Zoom not supported"
14a. Pan scroll bar adjusted beyond camera's physical limits - system constrains movement to maximum left/right range and displays current limit.
14b. Homeowner doesn't adjust pan/zoom scroll bar - The system displays the current viewing window.
15a. Communication with camera fails during pan command - system displays error message "Unable to send pan command" and maintains previous position.
16a. Camera fails to respond to pan command - system retries command up to three times, displays error message if unsuccessful, and logs the issue.
16b. Camera mechanical failure prevents panning - system displays error message "Camera movement error" and suggests contacting support; see use case: "Report camera malfunction"
18a. Zoom scroll bar adjusted beyond camera's zoom limits - system constrains zoom to minimum/maximum zoom range and displays current limit.
19a. Communication with camera fails during zoom command - system displays error message "Unable to send zoom command" and maintains previous zoom level.
20a. Camera fails to respond to zoom command - system retries command up to three times, displays error message if unsuccessful, and logs the issue.
20b. Camera optical failure prevents zooming - system displays error message "Camera zoom error" and suggests contacting support; see use case: "Report camera malfunction"
22a. Homeowner selects "reset view" button - system returns camera to default pan position and zoom level; see use case: "Reset camera view to default"

1-22. 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:

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

Open Issues:

1. Will system response via the Internet be acceptable to get all input buttons?
2. If the homeowner wants to return to the floor plan page or thumbnail page, will the camera stay at this new view or return to the previous view?
3. What if a specific camera is broken?

4. What if a new view of the camera is not loaded?
5. Will there be preset positions that homeowners can save and quickly return to?
6. How quickly should the camera respond to scroll bar adjustments?
7. Should continuous scrolling result in smooth camera movement or step-by-step adjustments?
8. Will there be numerical indicators showing exact pan angle and zoom percentage?
9. Should there be keyboard shortcuts or arrow keys for pan/zoom control?
10. How will the system handle latency between command and camera response over slow connections?
11. Should pan and zoom be lockable to prevent accidental adjustments?
12. Will the system support digital zoom in addition to optical zoom?

Reference in SEPA dialog slide: slide 80, Applying Patterns

c. Begin camera recording

Use Case:	Begin camera recording
Primary actor:	Homeowner
Goal In Context:	To start recording video from a specific camera
Preconditions:	System should be ready, and internet should be set; appropriate user ID and passwords must be obtained; camera must be enabled and functioning.
Trigger:	Homeowner decides to record video from 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 "begin" button in the recording side panel to start recording.
11. The system checks available storage space.
12. The system initiates recording and displays a recording indicator.
13. The system displays the current recording duration.
14. The homeowner selects "stop" button when finished.
15. The system stops recording and saves the video file.
16. The system displays confirmation message with file name and storage location.

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 are remain? The system prevent the homeowner from accessing the camera .

10a. If the camera is disabled, “begin” button is disabled – see use case : “Enable camera”

11a. Insufficient storage space available - system displays error message and prompts homeowner to free up space or change storage settings; see use case: "Manage storage settings"

12a. Recording fails to initiate due to camera malfunction - system displays error message and logs the issue; see use case: "Report camera malfunction"

14a. Connection lost during recording - system automatically saves recorded content up to disconnection point and notifies homeowner upon reconnection.

14b. Homeowner closes browser or logs out without stopping recording - system continues recording for predefined maximum duration then auto-stops and saves file.

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

When available: First increment

Frequency of use: Several times per week

Channel to actor: PC-based system with web browser

Secondary actor: Support technician, Webmaster, Camera, Storage Server

Channels to secondary actors:

1. Support technician: phone line.
2. Webmaster: E-mail.
3. Camera: wireless connectivity
4. Storage Server: network connection

Open Issues:

1. What is the maximum recording duration allowed per session?
2. What video quality/resolution settings will be available for recording?
3. How will the system handle concurrent recording requests from multiple cameras?
4. What happens if storage fills up during an active recording session?
5. Will recordings be stored locally, on cloud storage, or both?
6. What file format will be used for saved recordings?
7. How long will recorded videos be retained before automatic deletion?

Reference in meeting log 2025.10.29

d. Stop camera recording

Use Case:	Stop camera recording
Primary actor:	Homeowner
Goal In Context:	To stop recording video from a specific camera
Preconditions:	System should be ready, and internet should be set; appropriate user ID and passwords must be obtained; camera must be currently recording.
Trigger:	Homeowner decides to stop recording video from 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 with recording indicator active.
10. The homeowner selects the "stop" button to end recording.
11. The system stops the recording process.
12. The system saves the recorded video file to designated storage location.
13. The system generates a unique file name with timestamp.
14. The system displays confirmation message showing file name, duration, size, and storage location.
15. The system updates the camera state to show recording has stopped.

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)

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 are remain? The system prevent the homeowner from accessing the camera .

9a. Selected camera is not currently recording - "stop" button is disabled; see use case: "Begin camera recording"

11a. Connection lost before stop command is received - system continues recording until connection is restored or maximum duration is reached, then auto-saves.

12a. File save fails due to storage error - system displays error message, attempts to save to alternate location, and notifies homeowner; see use case: "Manage storage settings"

12b. File save fails due to corrupted data - system displays error message indicating

partial or no video could be saved and logs the error.

13a. File naming conflict occurs - system appends additional identifier to ensure unique file name.

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

When available: First increment

Frequency of use: Several times per week

Channel to actor: PC-based system with web browser

Secondary actor: Support technician, Webmaster, Camera, Storage Server

Channels to secondary actors:

1. Support technician: phone line.
2. Webmaster: E-mail.
3. Camera: wireless connectivity
4. Storage Server: network connection

Open Issues:

1. What happens if the homeowner navigates away from the page while recording is in progress?
2. Should there be a confirmation dialog before stopping to prevent accidental stops?
3. Will the system allow immediate playback of the just-recorded video?
4. How will the system handle multiple users trying to stop the same recording simultaneously?
5. What metadata will be stored with the video file (timestamp, camera ID, duration, etc.)?
6. Should the system send a notification when recording is stopped?

Reference in meeting log 2025.10.29

e. Replay camera recording

Use Case:	Replay camera recording
Primary actor:	Homeowner
Goal In Context:	To view a previously recorded video from a specific camera
Preconditions:	System should be ready, and internet should be set; appropriate user ID and passwords must be obtained; recorded video files must exist in storage for the selected camera.
Trigger:	Homeowner decides to replay a previously recorded video from 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 "show" button to view recording.
11. The system displays a list of available recorded videos for the selected camera with details (date, time, duration, file size).
12. The homeowner selects a specific recording from the list.
13. The system retrieves the selected video file from storage.
14. The system displays the recorded video within the viewing window.
15. The system provides playback controls (play, pause, stop, forward, rewind, speed control).
16. The homeowner uses playback controls to view the recording.
17. The homeowner closes the playback window when finished viewing.

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)

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 are remain? The system prevent the homeowner from accessing the camera .

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

11a. No recorded videos available for the selected camera - system displays message "No recordings found for this camera" and prompts homeowner to begin recording; see use case: "Begin camera recording"

11b. Homeowner applies filters (date range, duration) - system displays filtered list of

recordings.

13a. Video file not found or has been deleted - system displays error message "Recording file not available" and updates the recording list.

13b. Video file is corrupted or cannot be loaded - system displays error message and offers option to download file for recovery attempts.

14a. Insufficient bandwidth for smooth playback - system adjusts playback quality or buffers video before playing.

14b. Playback fails due to unsupported codec or format - system displays error message and suggests alternative viewing options or file conversion.

15a. Homeowner selects download option - system initiates download of the video file to local storage; see use case: "Download camera recording"

15b. Homeowner selects delete option - system prompts for confirmation before deleting; see use case: "Delete camera recording"

1-17. An alarm condition is encountered - see use case: "alarm condition encountered."

When available: First increment

Frequency of use: Several times per week

Channel to actor: PC-based system with web browser

Secondary actor: Support technician, Webmaster, Camera, Storage Server

Channels to secondary actors:

1. Support technician: phone line.
2. Webmaster: E-mail.
3. Camera: wireless connectivity
4. Storage Server: network connection

Open Issues:

1. What video formats will be supported for playback?
2. Will the system support frame-by-frame navigation for detailed viewing?
3. Should the system allow creating clips or snapshots from recorded videos?
4. Will there be a thumbnail preview or timeline scrubbing capability?
5. How will the system handle playback of very large video files?
6. Should multiple recordings be playable simultaneously in split-screen view?
7. Will playback speed adjustment be available (slow motion, fast forward)?
8. Should the system track which recordings have been viewed?
9. What is the maximum number of recordings that can be stored per camera?

Reference in meeting log 2025.10.29

f. Set camera password

Use Case:	Set camera password
Primary actor:	Homeowner
Goal In Context:	To assign or change a password for a specific camera to restrict unauthorized access
Preconditions:	System should be ready, and internet should be set; appropriate user ID and passwords must be obtained; homeowner must have administrative privileges for camera settings.
Trigger:	Homeowner decides to set or change a password for 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 "SET" button from password panel to set camera password.
11. The system displays password setting dialog box.
12. The homeowner enters a new password for the camera in 4 digits number.
13. The homeowner confirms the new password by re-entering it.
14. The system validates that both password entries match.
15. The system saves the new camera password.
16. The system displays confirmation message "Camera password set successfully"
17. The system updates the camera icon to indicate password protection is active.

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)

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 are remain? The system prevent the homeowner from accessing the camera .

12a. Homeowner cancels password setting - system closes dialog box and returns to camera state display without changes.

14a. Password entries do not match - system displays error message "Passwords do not match. Please re-enter" and prompts homeowner to enter passwords again.

14b. After three failed matching attempts - system cancels password setting operation and returns to camera state display.

15a. System fails to save password - system displays error message "Unable to save password. Please try again" and logs the error.

1-17. An alarm condition is encountered - see use case: "alarm condition encountered."

When available: First increment

Frequency of use: Few times per month

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. Should the system enforce password expiration and require periodic changes?
2. Will there be a password recovery mechanism if the homeowner forgets the camera password?
3. Should the system maintain a history of previous passwords to prevent reuse?
4. Can different users have different passwords for the same camera?
5. Should the system log all password change attempts for security audit?
6. Will there be a master password that can override individual camera passwords?

Reference in meeting log 2025.10.29

g. Delete camera password

Use Case:	Delete camera password
Primary actor:	Homeowner
Goal In Context:	To remove password protection from a specific camera to allow unrestricted access
Preconditions:	System should be ready, and internet should be set; appropriate user ID and passwords must be obtained; homeowner must have administrative privileges; camera must currently have a password set.
Trigger:	Homeowner decides to remove password protection from 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 "DELETE" button from password panel to delete camera password.
11. The system prompts for the current camera password.
12. The homeowner enters the current camera password.
13. The system validates the camera password.
14. The system displays confirmation dialog "Remove password protection from this camera? This will allow unrestricted access."
15. The homeowner confirms the deletion.
16. The system removes the camera password from storage.
17. The system displays confirmation message "Camera password deleted successfully"
18. The system updates the camera icon to indicate password protection is removed.

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)

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 are remain? The system prevent the homeowner from accessing the camera .

10a. Camera does not have a password - "DELETE" button is disabled or displays

message "No password set for this camera"

12a. Homeowner cancels password deletion - system closes dialog box and returns to camera state display without changes.

13a. The camera password is incorrect or not recognized - if input tries are less than three then prompts for reentry. Otherwise cancels deletion operation.

13b. The camera password is incorrect or not recognized and no input tries remain - The system cancels the password deletion operation and returns to camera state display.

15a. Homeowner cancels the confirmation - system returns to camera state display without deleting the password.

16a. System fails to delete password - system displays error message "Unable to delete password. Please try again" and logs the error.

1-18. An alarm condition is encountered - see use case: "alarm condition encountered."

When available: First increment
Frequency of use: Few times per month
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. Should there be a waiting period or additional confirmation before password deletion takes effect?
2. Will the system send notifications to all authorized users when a camera password is deleted?
3. Should the system log all password deletion attempts for security audit?
4. Can password deletion be restricted to certain user roles or require multiple authorizations?
5. Should there be a recovery period during which deleted passwords can be restored?
6. What happens to scheduled recordings or other automated features when password is deleted?
7. Should the system warn about security implications of removing password protection?

Reference in meeting log 2025.10.29

h. View thumbnail Shots

Use Case:	View thumbnail shots
Primary actor:	Homeowner
Goal In Context:	To view thumbnail snapshots from all cameras simultaneously in a grid layout
Preconditions:	System should be ready, and internet should be set; appropriate user ID and passwords must be obtained; at least one camera must be configured in the system.
Trigger:	Homeowner decides to view thumbnails from all 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 “all cameras”
4. The system retrieves the list of all configured cameras.
5. The system displays a grid layout with thumbnail windows for each camera.
6. The system displays thumbnails only for cameras that are enabled and not password-protected.
7. The system shows camera names or labels below each thumbnail.
8. The system updates each thumbnail with a snapshot at one frame per second.
9. The system displays the status of each camera (enabled, disabled, password-protected) on the thumbnail.
10. The homeowner views the thumbnail grid to monitor multiple cameras.
11. The homeowner selects a specific camera thumbnail by clicking on it.
12. The system asks for password if the selected camera has a password.
13. The homeowner enters the password.
14. The system validates the password.
15. The system transitions to the full view page for the selected camera - see use case: "Display Specific camera view"

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)

4a. No cameras configured in the system - system displays message "No cameras available" and prompts to configure cameras.

6a. All cameras are disabled - system displays message "All cameras are currently disabled" with thumbnails showing disabled status.

6b. All cameras are password-protected - system displays thumbnails with lock icons and camera names, but no live snapshots.

6c. Camera is password-protected - system displays thumbnail with lock icon overlay and camera name, but no live snapshot until password is entered.

6d. Camera is disabled - system displays greyed-out thumbnail with "Disabled" label and no live snapshot.

8a. Camera fails to provide snapshot - system displays error icon or "No signal" message in the thumbnail for that camera.

8b. Insufficient bandwidth for multiple camera feeds - system reduces update frequency

or displays lower quality thumbnails with notification "Limited bandwidth - reduced quality"

9a. Camera connection lost - system displays "Connection lost" message on the affected thumbnail and attempts to reconnect.

12a. Selected camera does not have a password - go to procedure 15.

14a. The password is incorrect or not recognized - if input tries are less than three then prompts for reentry. Otherwise returns to thumbnail view.

14b. The password is incorrect or not recognized and no input tries remain - The system returns to thumbnail view without accessing the camera.

11a. Homeowner selects "enable" option from thumbnail context menu for a disabled camera - see use case: "Enable camera"

11b. Homeowner right-clicks on thumbnail to access camera options menu (enable, disable, set password, delete password) - system displays context menu with available options based on camera status.

1-15. 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:

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

Open Issues:

1. What is the maximum number of camera thumbnails that can be displayed simultaneously?
2. Will the thumbnail grid layout be fixed or dynamically adjust based on number of cameras?
3. Should the homeowner be able to customize thumbnail size or grid arrangement?
4. Will there be filtering options to show only enabled cameras or cameras from specific locations?
5. Should the system highlight thumbnails when motion is detected?
6. Will there be a full-screen mode for the thumbnail grid?
7. Can the homeowner initiate recording directly from the thumbnail view?
8. Should thumbnail refresh rate be adjustable to conserve bandwidth?
9. Will the system remember the last viewed layout preferences?
10. Should there be an option to sort thumbnails by camera name, location, or priority?

Reference in SEPA dialog slide: slide 31, Developing Another Preliminary User Scenario

i. Enable camera

Use Case:	Enable camera
Primary actor:	Homeowner
Goal In Context:	To activate a disabled camera for viewing and recording
Preconditions:	System should be ready, and internet should be set; appropriate user ID and passwords must be obtained; camera must be currently disabled.
Trigger:	Homeowner decides to enable a disabled 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 showing disabled status.
10. The homeowner selects the "enable/disable" button to enable the camera.
11. The system prompts for confirmation to enable the camera.
12. The homeowner confirms the action.
13. The system sends activation command to the camera.
14. The camera responds with acknowledgment.
15. The system updates the camera state to enabled.
16. The system displays confirmation message "Camera enabled successfully"
17. The system updates the camera icon on the floor plan to show enabled status.
18. The "view", "begin", and "show" buttons become active.

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)

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 are remain? The system prevent the homeowner from accessing the camera .

9a. Camera is already enabled - "enable/disable" button shows "disable" option instead; see use case: "Disable camera"

12a. Homeowner cancels the action - system returns to camera state display without changes.

13a. Communication with camera fails - system displays error message "Unable to communicate with camera" and suggests checking camera connectivity.

14a. Camera fails to respond or acknowledge - system retries command up to three

times, then displays error message and logs the issue; see use case: "Report camera malfunction"

14b. Camera responds with error status - system displays specific error message and suggests troubleshooting steps or contacting support.

1-18. An alarm condition is encountered - see use case: "alarm condition encountered."

When available: First increment
Frequency of use: Few times per week
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. Should there be different privilege levels for enabling/disabling cameras?
2. Will the system log all enable/disable actions for audit purposes?
3. Should the system send notifications when cameras are enabled?
4. How long should the system wait for camera acknowledgment before timing out?
5. Can multiple cameras be enabled simultaneously?
6. Should there be a schedule feature to automatically enable cameras at certain times?

Reference in meeting log 2025.10.29

j. Disable camera

Use Case:	Disable camera
Primary actor:	Homeowner
Goal In Context:	To deactivate an enabled camera to stop viewing and recording capabilities
Preconditions:	System should be ready, and internet should be set; appropriate user ID and passwords must be obtained; camera must be currently enabled.
Trigger:	Homeowner decides to disable an enabled 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 showing enabled status.
10. The homeowner selects the "enable/disable" button to disable the camera.
11. The system prompts for confirmation to disable the camera.
12. The homeowner confirms the action.
13. The system checks if camera is currently recording.
14. The system stops any active recording - see use case: "Stop camera recording"
15. The system sends deactivation command to the camera.
16. The camera responds with acknowledgment.
17. The system updates the camera state to disabled.
18. The system displays confirmation message "Camera disabled successfully"
19. The system updates the camera icon on the floor plan to show disabled status.
20. The "view", "begin", and "show" buttons become inactive (greyed out).

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)

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 are remain? The system prevent the homeowner from accessing the camera .

9a. Camera is already disabled - "enable/disable" button shows "enable" option instead; see use case: "Enable camera"

12a. Homeowner cancels the action - system returns to camera state display without changes.

13a. Camera is currently recording - system prompts "Camera is recording. Recording will be stopped and saved. Continue?" before proceeding.

14a. Recording stop fails - system displays error message and asks if homeowner wants to force disable; if confirmed, proceeds with disable command.

15a. Communication with camera fails - system displays error message "Unable to communicate with camera" and suggests checking camera connectivity.

16a. Camera fails to respond or acknowledge - system retries command up to three times, then displays error message and logs the issue; see use case: "Report camera malfunction"

16b. Camera responds with error status - system displays specific error message and suggests troubleshooting steps or contacting support.

1-20. An alarm condition is encountered - see use case: "alarm condition encountered."

When available: First increment

Frequency of use: Few times per week

Channel to actor: PC-based system with web browser

Secondary actor: Support technician, Webmaster, Camera, Storage Server

Channels to secondary actors:

1. Support technician: phone line.
2. Webmaster: E-mail.
3. Camera: wireless connectivity
4. Storage Server: network connection

Open Issues:

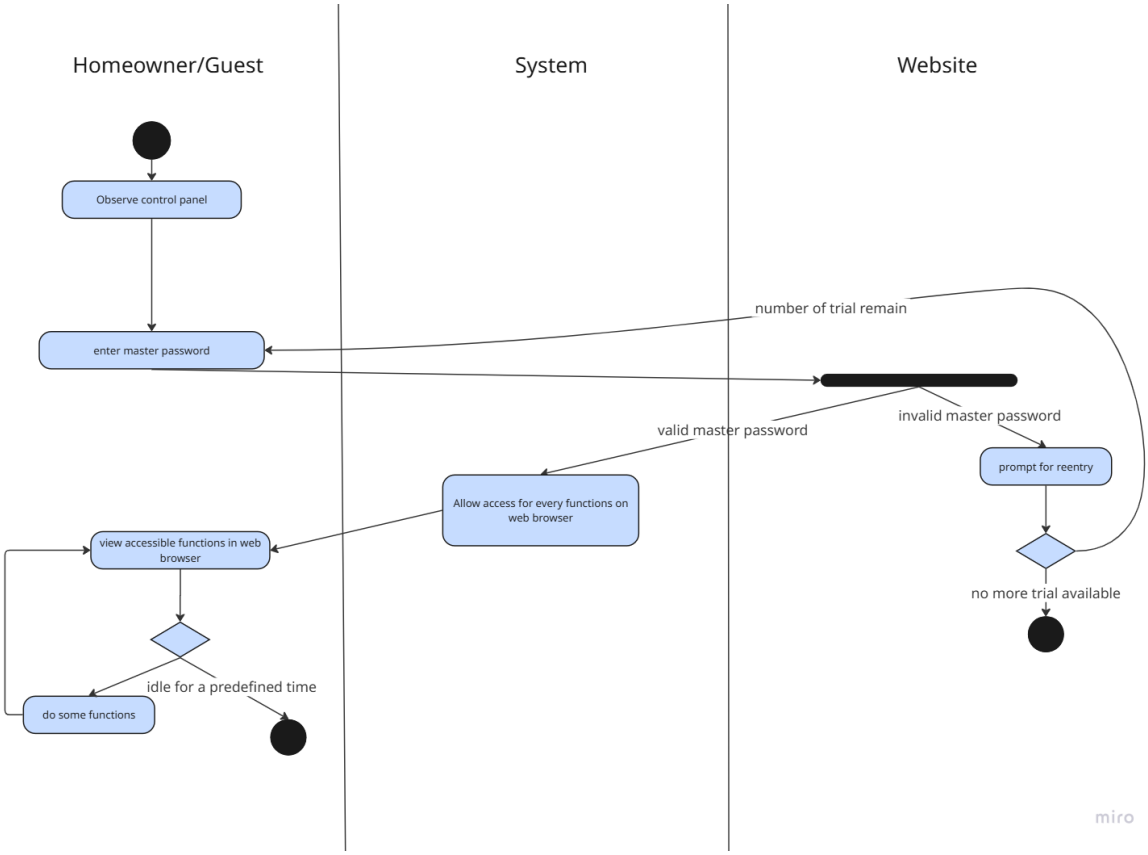
1. Should there be different privilege levels for enabling/disabling cameras?
2. Will the system log all enable/disable actions for audit purposes?
3. Should the system send notifications when cameras are disabled?
4. How long should the system wait for camera acknowledgment before timing out?
5. Can multiple cameras be disabled simultaneously?
6. Should disabled cameras still be visible on the floor plan or hidden?
7. What happens to scheduled recordings when a camera is disabled?
8. Should there be a "privacy mode" that temporarily disables cameras for a set duration?

Reference in meeting log 2025.10.29

VII. Sequence Diagram

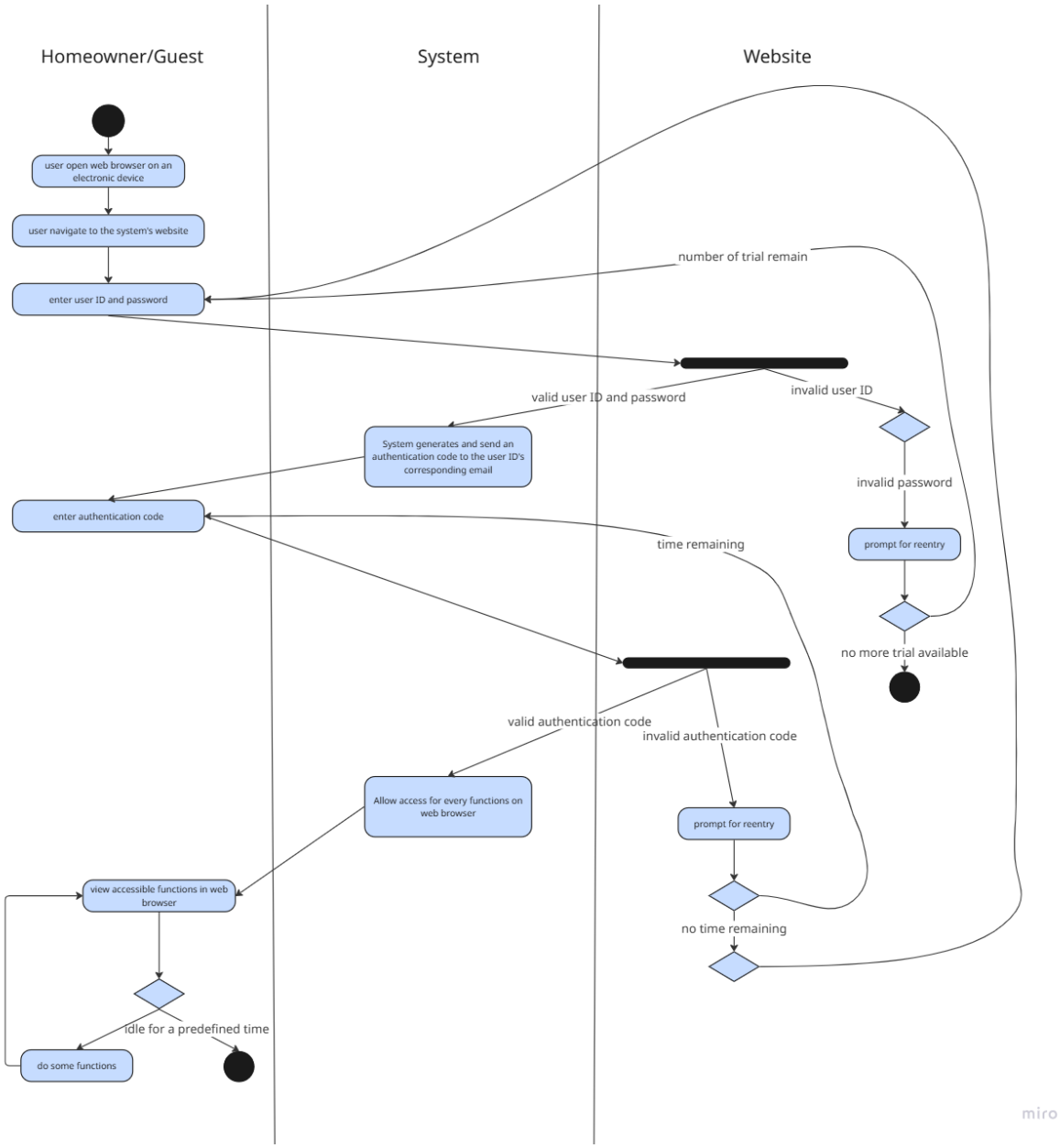
1. Common Sequence Diagram

a. Log onto the system through control panel



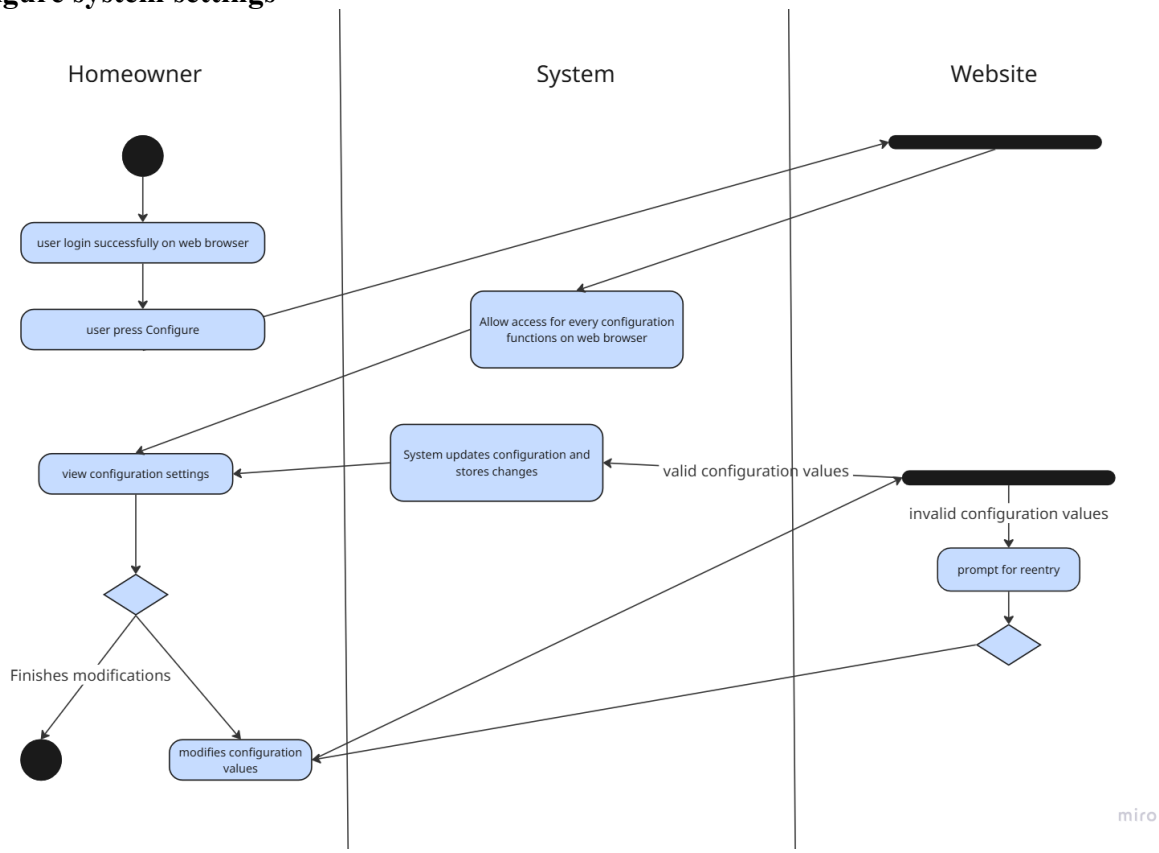
Reference in meeting log 2025.10.28

b. Log onto the system through web browser



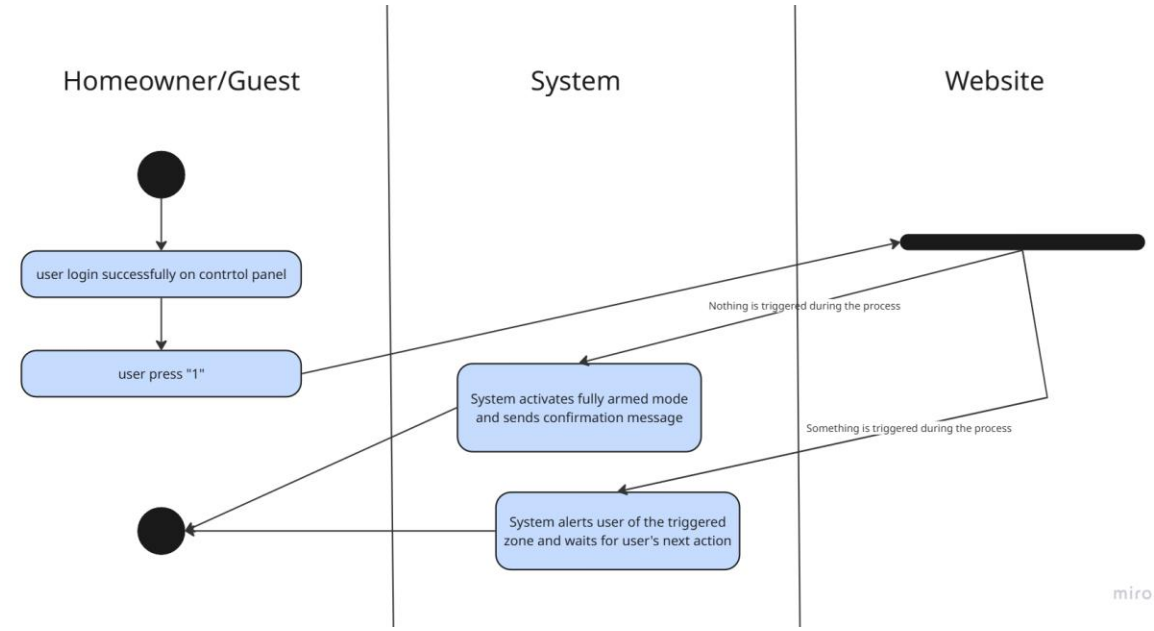
<u>Reference in meeting log 2025.10.28</u>

c. Configure system settings



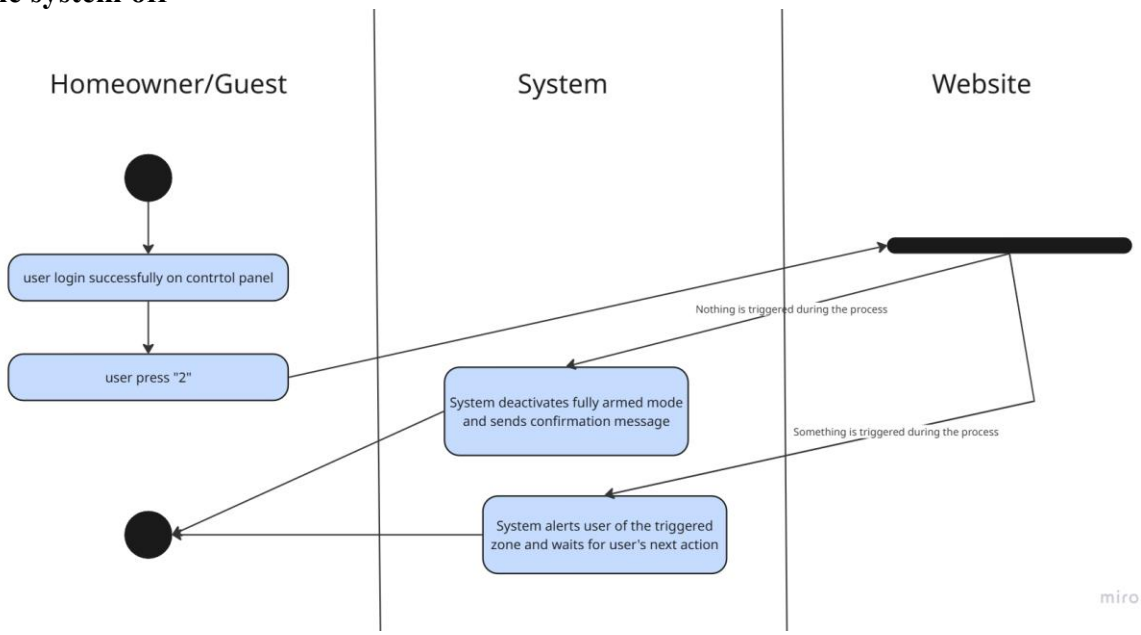
Reference in meeting log 2025.10.28

d. Turn the system on



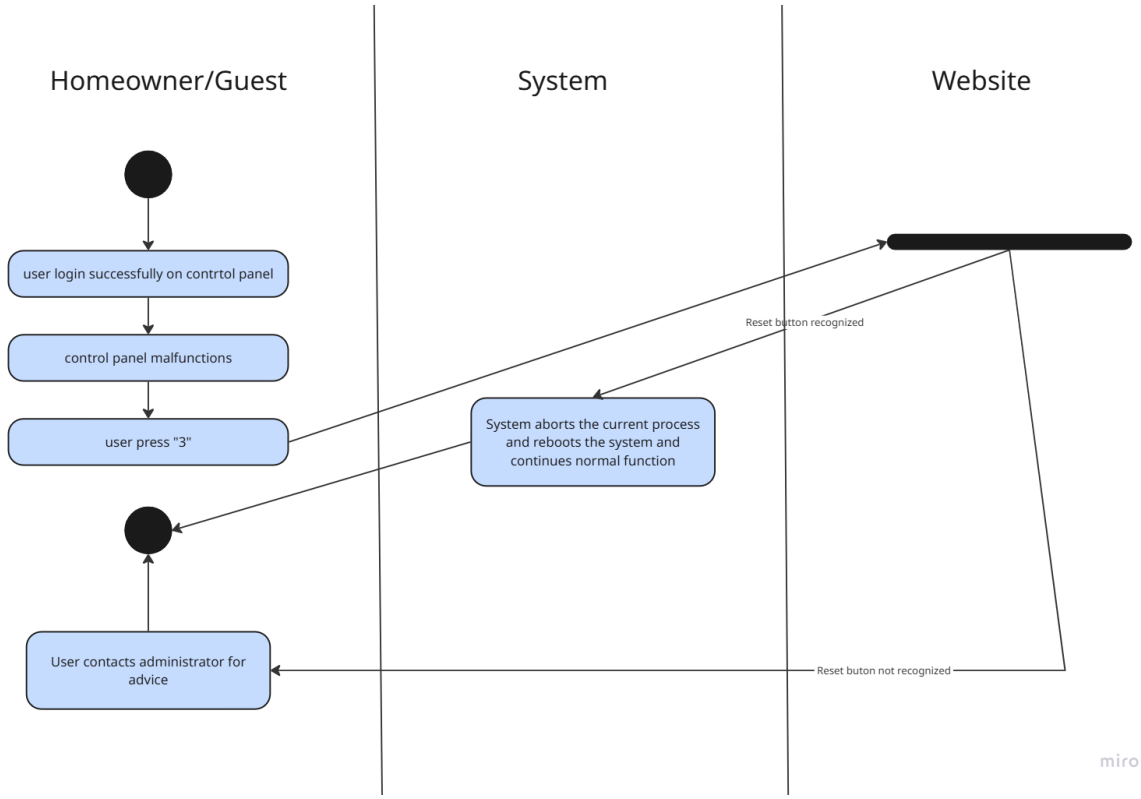
Reference in meeting log 2025.10.28

e. Turn the system off



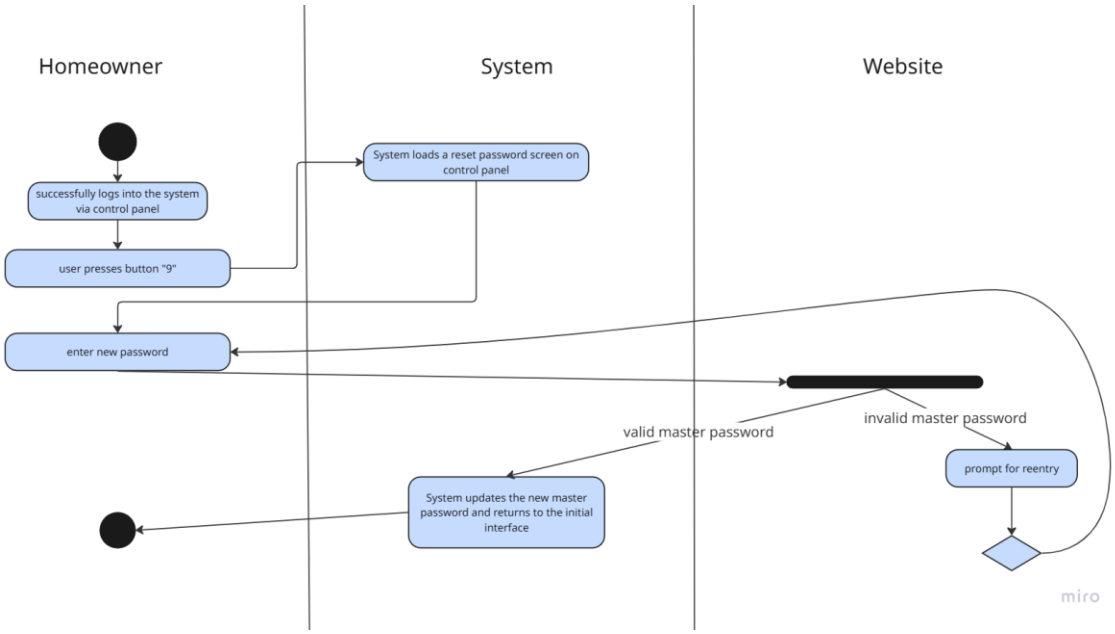
Reference in meeting log 2025.10.28

f. Reset the system



Reference in meeting log 2025.10.28

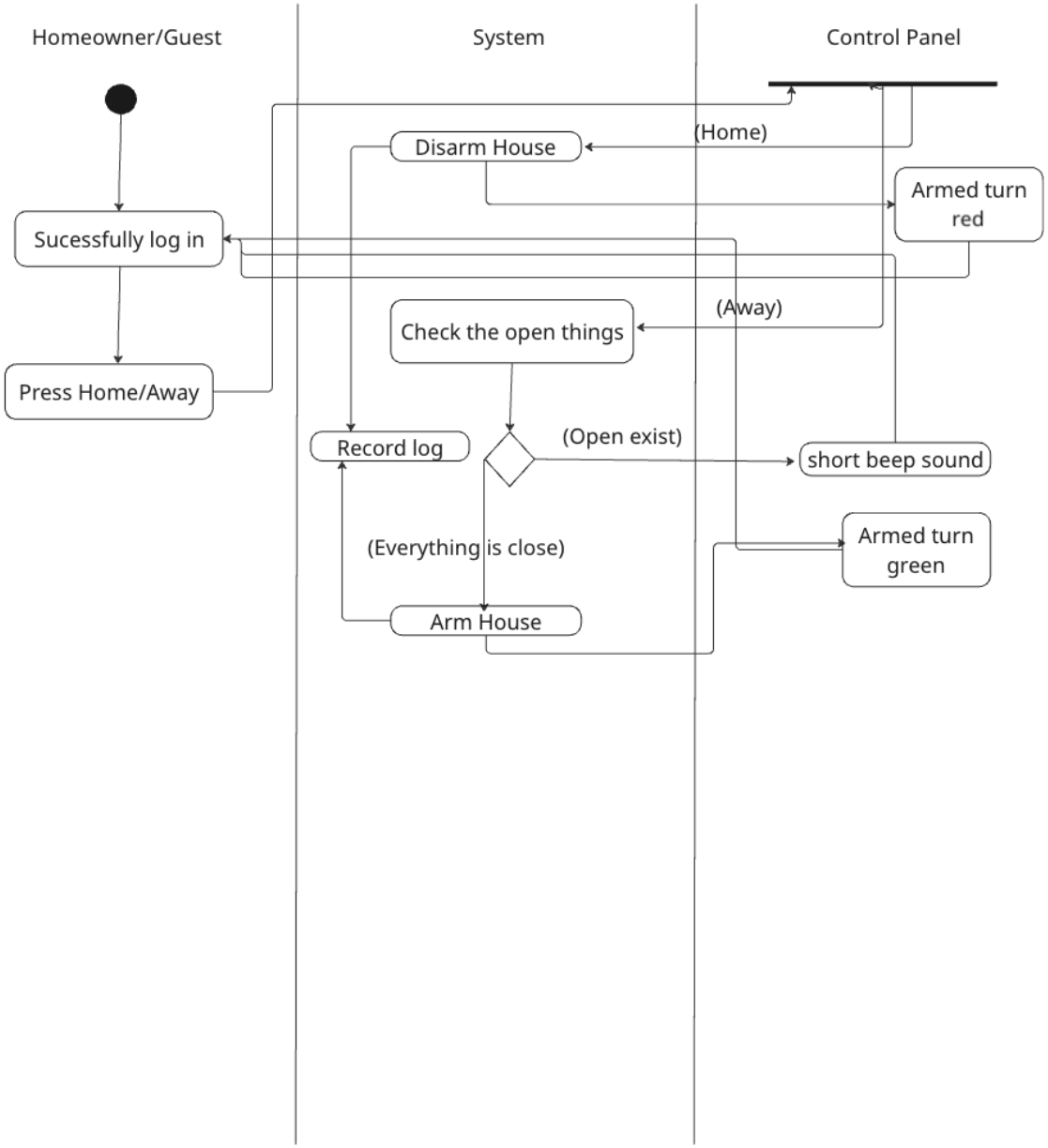
g. Change master password through control panel



Reference in meeting log 2025.10.28

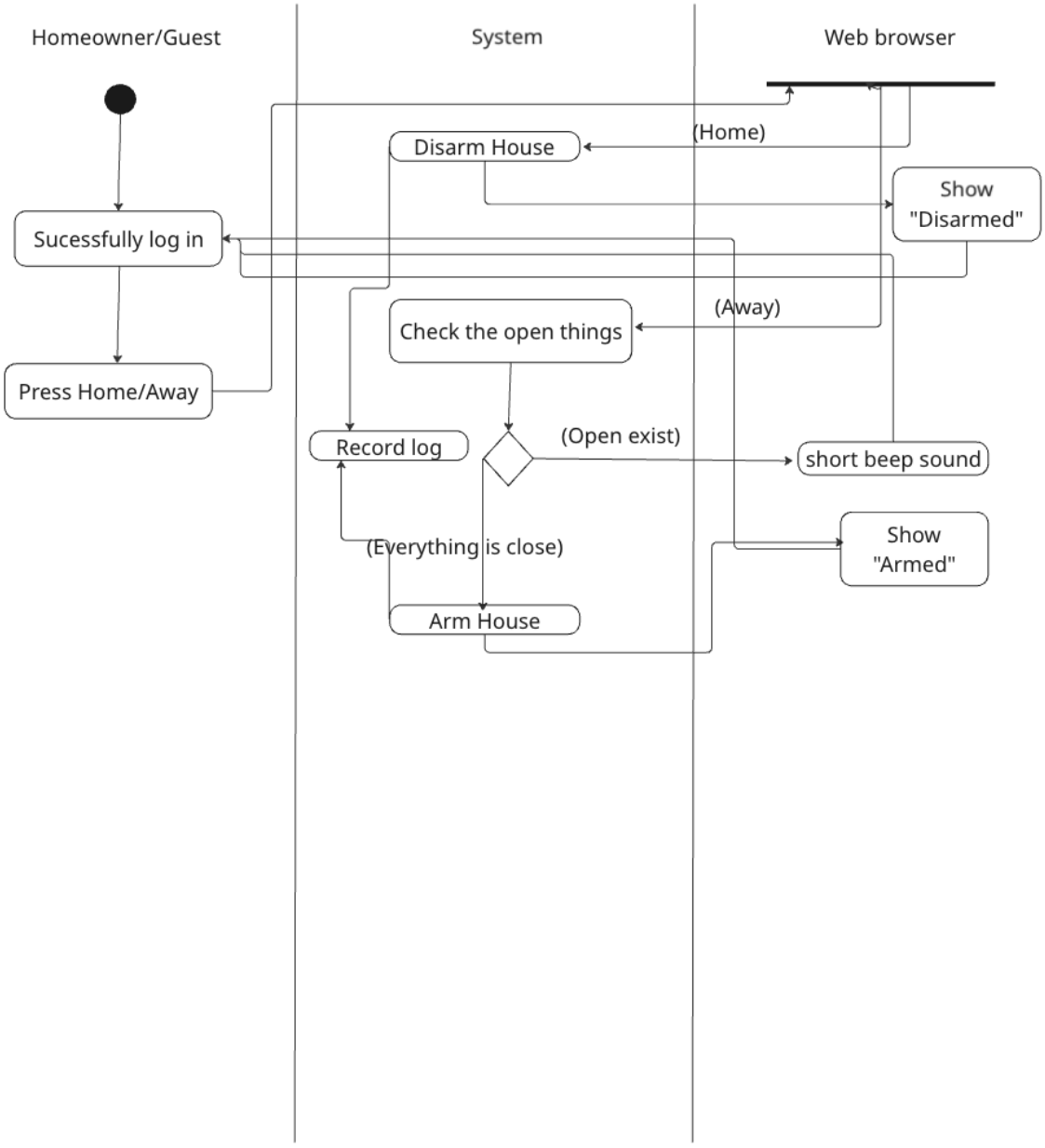
2. Security Sequence Diagram

a. Arm/disarm system through control panel



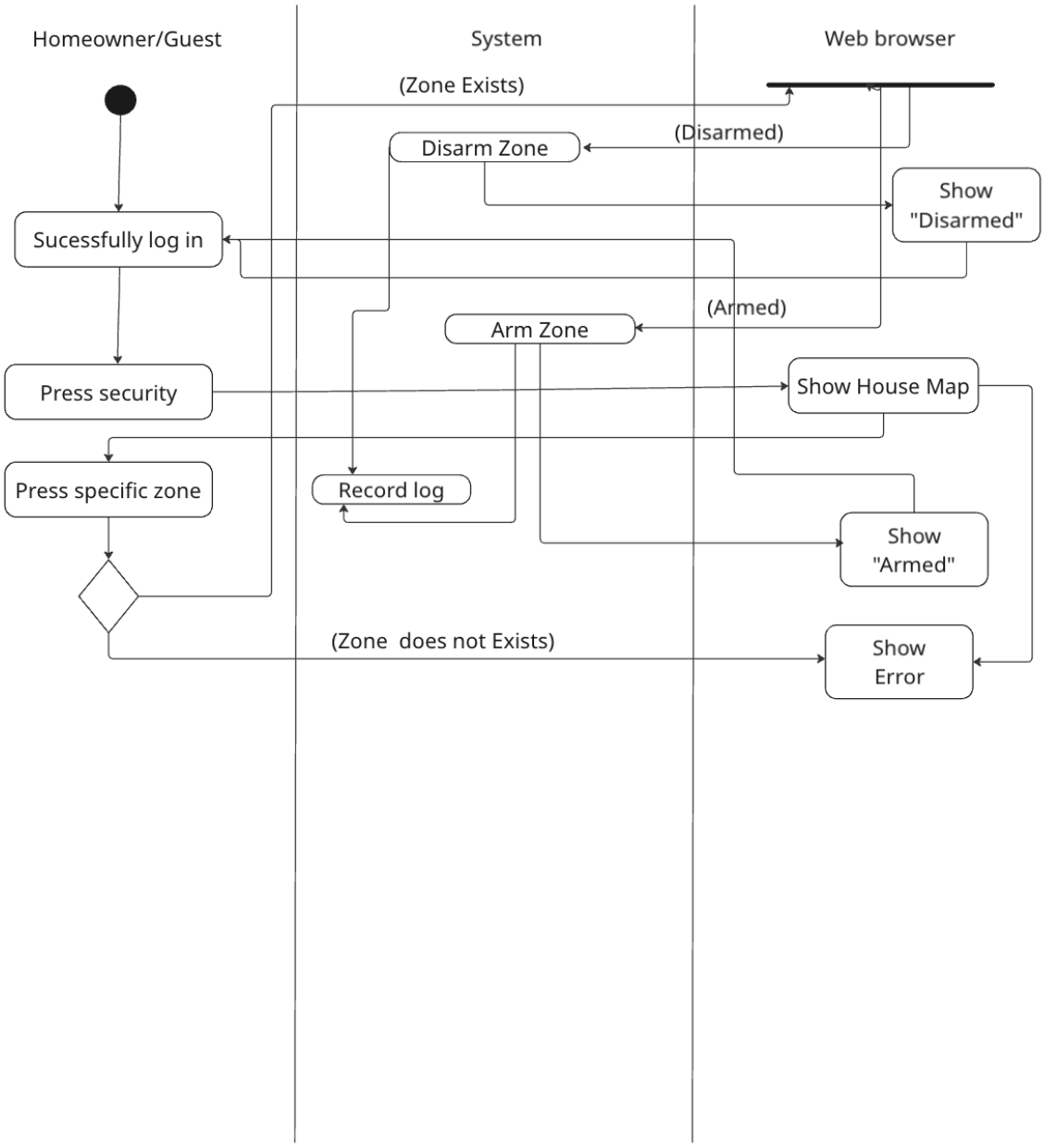
Reference in meeting log 2025.10.31

b. Arm/disarm system through web browser



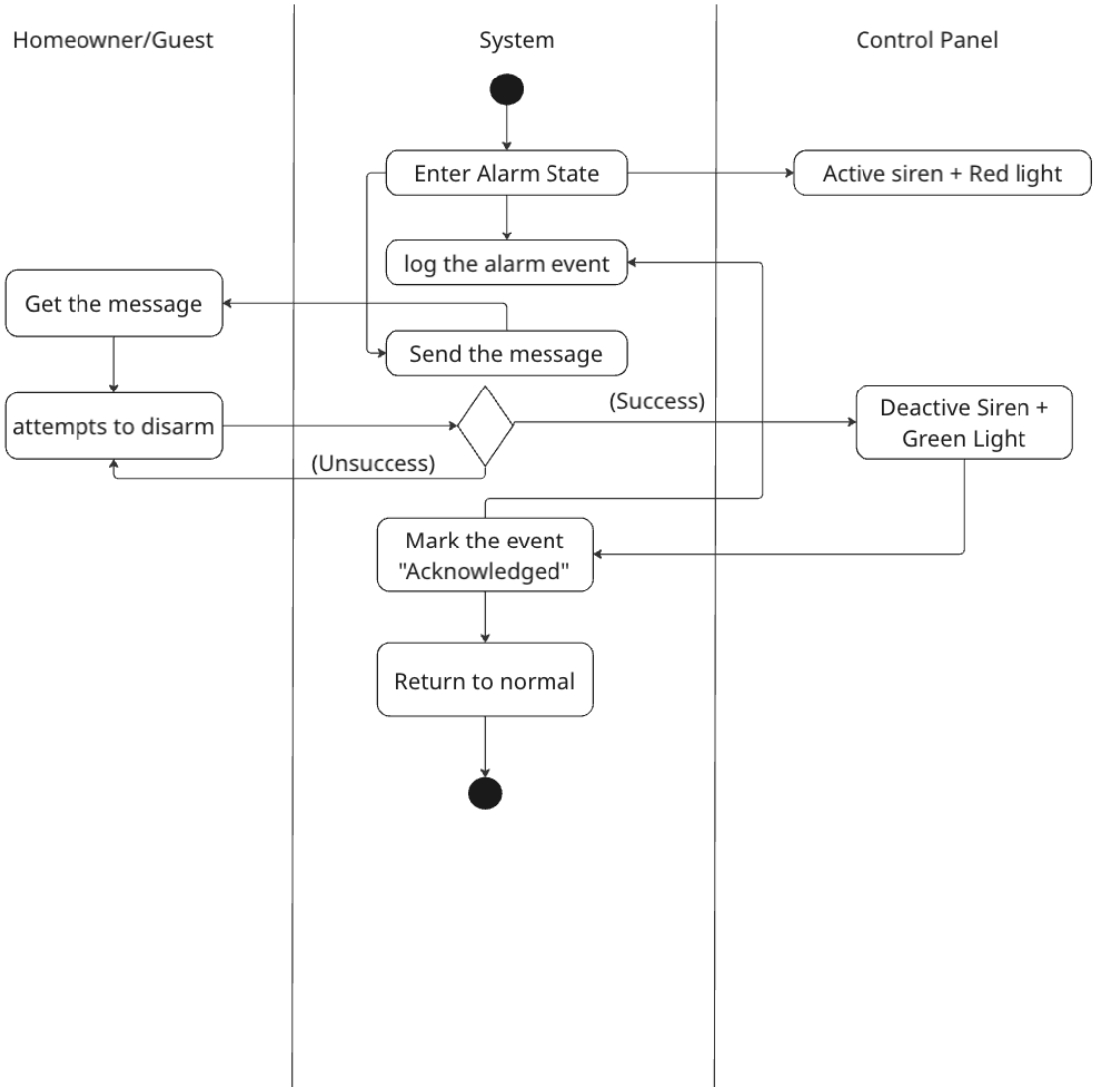
Reference in meeting log 2025.10.31

c. Arm/disarm safety zone selectively



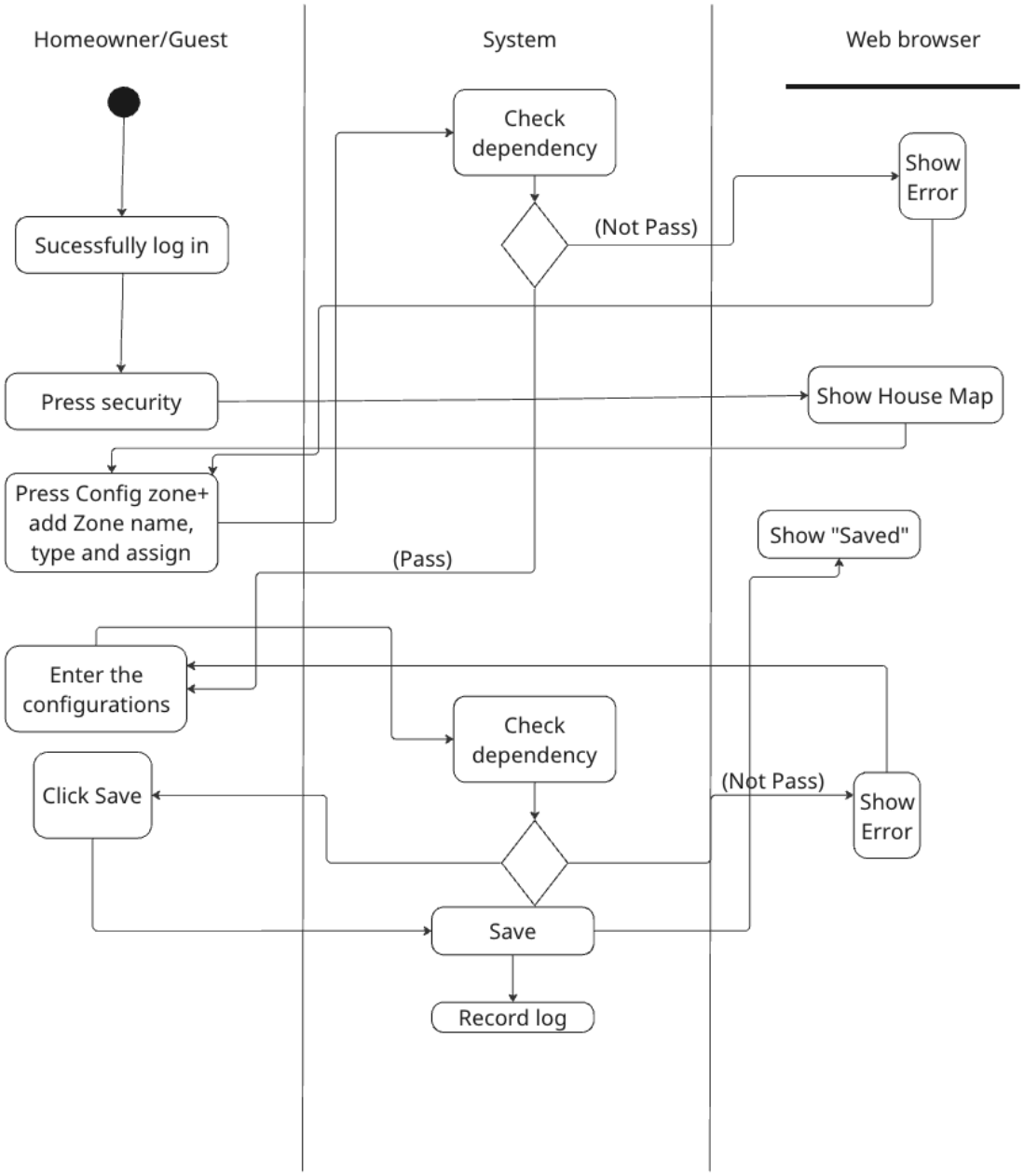
Reference in meeting log 2025.10.31

d. Alarm condition encountered



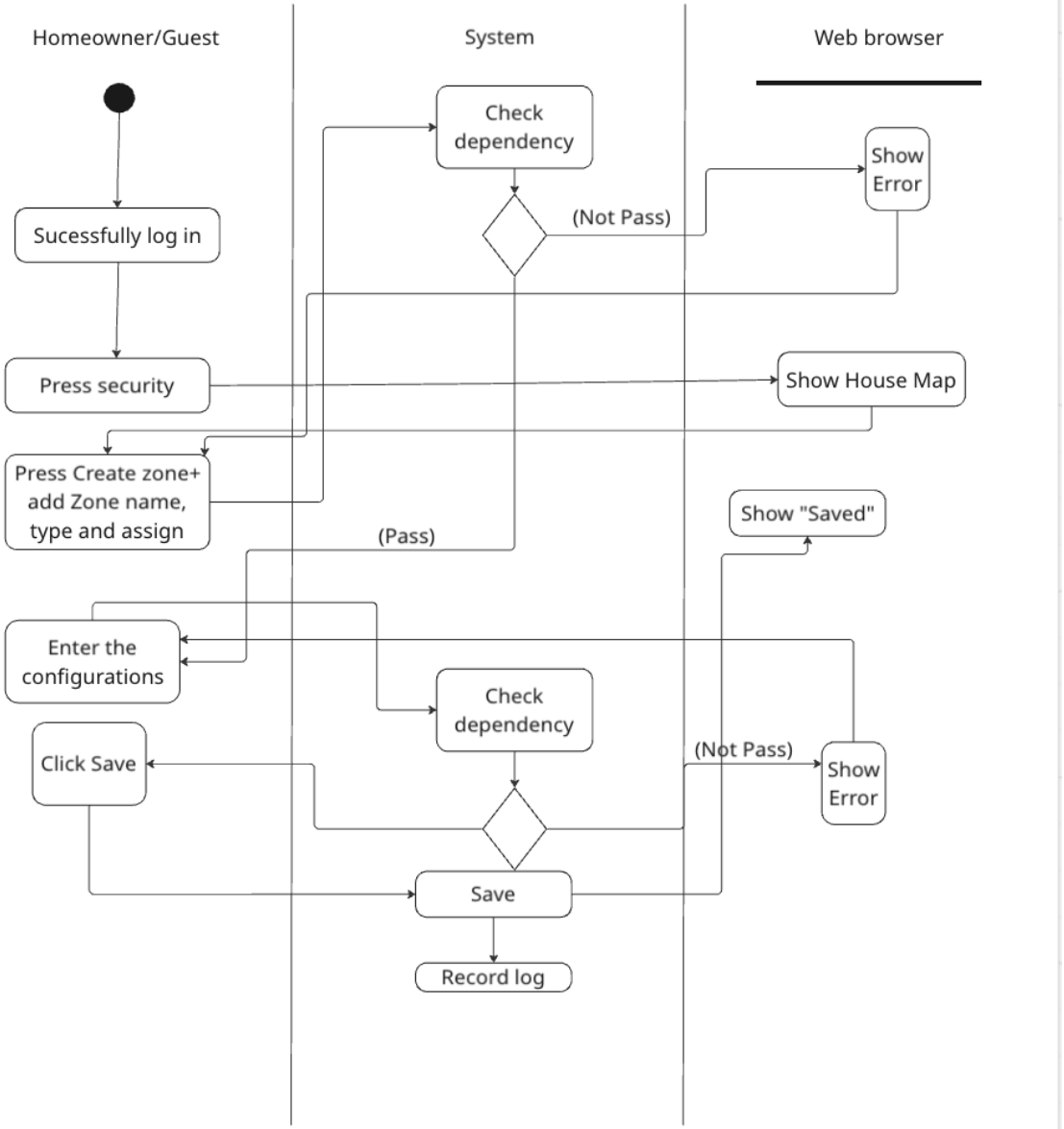
<u>Reference in meeting log 2025.10.31</u>

e. Configure safety zone



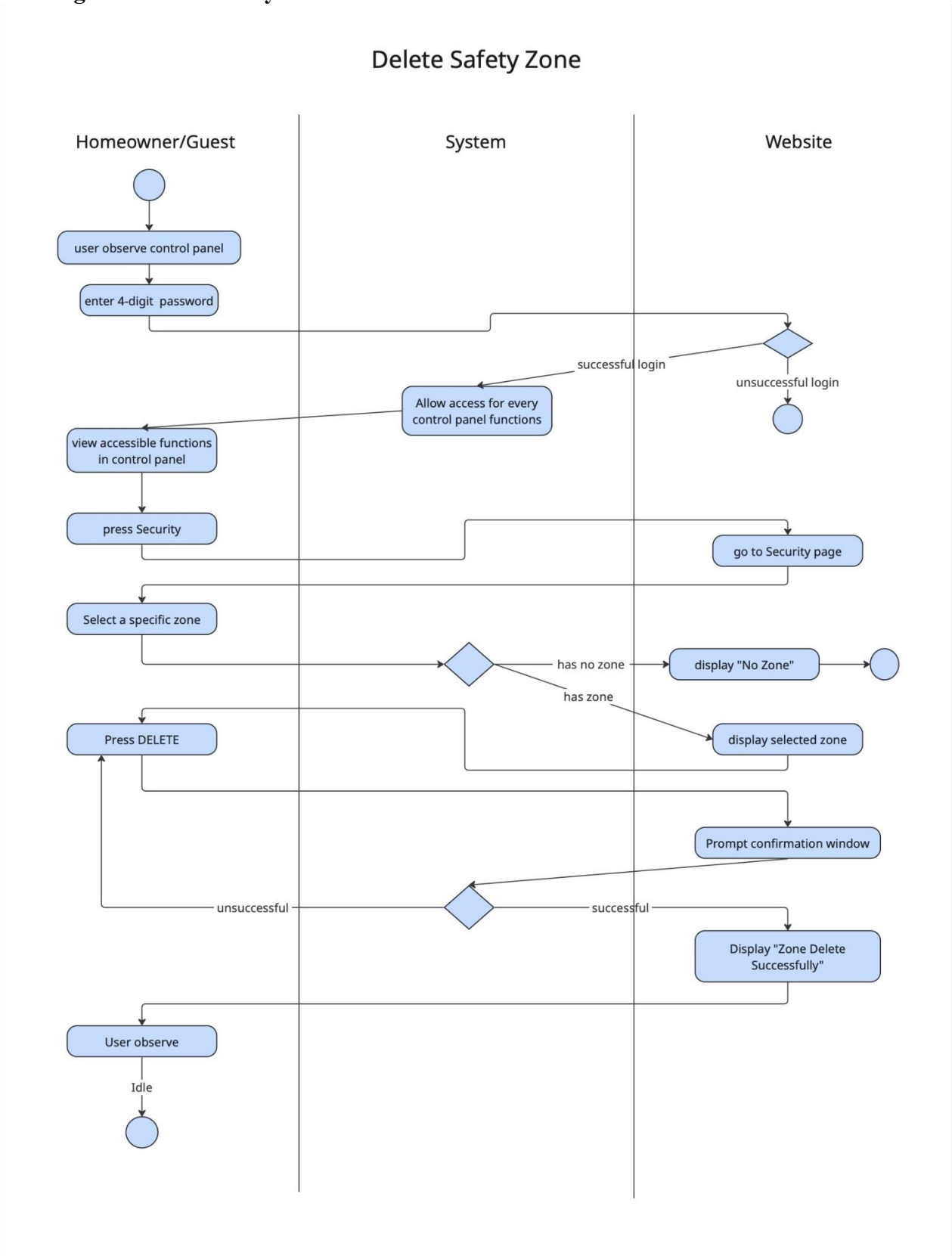
Reference in meeting log 2025.10.31

f. Create new safety zone



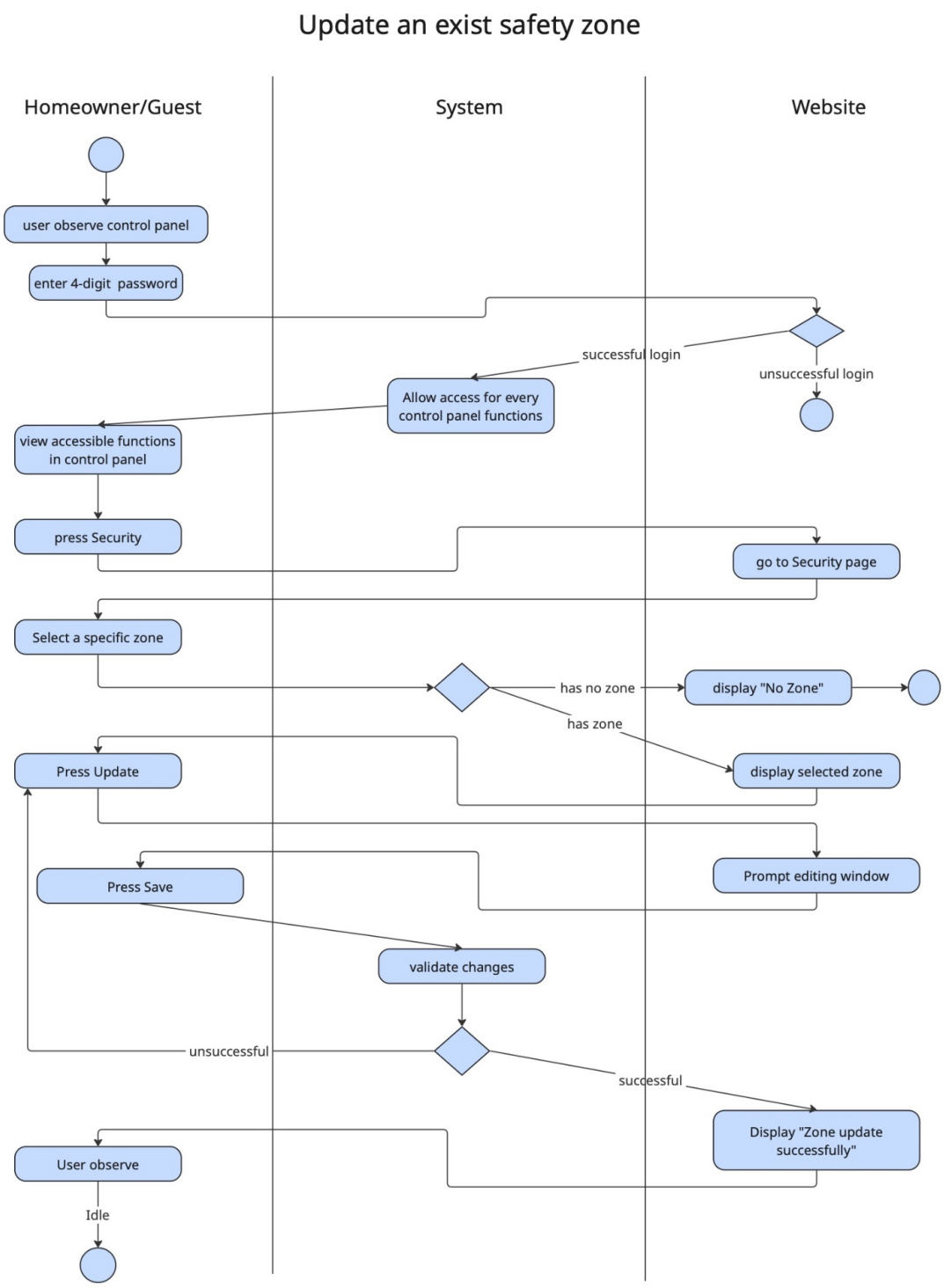
Reference in meeting log 2025.10.31

g. Delete safety zone



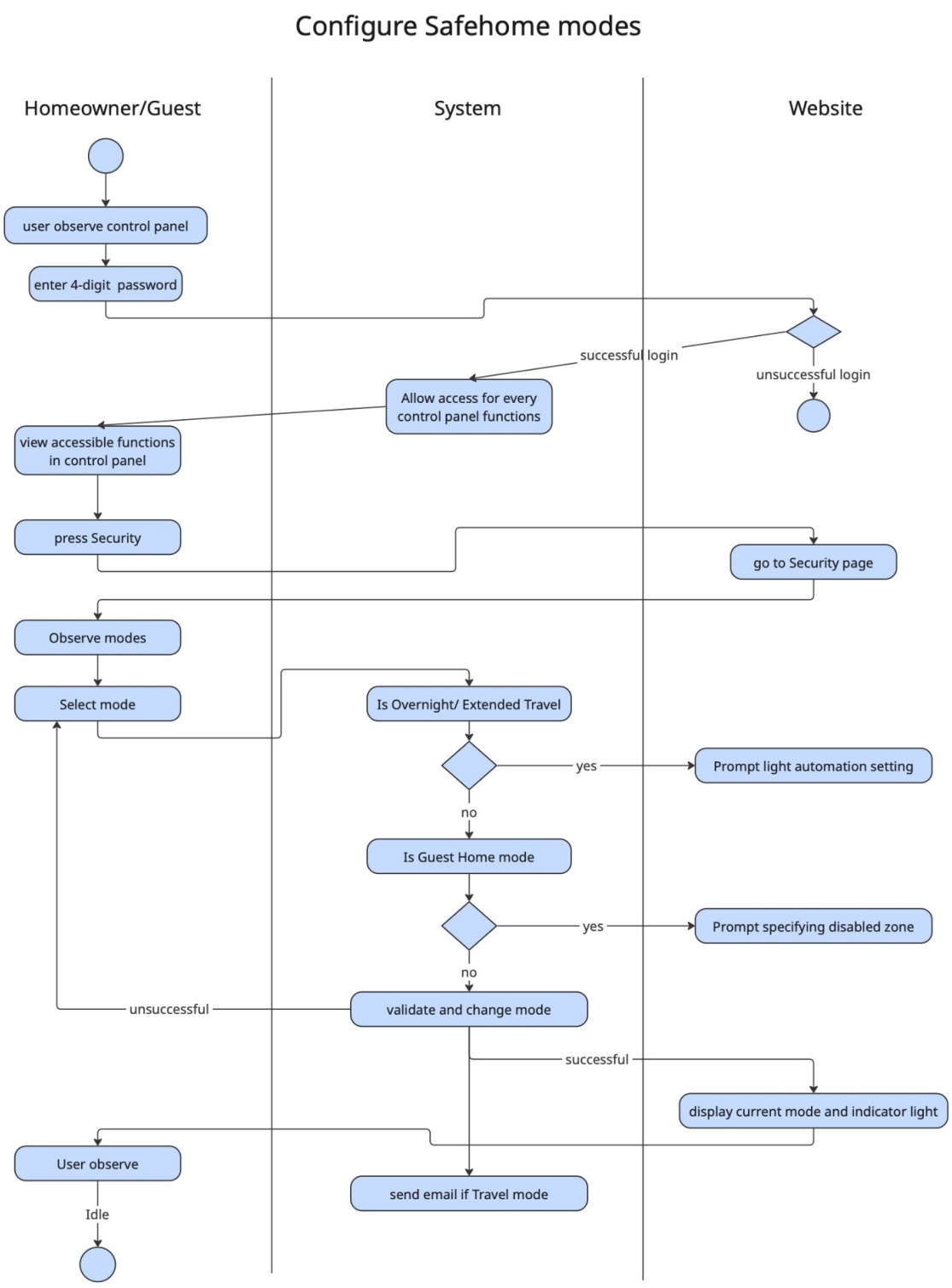
Reference in meeting log 2025.10.27

h. Update an exist safety zone



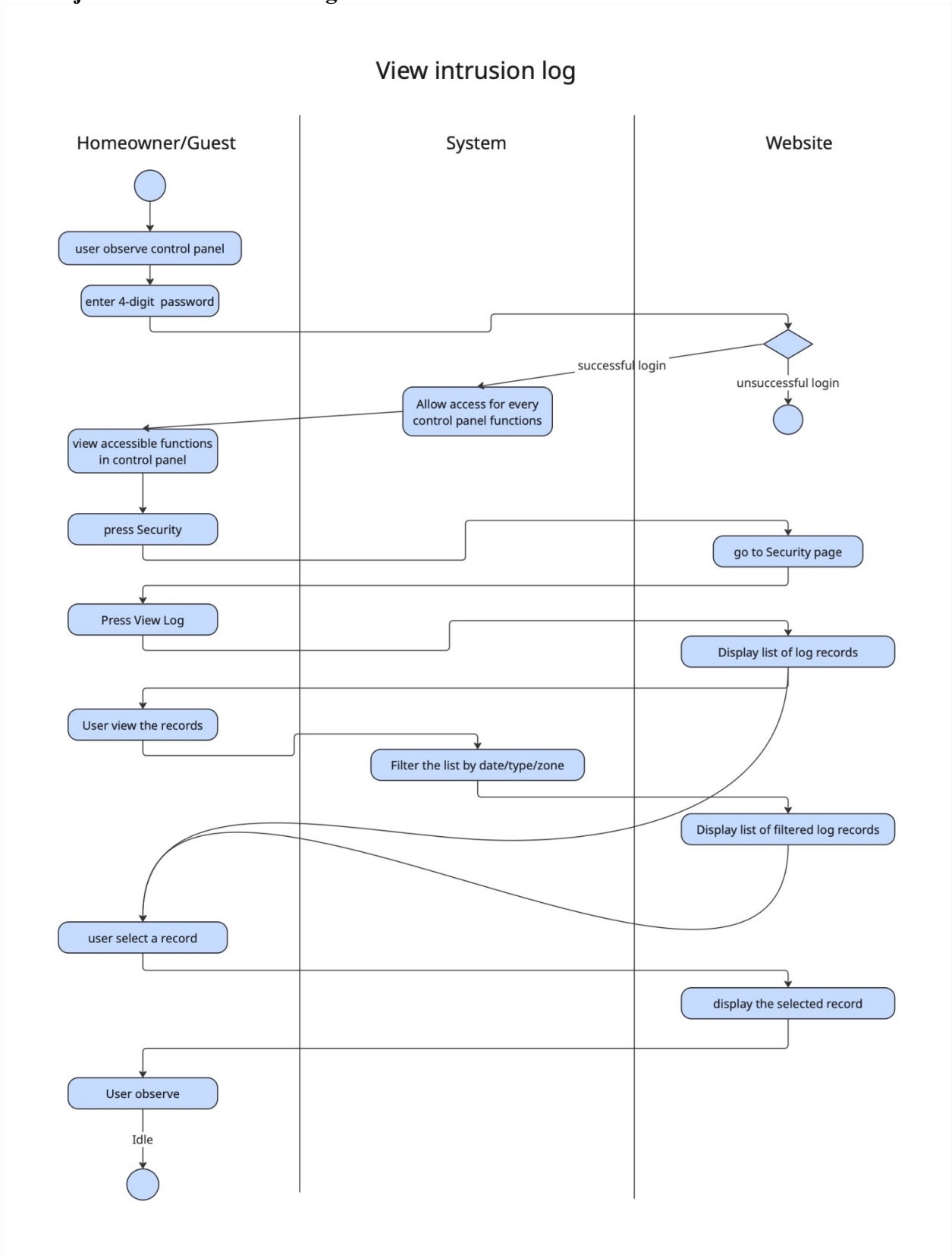
Reference in meeting log 2025.10.27

i. Configure Safehome modes



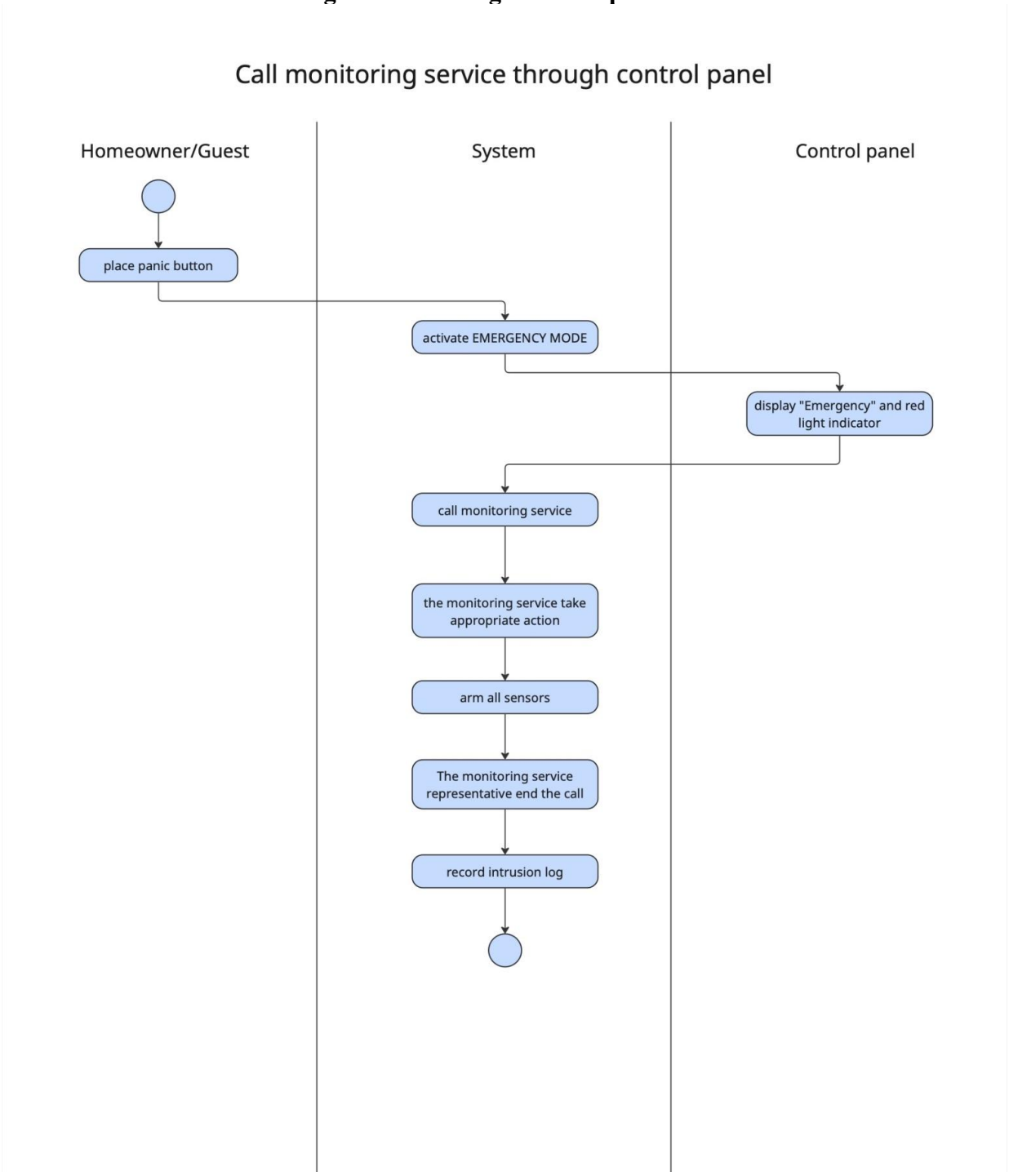
Reference in meeting log 2025.10.27

j. View intrusion log



Reference in meeting log 2025.10.27

k. Call monitoring service through control panel

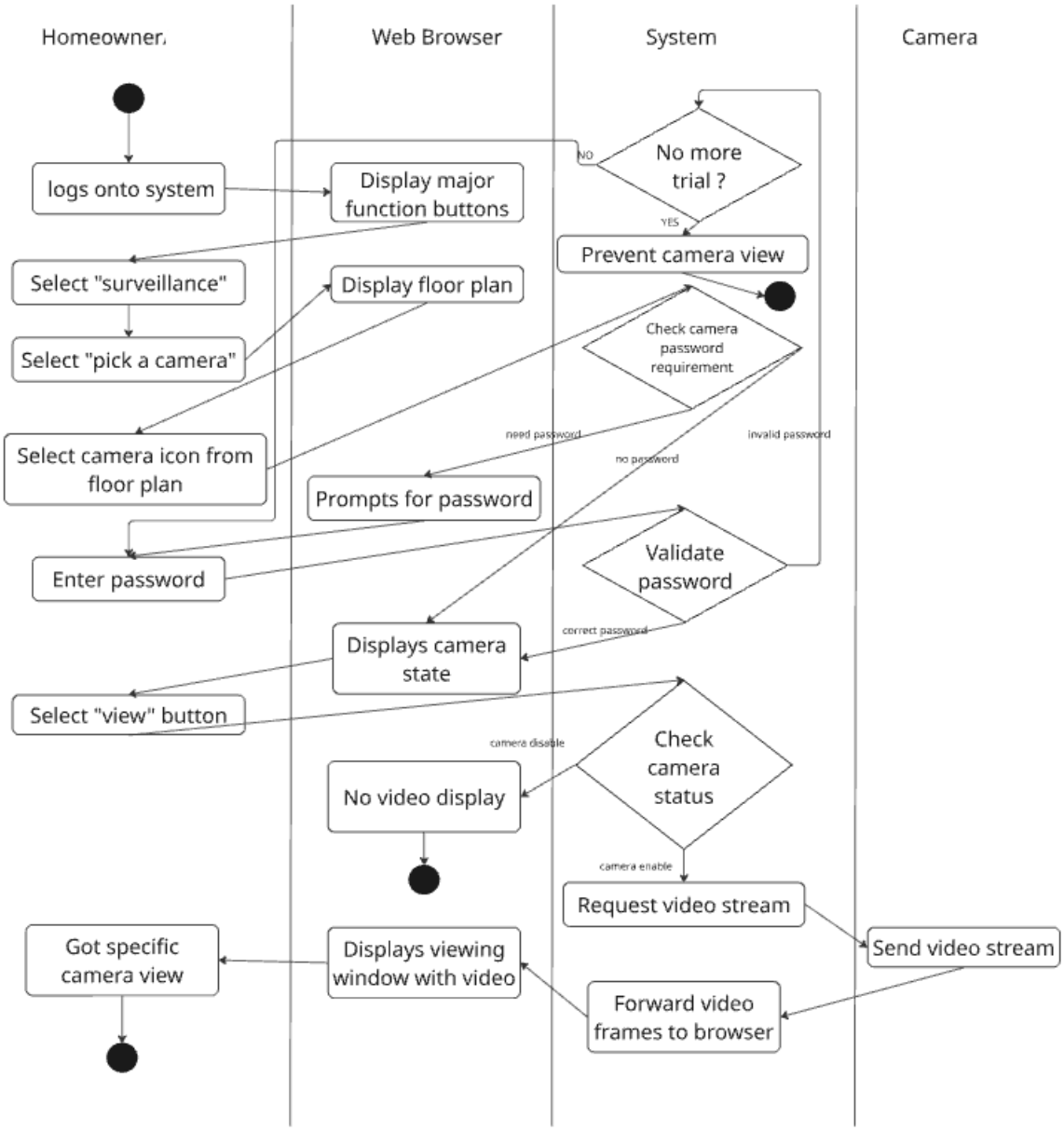


Reference in meeting log 2025.10.27

3. Surveillance Sequence Diagram

a. Display Specific camera view

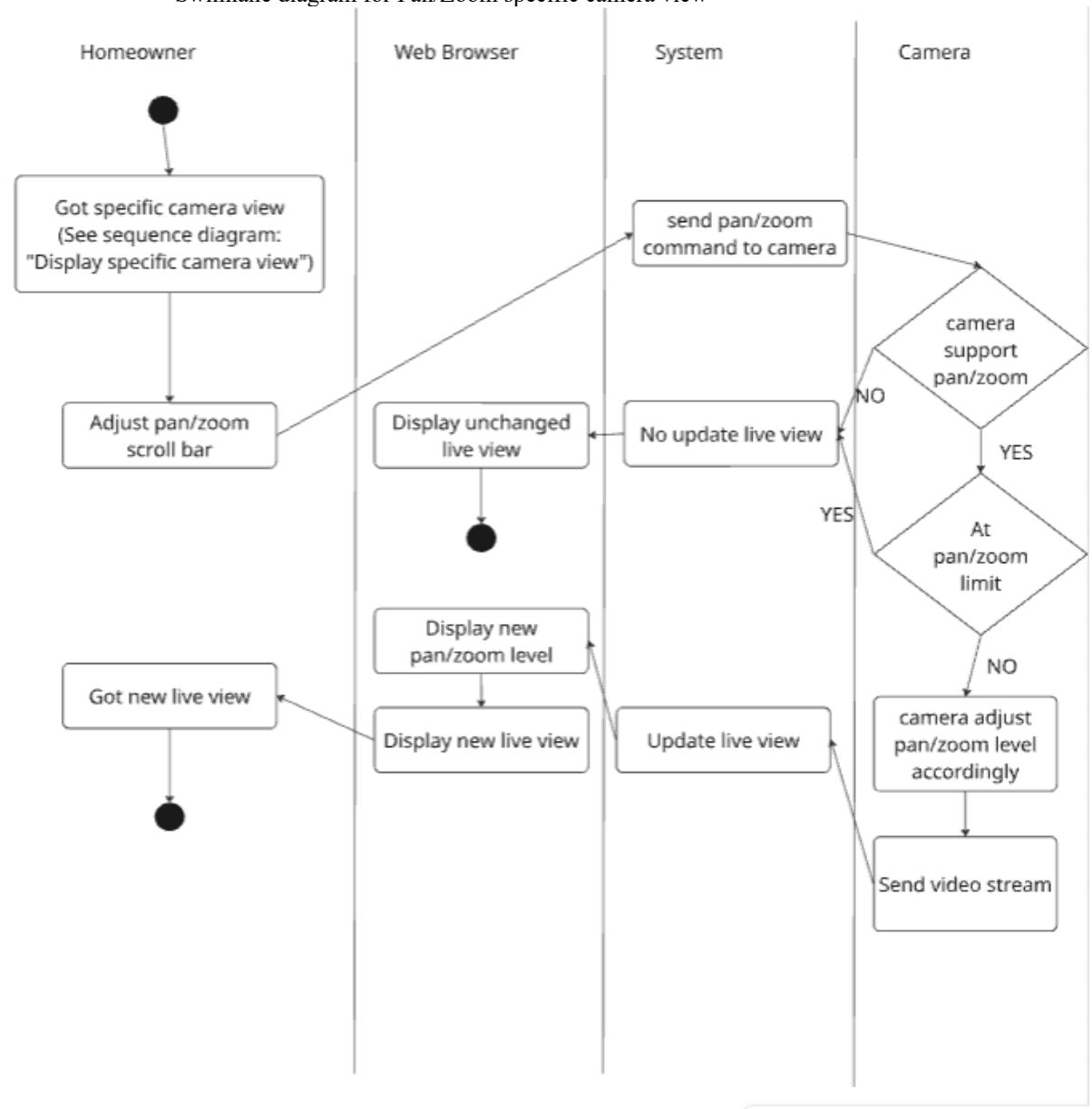
Swimlane diagram for Display Specific camera view



Reference in meeting log 2025.10.29

b. Pan/Zoom specific camera view

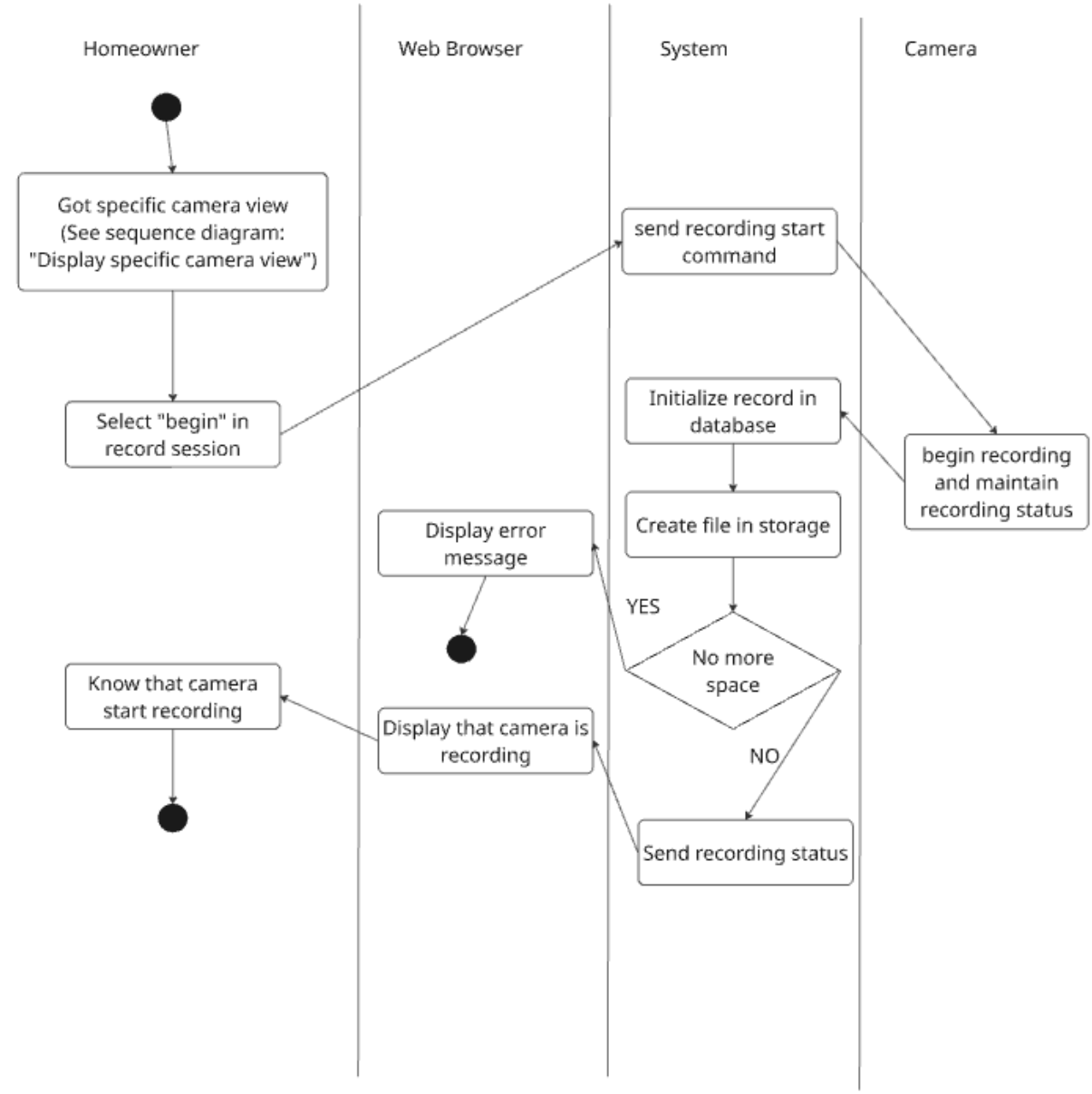
Swimlane diagram for Pan/Zoom specific camera view



Reference in meeting log 2025.10.29

c. Begin camera recording

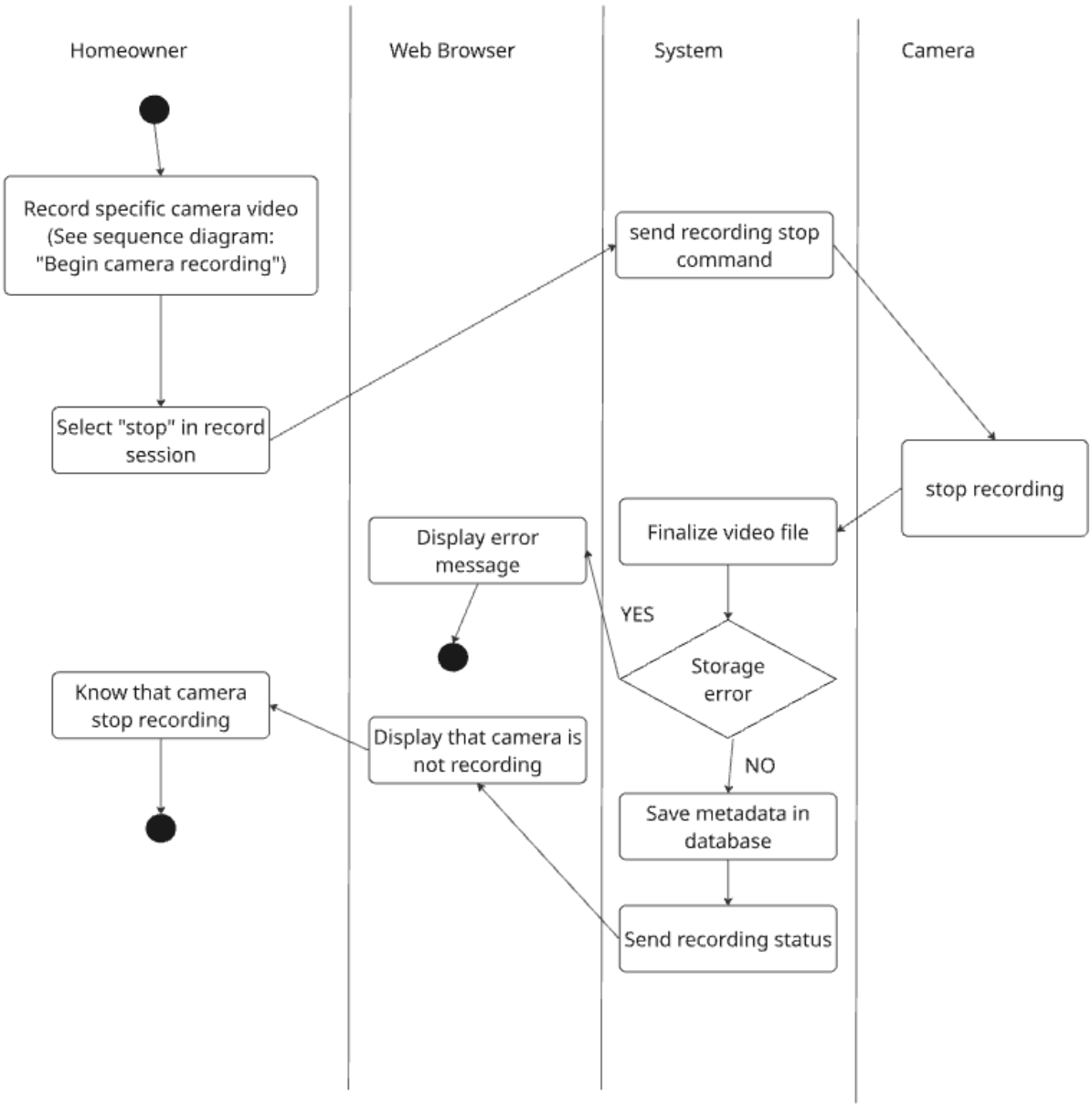
Swimlane diagram for Begin camera recording



Reference in meeting log 2025.10.29

d. Stop camera recording

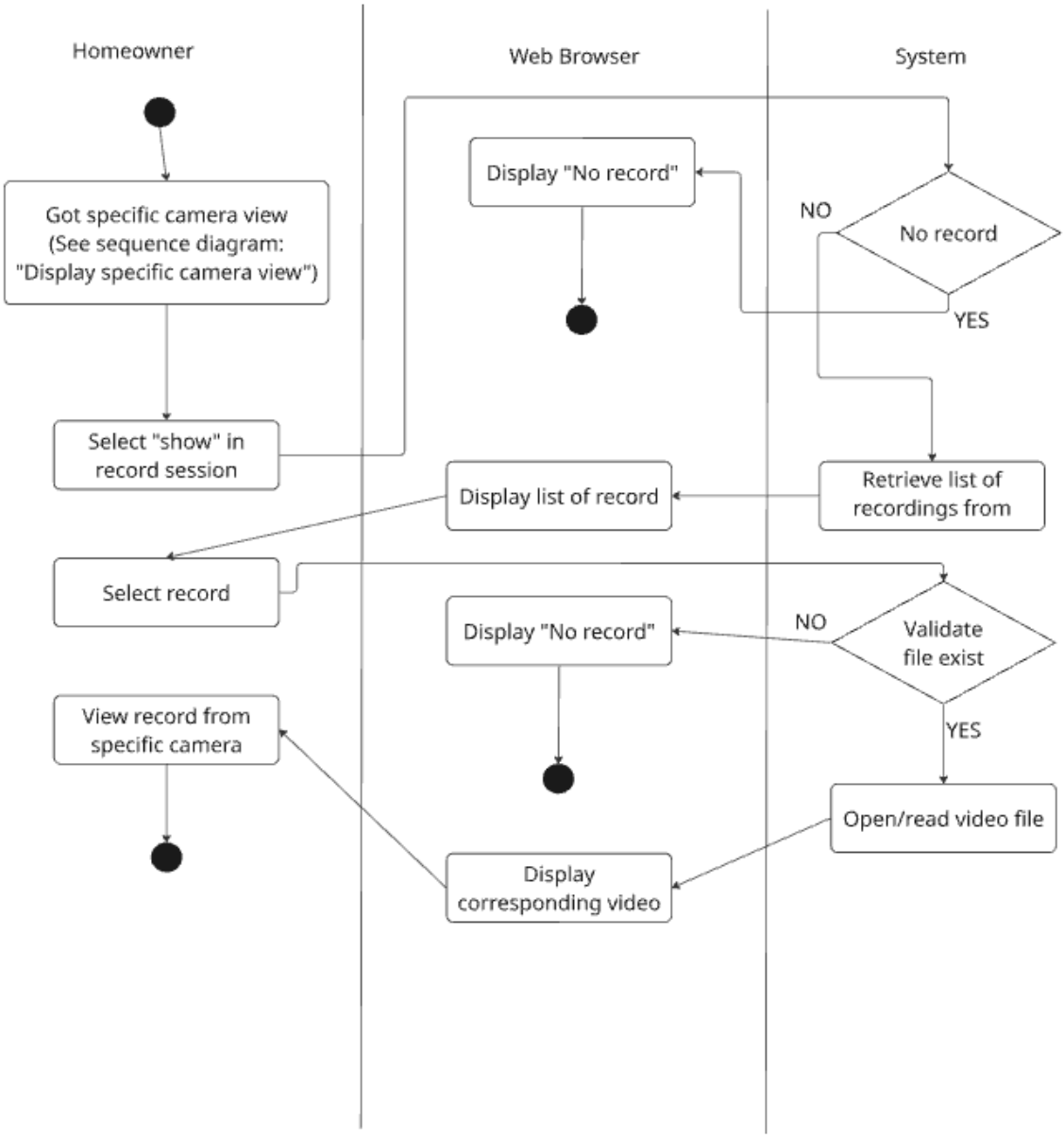
Swimlane diagram for Stop camera recording



Reference in meeting log 2025.10.29

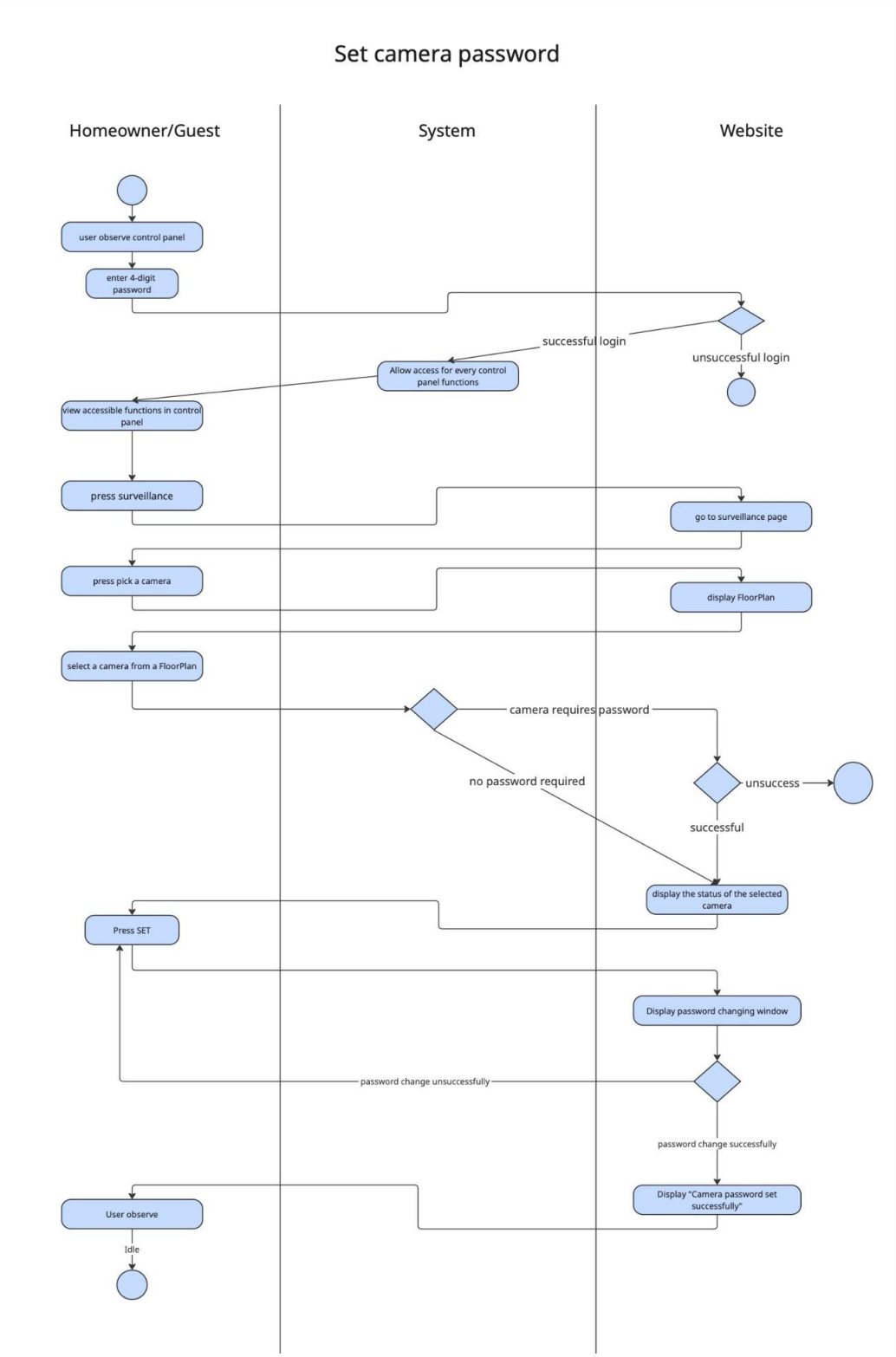
e. Replay camera recording

Swimlane diagram for Replay camera recording



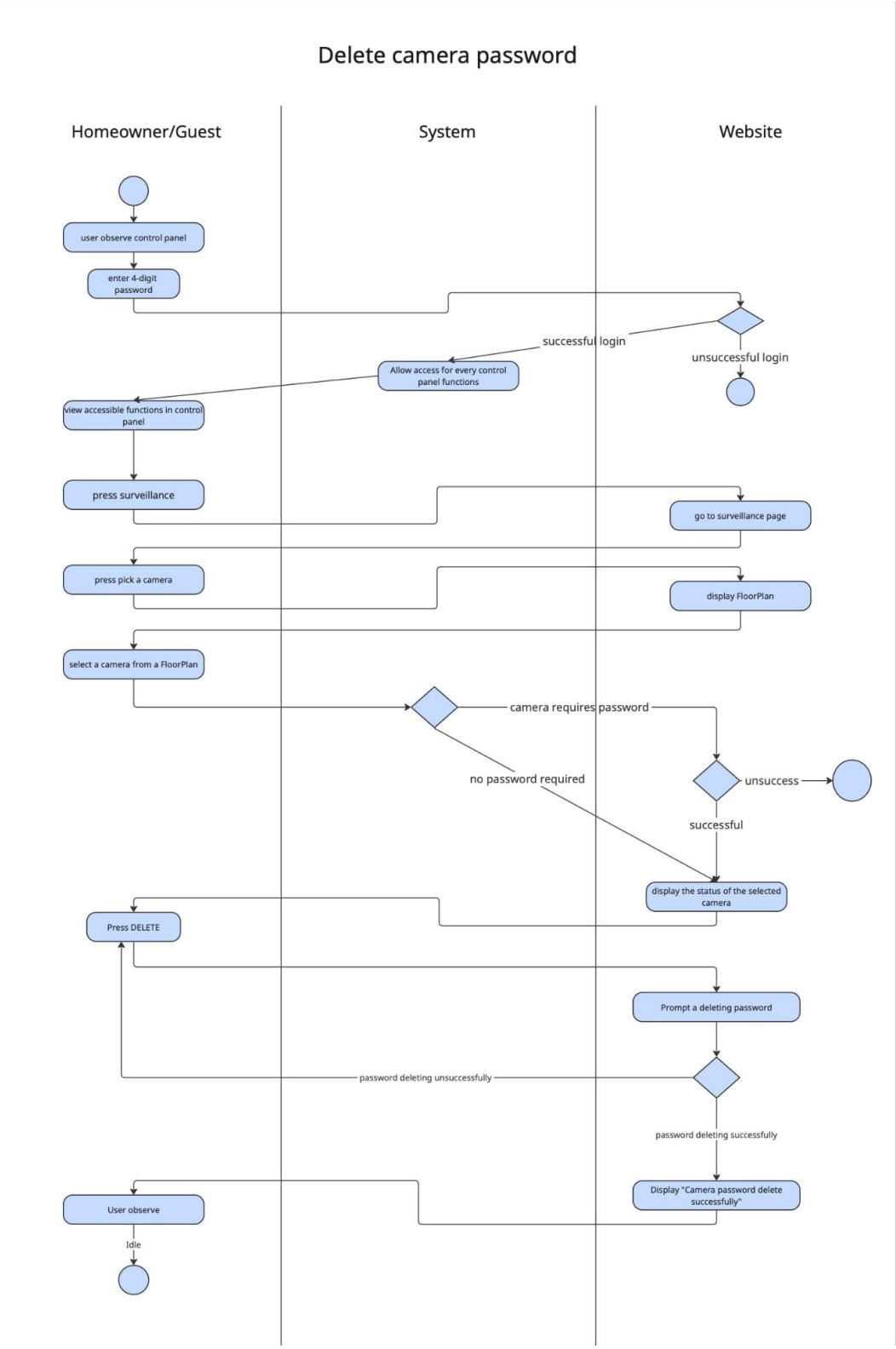
Reference in meeting log 2025.10.29

f. Set camera password



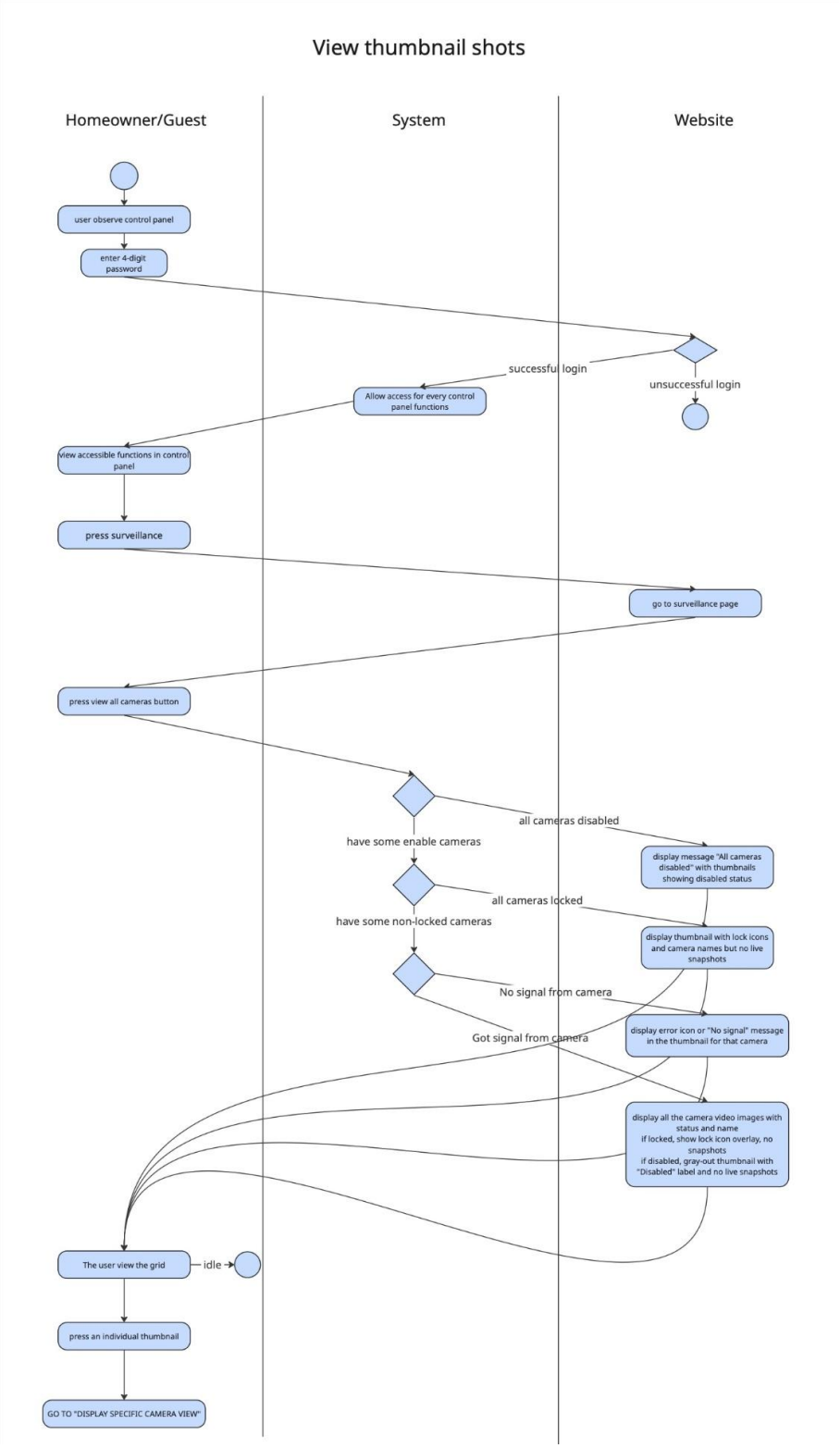
Reference in meeting log 2025.10.27

g. Delete camera password



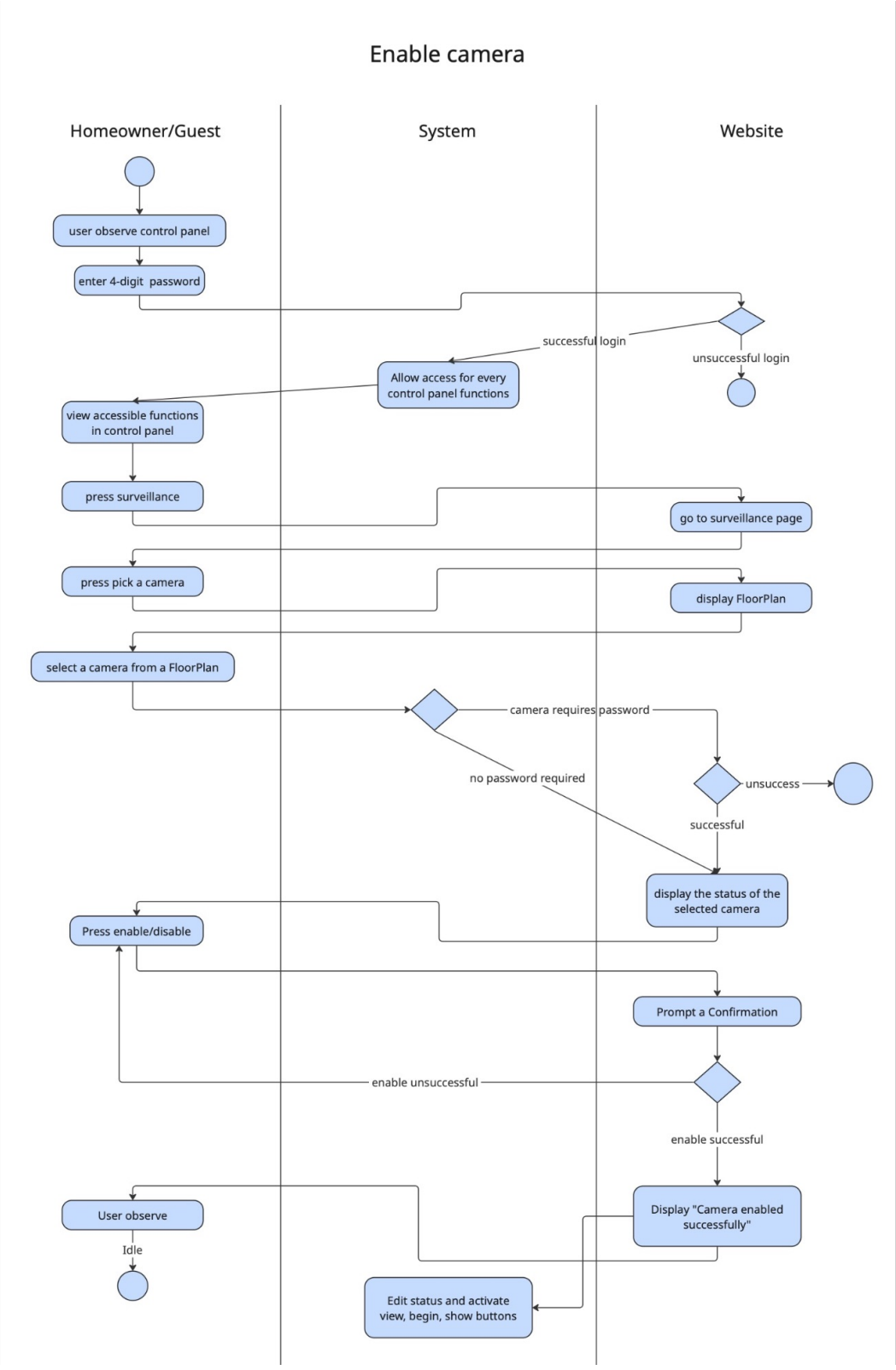
Reference in meeting log 2025.10.27

h. View thumbnail Shots



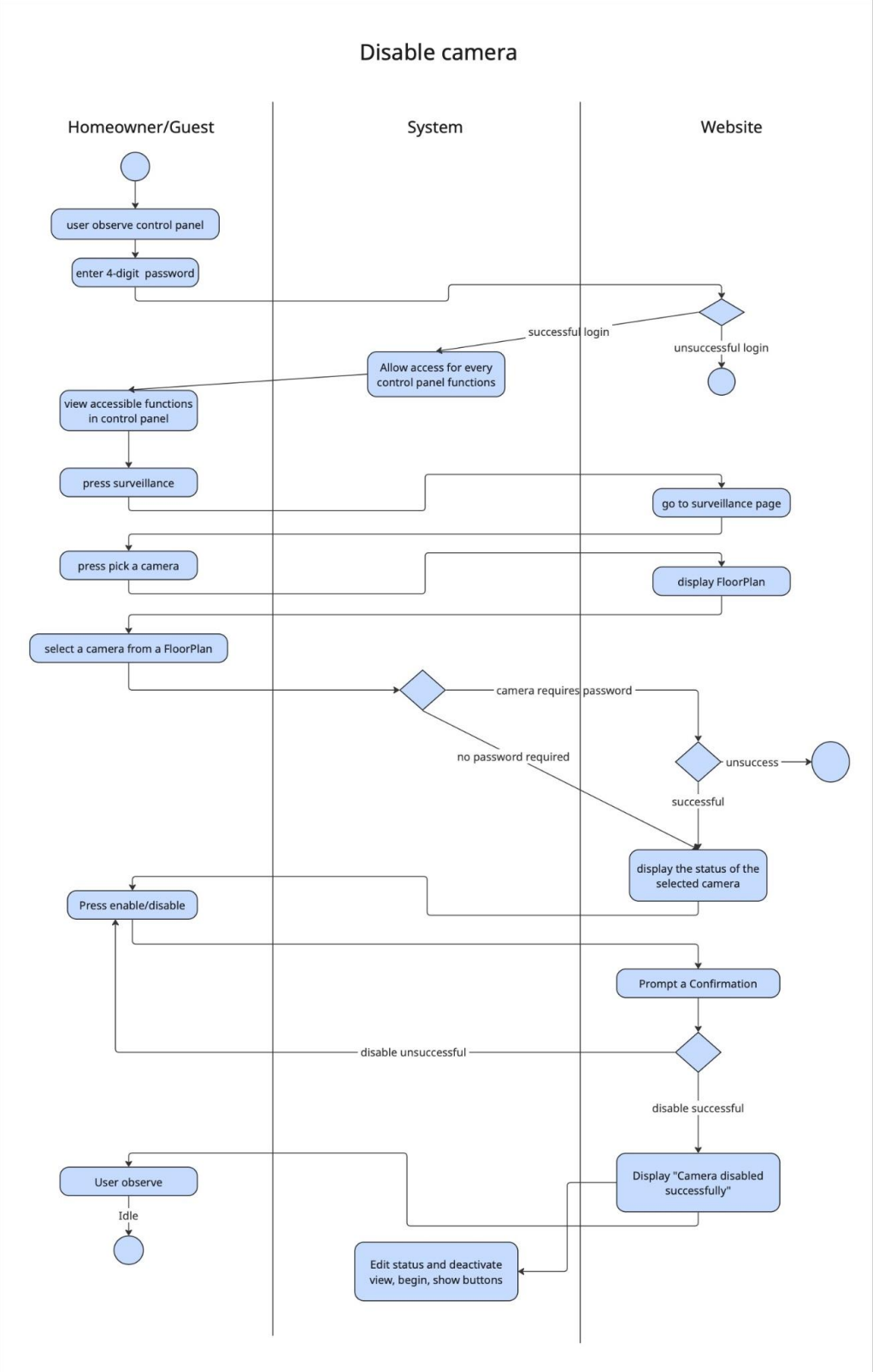
Reference in meeting log 2025.10.27

i. Enable camera



Reference in meeting log 2025.10.27

j. Disable camera



Reference in meeting log 2025.10.27

VIII. Who did what

Team member A
1. Use case scenario for surveillance functions 2. Use case scenario for common functions **([LoginCP] in Fig. 7 on page 10)** 3. Sequence diagram for surveillance functions 4. Sequence diagram for common functions 5. Use case diagram 6. Refinement of some use case scenario 7. Refinement of sequence diagram 8. Finding reference from SEPA 9. Writing overview
Team member 20230943
1. Use case diagram for security functions 2. Use case diagram for configure safety zone functions 3. Use case diagram for surveillance functions 4. Sequence diagram for security functions 5. Sequence diagram for surveillance functions 6. Refinement of some use case scenario 7. Refinement of sequence diagram 8. Finding reference from SEPA
Team member 20230970
1. Use case scenario for security functions 2. Sequence diagram for security functions 3. Refinement of some use case scenario 4. Refinement of sequence diagram 5. Plan a project schedule 6. Finding reference from SEPA
Team member 20230988
1. Use case scenario for surveillance functions 2. Use case scenario for security functions 3. Sequence diagram for surveillance functions 4. Finding reference from SPEA 5. Refinement of some use case scenario 6. Refinement of sequence diagram 7. Finding reference from SEPA
Team member 20231008
1. Use case scenario for common functions **2.** Sequence diagram for common functions 3. Refinement of some use case scenario 4. Refinement of sequence diagram 5. Finding reference from SEPA

IX. Meeting logs

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

Date: 27 October 2025
Participants: 20230943, 20231008, 20230988, 20230970
Main Responsible: 20230943
Agenda / Tasks Discussed:

Use Case Diagrams: Security Function, Configure Safety Zone Function, Surveillance Function

Sequence Diagrams:
• Delete / Update existing safety zone
• Configure SafeHome modes
• View intrusion log
• Call monitoring service
• Set / Delete camera password
• View thumbnail shots
• Enable / Disable camera

Check for conflicts

Discussion Summary & Decisions:
Team discussed the flow of safety and camera operations. Verified consistency between Security and Surveillance functions. Agreed on naming conventions and consistent actor usage across diagrams.

Next Actions / Notes:
20230943 will refine diagrams and resolve identified conflicts before the next meeting. Others will review for logical consistency.

Date: 28 October 2025
Participants: 20230943, 20231008, 20230988, 20230970
Main Responsible: 20231008
Agenda / Tasks Discussed:

Common Use Cases:
• Log onto the system (control panel / web browser)
• Configure system setting
• Turn system on / off
• Reset system
• Change master password

Sequence Diagrams for corresponding use cases

Discussion Summary & Decisions:
Discussed system authentication flow and general control functions. Decided to unify login interfaces and ensure secure master password update process.

Next Actions / Notes:
20231008 will finalize common use case diagrams and prepare initial sequence diagrams for review. Others will test consistency with the security module.

Date: 29 October 2025
Participants: 20230943, 20231008, 20230988, 20230970
Main Responsible: 20230988
Agenda / Tasks Discussed:

Security Use Cases: Configure SafeHome modes, View intrusion log, Call monitoring service

Surveillance Use Cases:
• Display specific camera view
• Pan / Zoom camera view
• Begin / Stop camera recording
• Replay camera recording
• Set / Delete camera password
• Enable / Disable camera

Sequence Diagrams: Display / Pan / Zoom / Record / Replay camera view

Discussion Summary & Decisions:
Focused on camera-related system features. Discussed real-time constraints, user control flow, and error handling. Confirmed UI trigger points for surveillance actions.

Next Actions / Notes:
20230988 will detail sequence flows and ensure consistency with previous camera control requirements. The team will review integration with the Security module.

Date: 31 October 2025
Participants: 20230943, 20231008, 20230988, 20230970
Main Responsible: 20230970
Agenda / Tasks Discussed:

Security Use Cases:
• Arm / Disarm system (control panel / web browser)
• Selective safety zone control
• Alarm condition
• Configure / Create / Delete / Update safety zone

Sequence Diagrams for corresponding use cases

Discussion Summary & Decisions:
Finalized arm/disarm and safety zone workflows. Clarified alarm triggers and their connection with the monitoring service. Agreed on error conditions and zone update rules.

Next Actions / Notes:
20230970 will complete remaining sequence diagrams. All members will cross-check with 20230943's earlier diagrams for uniformity.

Appendix A. Glossary

1. Control panel: a small gadget to display basic information and receive your commands
    1. See Fig. 1 in page 6, use case “Log onto the system through control panel” in page 11, and …
2. Safety Zone: A designated area or section of the home where specific security rules (e.g., alarm or sensor activation) are applied.
3. Arm / Disarm: To activate (arm) or deactivate (disarm) the SafeHome security system or safety zones.
4. Intrusion Log: A record of detected intrusion events stored by the system.
5. Surveillance Mode: Mode that manages camera-related operations such as viewing, recording, and replaying video.
6. Monitoring Service: External or internal service that receives alerts when the system detects an alarm or emergency.
7. User Authentication: The process of verifying a user’s identity before granting access to system features.
8. Use Case: A specific interaction or functionality that describes how a user (actor) interacts with the system.
9. Actor: An entity (user, device, or external system) that interacts with the SafeHome system.
10. Sequence Diagram: A UML diagram showing how system components or actors interact over time for a specific function.