Software Analysis Models

for

SafeHome project

Version 1.0

Prepared by Jinho Choi, Junsu Kim, Le Do Tuan Khanh

Team 4

Mar 29th 2009

Software Analysis Models

for

SafeHome project

Version 1.0

Prepared by Jinho Choi, Junsu Kim, Le Do Tuan Khanh

Team 4

Mar 29th 2009

Revisions

Version	Primary Author(s)	Description of Version	Date Completed
1.0	Jinho Choi Junsu Kim Le Do Tuan Khanh	Software analysis model frame making	Mar 29th 2009

Contents

List of figures

List of tables

1 Introduction

1.1 Purpose

This analysis model document describes the use cases, use case diagrams, use case scenarios and swimlane diagrams for the SafeHome project which is carried out by the members of Team 4 as their Software Engineering course's final project.

1.2 Intended Audience and Reading Suggestions

This document is intended to be used by Team 4's members who implement the SafeHome project. The document is to help the understanding and collaboration between team members. Besides, the document is also aimed for Professor and Teaching Assistants (TAs) to evaluate the project and Team 4's performance.

The organization of the document is as follows:
- Chapter 1 provides an overview of this document and SafeHome project.
- Chapter 2 describes use cases, use case diagrams, and swimlane diagrams for the SafeHome system.
- Chapter 3 describes the traceability between use cases of the system.

In addition, readers can make use of the Term Index (Appendix A) and Glossary (Appendix B) for a faster mining through the document. Meanwhile, Meeting Minutes (Appendix C) and Who-did-what List (Appendix D) are geared to support the supervision of Professor and TAs, as the senior managers of the project, over the team work's allocation. Interested readers can also refer to the Reference Materials (Appendix E) for more information about some specific themes.

2 System Features

2.1 List of Actors

Primary Actor	Use Cases
User	
Sensor/Motion detector	
Monitoring company	

2.2 Overall system

2.2.1 Descriptions

User can access SafeHome system directly via Control Panel interface or wirelessly via Web interface to use system's functionality suits including secure the house, observe the house and configure the system.

These functionality suits will be described as different system features in the following subsequent sections.

2.2.2 Use Case Diagram
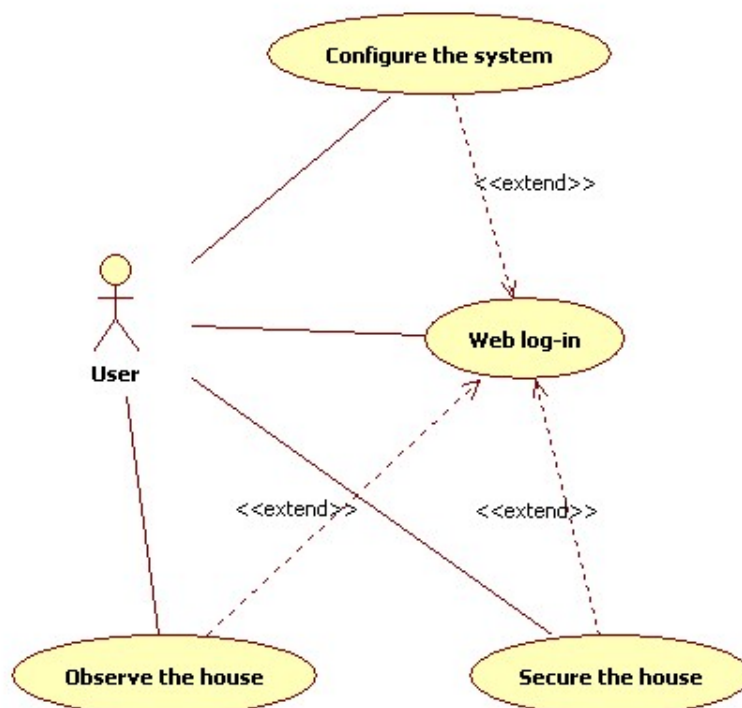
Figure 1 – Use case diagram for overall system

2.2.3 Use Case Scenarios

2.2.3.1 Web log-in

Use Case ID:	UC1		
Use Case Name:	Web log-in		
Created By:	Khanh	Last Updated By:	Khanh
Date Created:	Mar 28th 2009	Date Last Updated:	Mar 28th 2009

Actors:	Web user
Description:	Web user accesses SafeHome system via Web interface to control his/her house, either locally or remotely. The web log-in contains of a web user id, web password and Control Panel password.
Trigger:	N/A.
Preconditions:	N/A.
Postconditions:	1. Web user shall be verified for using further functionalities.
Normal Flow:	**1.0 Web log-in** 1. Web user enters user id and web password to log into the web interface. 2. System retrieves the user id and web password from Central Processor to check for a match. 3. System informs web user to enter Control Panel password 4. Web user enters Control Panel password. 5. System retrieves Control Panel password from Central Processor to check for a match. 6. System informs log-in success and navigate web user to the main web interface.
Alternative Flows:	**1.1 Web log-out before Control Panel log-in** (at step 4 in 1.0) 1. Web user chooses to log-out of the web interface. 2. System cleans the transaction and moves the web user to the first web log-in page. 3. Go back to step 1.
Exceptions:	**1.0.E.1 Wrong web id, password or Control Panel password** (at step 2 in 1.0) 1. System informs web user the log-in failure and the number of log-in times left (SR1). 2. Go back to step 1. **1.0.E.2 Maximum log-ins reached** (at step 2 in 1.0) 1. System blocks the transaction for 15 minutes and sends a

	notification to monitoring company.
	2. System informs web user about the transaction block and notification to monitoring company.
Includes:	N/A.
Priority:	High.
Frequency of Use:	High.
Business Rules:	N/A.
Special Requirements:	**SR1. Maximum number of subsequent failed log-ins in a block of 15 minutes.** 1. Web id and password failures are up to 5 times. 2. Control Panel password failures are up to 3 times.
Assumptions:	1. Every home owner with a valid web user id and password has only the control over 1 house (1 control panel).
Notes and Issues:	1. Web user id and password can be stored in cookie, but Control Panel password will not be stored locally at all. 2. Remote web log-in shall be logged to the company's server to trace for unauthorized access from Internet.

2.2.4 Swimlane Diagrams
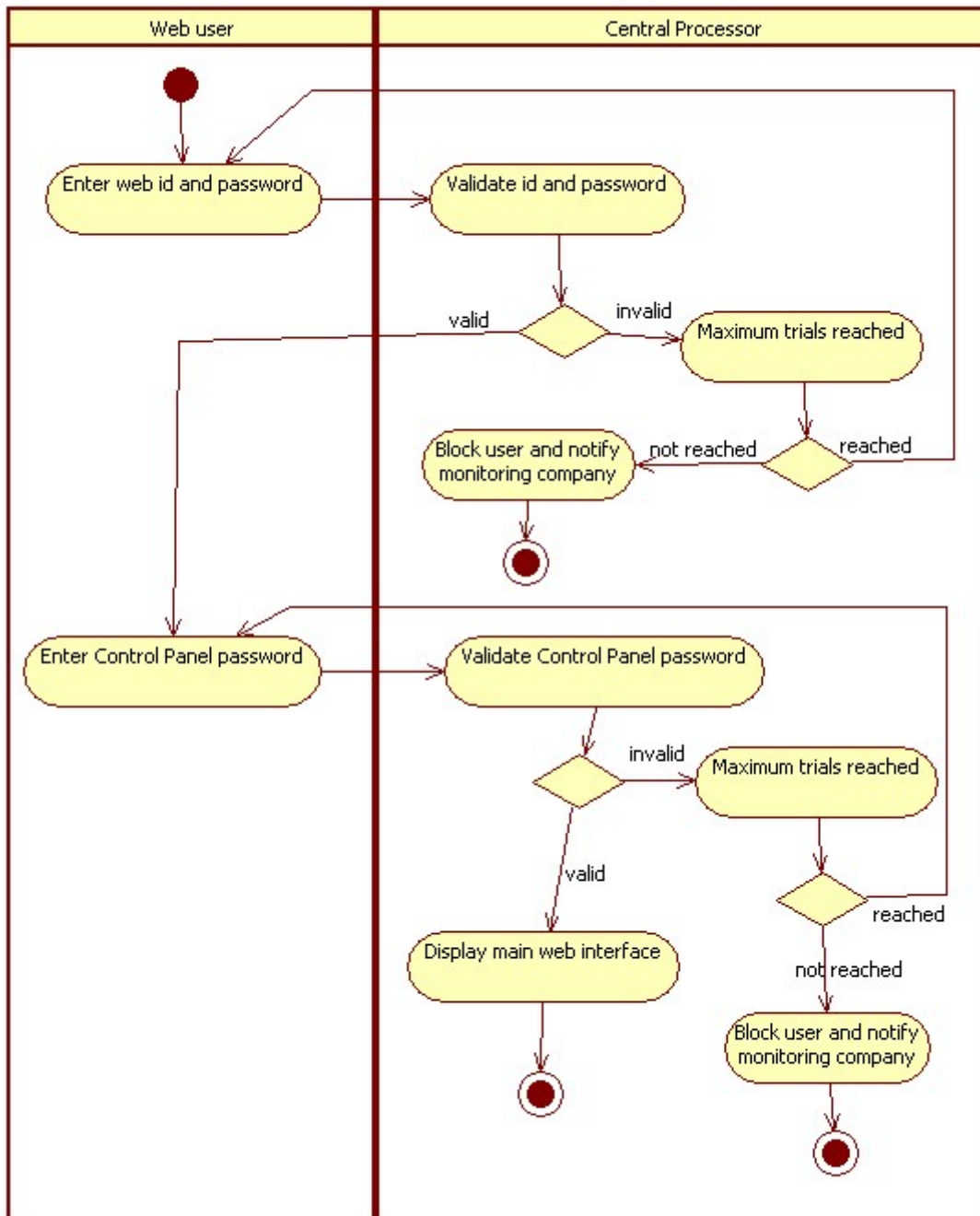
2.2.4.1 Web log-in

2.3 Secure the House

2.3.1 Descriptions

The home owner whose identity has been verified can arm/disarm the house, using control panel or Web interface, with the door sensors, window sensors, motion detectors, fire, CO, smoke level sensors and basement water level sensor. If an intruder or an accident is detected, the system shall alarm and inform the monitoring company. Home owner by his/her-self can announce the

emergency cases (such as heart attack) by request the system to sound the alarm and call the police. In addition, these controls can be performed either locally or via remote devices such as mobile phone or PC using Web interface.

2.3.2 Use Case Diagram
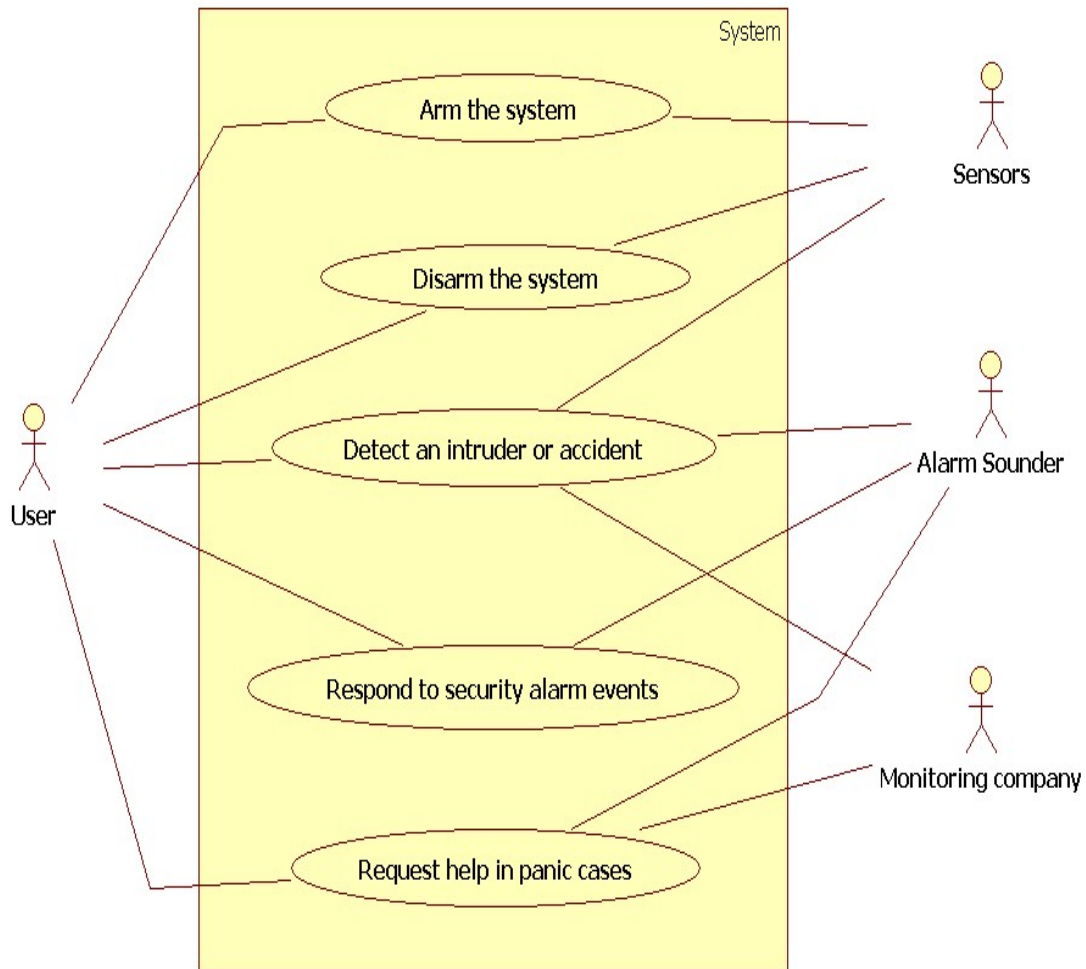
Figure 3 – Use case diagram for "secure the house" feature

2.3.3 Use Case Scenarios

2.3.3.1 Arm the system

Use Case ID:	UC11		
Use Case Name:	Arm the system		
Created By:	Jinho Choi	Last Updated By:	Jinho Choi
Date Created:	Mar 5th 2009	Date Last Updated:	Mar 28th 2009

Actors:	User
	Sensors

Description:	The user activates the sensors and motion detectors from the control panel or via web interface.
Trigger:	User decides to arm the system.
Preconditions:	1. If user uses web interface, user is logged the system.
	2. User has valid password for control panel.
	3. System is in ready mode.
	4. System must be fully configured.
Postconditions:	1. System is in armed condition.
Normal Flow:	**11.0 Arm the system via web interface**
	1. User selects "stay" or "away" button
	2. System checks the input button.
	3. System activates the sensors.
	4. System checks status of sensors.
	5. User observes armed condition of system
Alternative Flows:	**11.1 Arm the system from control panel**
	1. User selects "stay" or "away" button.
	2. System checks the input button.
	3. System requests password.
	4. User enters password.
	5. System checks the password.
	6. System activates the sensors.
	7. System checks status of sensors.
	8. User observes armed condition of system.
Exceptions:	**11.0.E.1 Enter wrong control panel password (**step 4 in 11.1**)**
	1. User enters wrong password.
	2. System requests password by 5 times.
	If the number of times is over 5, system shall announce the monitoring company
	11.0.E.2 No predefined configuration for security zones
	(step 3 in 11.0, step 6 in 11.1**)**
	1. System activates the sensors.
	2. If there is no configuration, system activates all sensors inside house.
	11.0.E.3 Can't activate the sensors (step 4 in 11.0, step 7 in 11.1**)**
	1. System checks the sensors.
	2. If Sensors cannot be activated, system should clearly inform user what condition error is.

Includes:	N/A
Priority:	High
Frequency of Use:	Many times per day
Business Rules:	1. If system is not ready, user must check all sensors to determine which are open and close it. It's not responsibility of monitoring company.
Special Requirements:	1. All web pages generated by the system shall be fully downloadable in no more than 10 seconds over a 40KBps modem connection 2. Security protocol shall be used in communications in networking. 3. Connection from remote control shall be lead through a proxy server provided by a reliable company 4. Information on web access to system shall be stored and monitored by the monitoring company to detect web hacking
Assumptions:	1. Only one user can use the system
Notes and Issues:	1. How can system check the status of sensors when system activates sensors? 2. How can system notify error conditions via control panel and web interface effectively?

2.3.3.2 Disarm the system

Use Case ID:	UC12		
Use Case Name:	Disarm the system		
Created By:	Jinho Choi	Last Updated By:	Jinho Choi
Date Created:	Mar 7th 2009	Date Last Updated:	Mar 29th 2009

Actors:	User Sensors
Description:	The user deactivates the sensors from the control panel or via web interface.
Trigger:	User decides to disarm the system.
Preconditions:	1. If user uses web interface, user is logged the system. 2. User has valid password for control panel. 3. System is in armed condition. 4. System must be fully configured.
Postconditions:	1. System is in disarmed condition
Normal Flow:	**12.0 Disarm the system via web interface** 1. User selects "reset" button. 2. System checks the input button.

	3. System deactivates the sensors
	4. System checks status of sensors.
	5. User observes disarmed condition of system.
Alternative Flows:	**12.1 Disarm the system from control panel**
	1. User selects "reset" button.
	2. System checks the input button.
	3. System requests password.
	4. User enters password.
	5. System checks the password.
	6. System deactivates the sensors.
	7. System checks status of sensors.
	8. User observes disarmed condition of system.
Exceptions:	**12.0.E.1 Enter wrong control panel password (**step 4 in 12.1**)**
	1. User enters wrong password.
	2. System requests password by 5 times.
	If the number of times is over 5, system shall announce the monitoring company
	12.0.E.2 Can't deactivate the sensors (step 3 in 12.0, step 6 in 12.1**)**
	1. System deactivates the sensors.
	2. If Sensors cannot be deactivated, system should clearly inform user what condition error is.
Includes:	N/A
Priority:	High
Frequency of Use:	Many times per day
Business Rules:	N/A
Special Requirements:	1. All web pages generated by the system shall be fully downloadable in no more than 10 seconds over a 40KBps modem connection
	2. Security protocol shall be used in communications in networking.
	3. Connection from remote control shall be lead through a proxy server provided by a reliable company
	4. Information on web access to system shall be stored and monitored by the monitoring company to detect web hacking
Assumptions:	1. Only one user can use the system
Notes and Issues:	1. In the case of away mode, the system shall ask the user to

	suspend for 2 minutes before activating the system. Could user disarm the system in 2 minutes?

2.3.3.3 Request help in panic cases

Use Case ID:	UC13		
Use Case Name:	Request help in panic cases		
Created By:	Jinho Choi	Last Updated By:	Jinho Choi
Date Created:	Mar 7th 2009	Date Last Updated:	Mar 29th 2009

Actors:	User Alarm sounder Monitoring company
Description:	User requests help in panic cases
Trigger:	User decides to request help
Preconditions:	1. If user uses web interface, user is logged the system 2. System is in armed condition 3. System must be fully configured.
Postconditions:	1. System sounds an alarm and is in panic condition
Normal Flow:	**13.0 Request help in panic cases** 1. User selects "panic" button to request help. 2. System checks the input button. 3. System commands alarm sounder to alarm. 4. Alarm sounder gives the alarm. 5. System announces to monitoring company. 6. User observes the panic condition of system.
Alternative Flows:	N/A
Exceptions:	N/A
Includes:	N/A
Priority:	High
Frequency of Use:	Rarely
Business Rules:	1. When monitoring company accepts the panic events, monitoring company must notify the homeowner information to police station
Special Requirements:	1. When the internet connection is broken, the system shall ask the home owner for changing to telephone line 2. Security protocols shall be used in communication in networking

Assumptions:	1. Control panel is located the place children cannot reach it.
Notes and Issues:	1. When home owner requests help, how could monitoring company notify the home owner's situation to police station or 119 station quickly?

2.3.3.4 Detect intruder or accident

Use Case ID:	UC14		
Use Case Name:	Detect intruder or accident		
Created By:	Jinho Choi	Last Updated By:	Jinho Choi
Date Created:	Mar 7th 2009	Date Last Updated:	Mar 29th 2009

Actors:	Sensors Alarm sounder User Monitoring Company
Description:	Intruder breaks in the house or fire, CO, smoke, and basement water level is detected to be dangerous.
Trigger:	Intruder, fire, CO, smoke, water
Preconditions:	1. If home owner uses web interface, home owner logged the system. 2. System is in armed condition. 3. System must be fully configured.
Postconditions:	1. Alarm sounder is sounding an alarm.
Normal Flow:	**14.0 Detect intruder or accident** 1. Sensors detect dangerous something such as an intruder, fire, smoke, CO, smoke and basement water level. 2. Sensors immediately announce the detection information (open signal) to system. 3. System checks the detection information of sensor. 4. System commands alarm sounder to alarm. 5. System sends the emergency message to the monitoring company. 6. Monitoring company and home owner views the detection information. 7. User observes the detection information.
Alternative Flows:	N/A
Exceptions:	N/A
Includes:	N/A

Priority:	High
Frequency of Use:	Rarely (Whenever the system detects dangerous something to secure home)
Business Rules:	N/A
Special Requirements:	1. All web pages generated by the system shall be fully downloadable in no more than 10 seconds over a 40KBps modem connection
	2. Security protocol shall be used in communications in networking.
	3. Connection from remote control shall be lead through a proxy server provided by a reliable company
	4. Information on web access to system shall be stored and monitored by the monitoring company to detect web hacking
	5. The time between detecting an intruder or an accident and alarming the case shall be within 1 second
Assumptions:	N/A
Notes and Issues:	N/A

2.3.3.5 Respond the security alarm events

Use Case ID:	UC15		
Use Case Name:	Respond the security alarm events		
Created By:	Jinho Choi	Last Updated By:	Jinho Choi
Date Created:	Mar 7th 2009	Date Last Updated:	Mar 28th 2009

Actors:	User
	Alarm sounder
Description:	User responds the security alarm events
Trigger:	Alarm events
Preconditions:	1. If monitoring company responds the security alarm events, monitoring company is logged the system.
	2. System is in armed condition.
	3. System must be fully configured.
Postconditions:	2. The security problem is solved.
	3. Alarm sounder stops alarming
Normal Flow:	**15.0 Respond the alarm by user**
	1. User checks the alarm event.
	2. User enters password.
	3. System checks the password.

	4. System commands alarm sounder to stop alarming.
	5. Alarm sounder stops alarming.
	6. User observes to stop alarming.
Alternative Flows:	**15.1 Respond the alarm by monitoring company**
	1. Monitoring company checks the alarm events.
	2. Monitoring company commands system to stop alarming.
	3. System receives the command.
	4. System commands alarm sounder to stop alarming.
	5. Alarm sounder stops alarming.
Exceptions:	**15.0.E.1 Can't respond the security alarm events (step 1 in 15.0)**
	1. User can't respond the alarm event.
	2. After 1 minute, system announces the security alarm event to monitoring company.
	15.0.E.2 Enter wrong control panel password (step 2 in 15.0)
	1. User enters wrong password.
	2. System requests password by 5 times.
	If the number of times is over 5, system shall announce the monitoring company
Includes:	N/A
Priority:	High
Frequency of Use:	Rarely (Whenever the alarm events happens)
Business Rules:	1. When user can't respond the security alarm events, monitoring company will send staff to his/her home for checking the security situation.
Special Requirements:	1. When security alarming event happens, system disables all other functions and waiting user password
Assumptions:	N/A
Notes and Issues:	N/A

2.3.4 Swimlane Diagrams

2.3.4.1 Arm the system via web interface
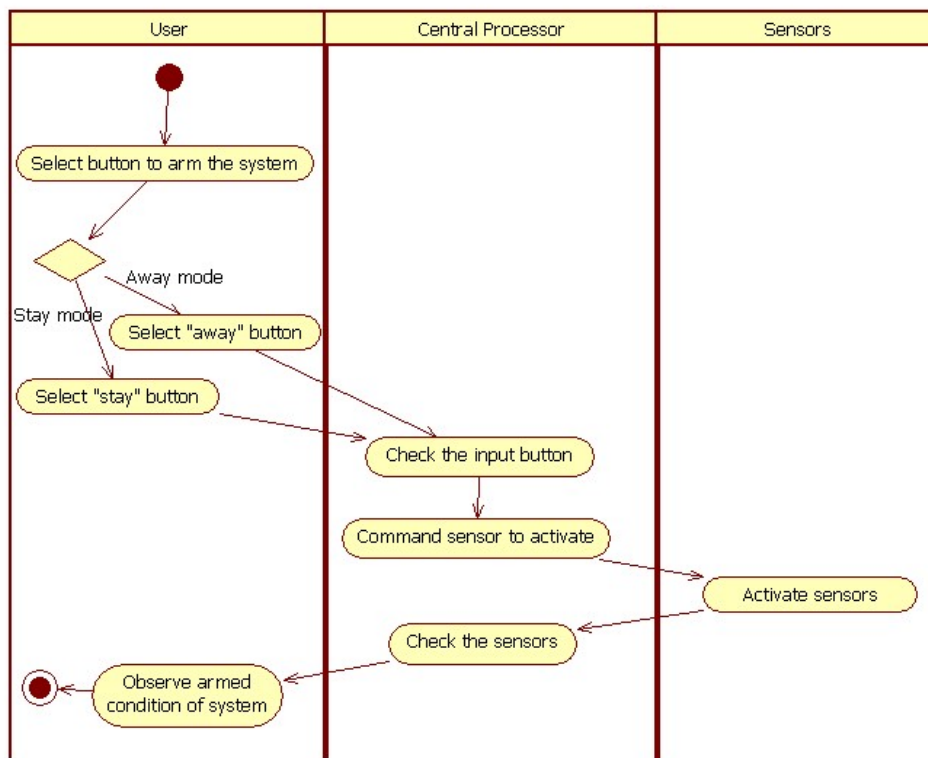
2.3.4.2 Arm the system from control panel
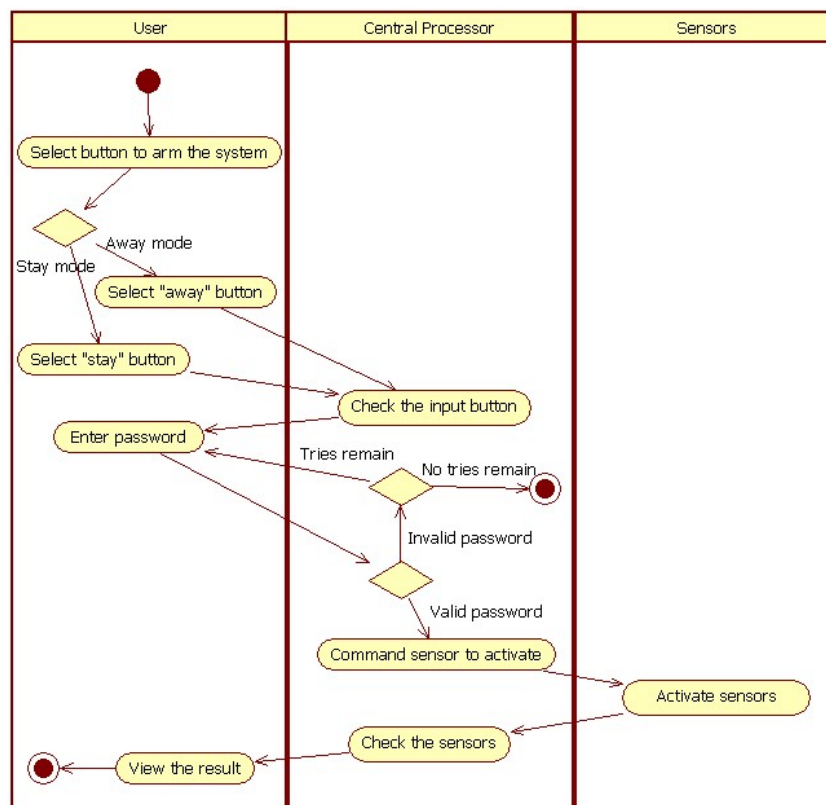
2.3.4.3 Disarm the system via web interface
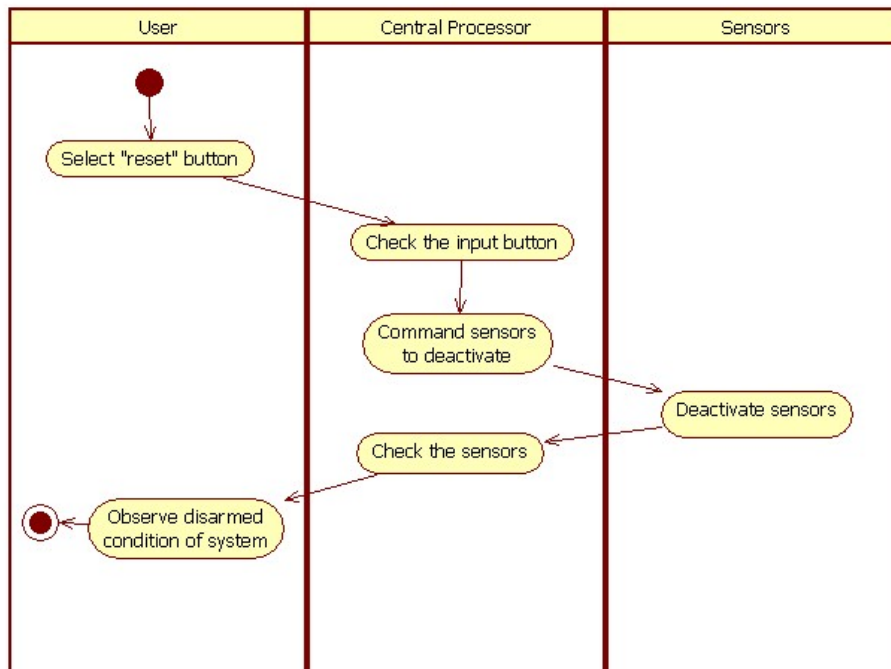
Figure 6 – Swimlane diagram for Disarm the system via web interface

2.3.4.4 Disarm the system from control panel
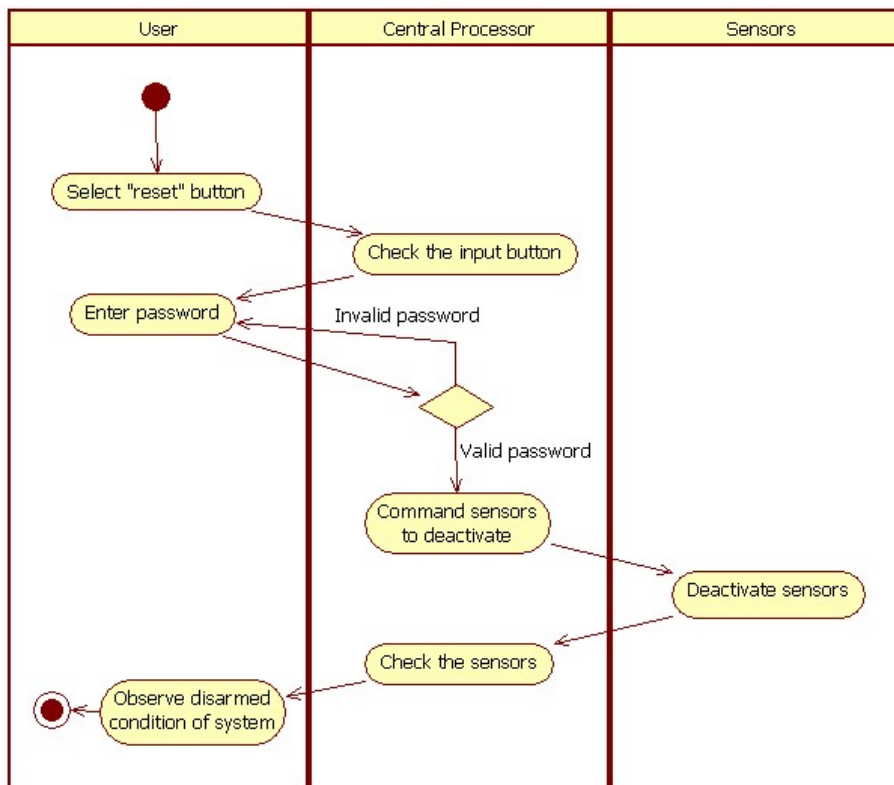
Figure 7 – Swimlane diagram for Disarm the system from control panel

2.3.4.5 Request help in panic cases
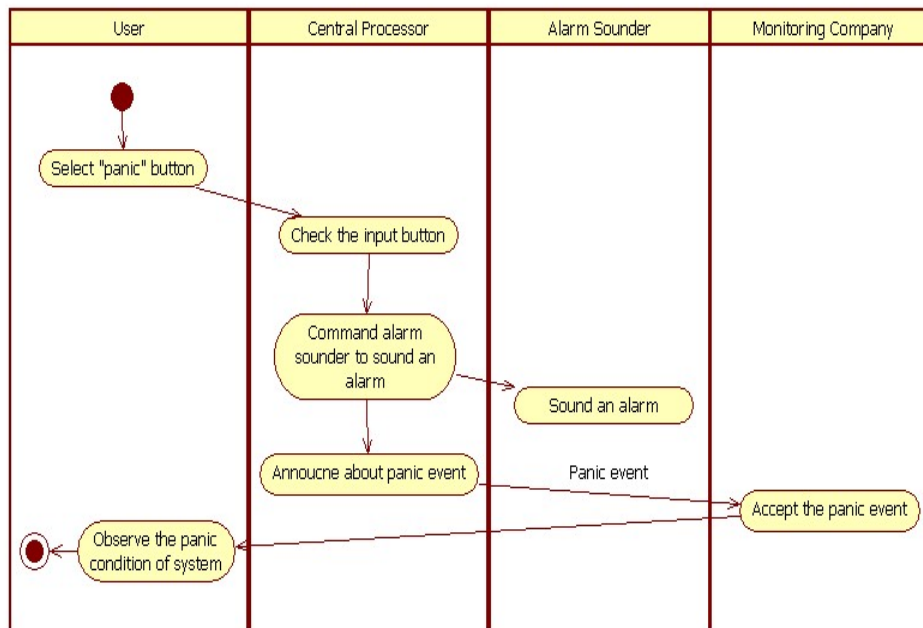
Figure 8 – Swimlane diagram for Request help in panic cases

2.3.4.6 Detect intruder or accident
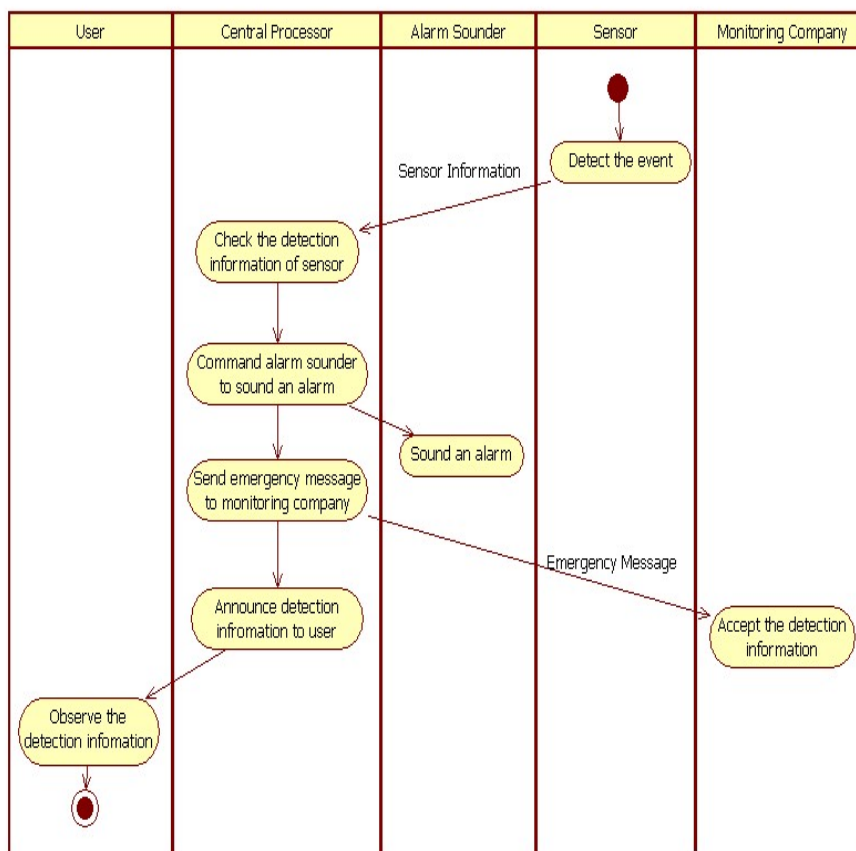
Figure 9 – Swimlane diagram for Detect intruder or accident

2.3.4.7 Respond the alarm by user
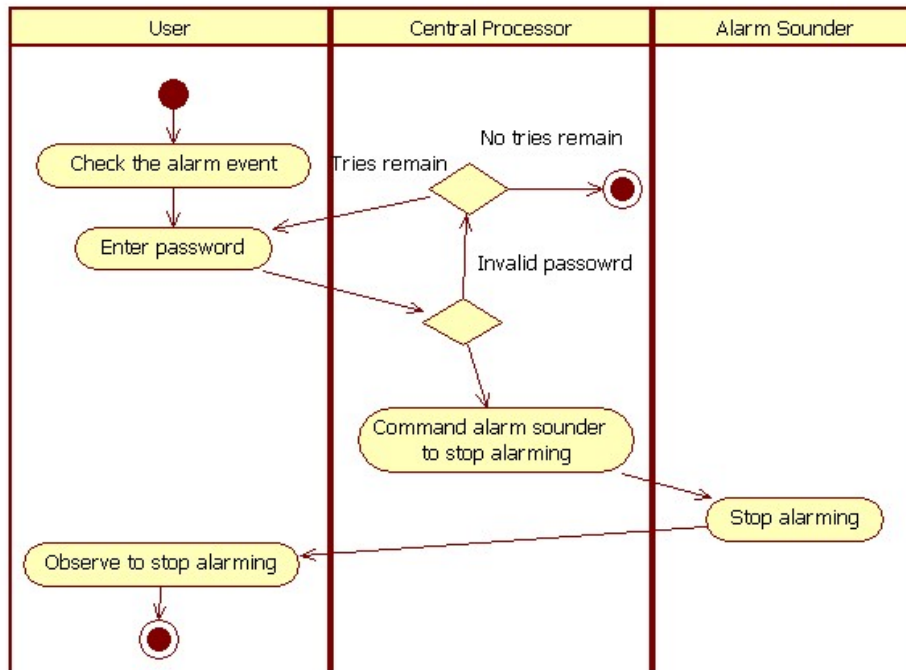
Figure 10 – Swimlane diagram for Respond the alarm by user

2.3.4.8 Respond the alarm by monitoring company
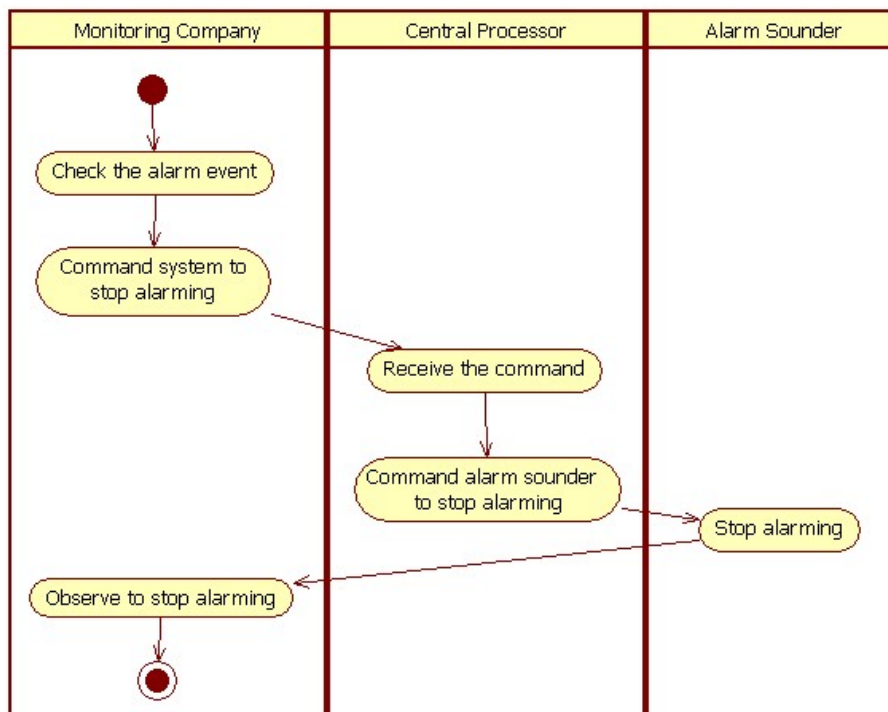
Figure 11 – Swimlane diagram for Respond the alarm by monitoring company

2.4 Observe the House

2.4.1 Descriptions

The home owner whose identity has been verified can observe the inside and outside of the house received from the wireless connected cameras via Web interface. The home owner can choose the camera(s) to view as well as zoom or pan the displays. In addition, the home owner can also record the scenes that he/she wants and play back the stored records. Similar to the "Secure the house" feature, this feature can be controlled locally or remotely.

2.4.2 Use Case Diagram
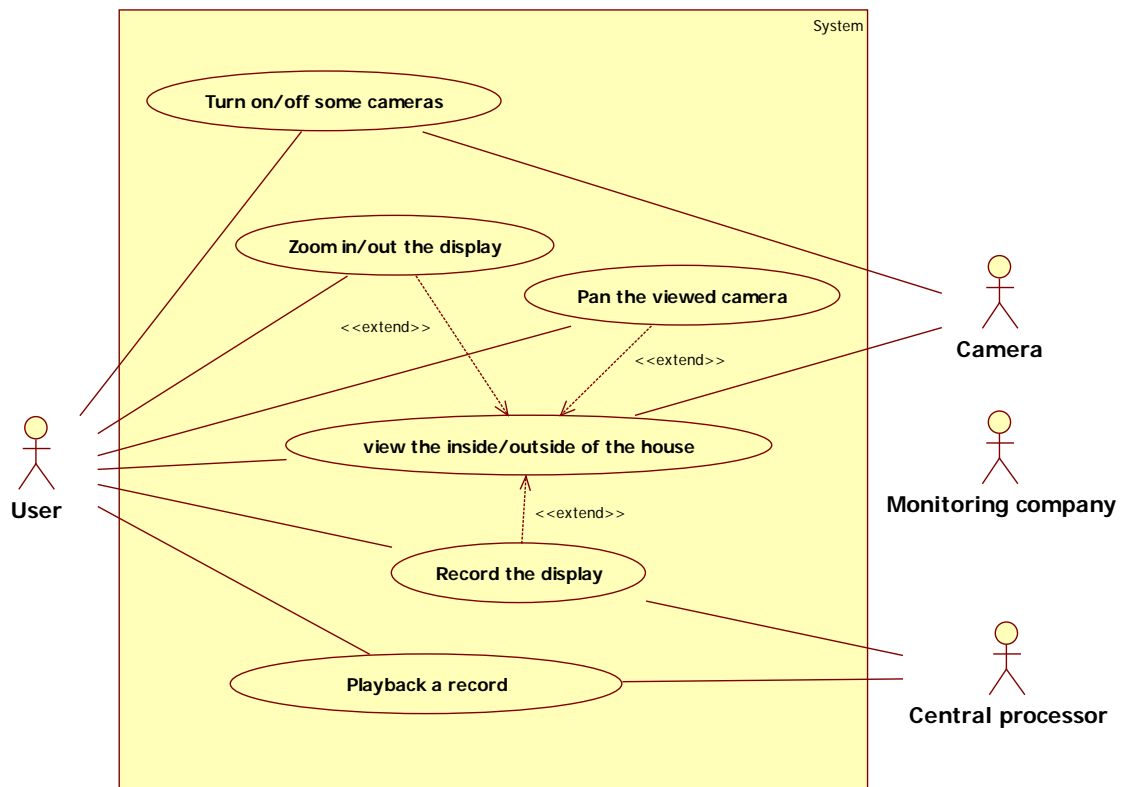
Figure 12 - Use case diagram for "Observe the house" feature

2.4.3 Use Case Scenarios

2.4.3.1 View In & Out

Use Case ID:	UC100		
Use Case Name:	View the inside/outside of the house		
Created By:	Jun su Kim	Last Updated By:	Jun su Kim
Date Created:	Mar 26th 2009	Date Last Updated:	Mar 26th 2009

Actors:	User
	Central Processor

	Camera
Description:	The User can view the inside or outside of house through cameras.
Trigger:	N/A.
Preconditions:	1. Cameras always operate even though the Central Processor turns out. 2. The surveillance zones are predefined. 1. User has logged into SafeHome Web interface
Postconditions:	N/A.
Normal Flow:	**100.0 View In & Out** 1. The user selects "surveillance" from the major function button. 2. The user selects "pick a camera" 3. The system displays the floor plan of the house. 4. The user selects a camera icon from the floor plan. 5. The user selects the "view" button. 6. The system displays a viewing window that is identified by the camera ID. (SR 100.0) 7. The system displays video output within the viewing window at specific frame per second. (SR 100.1)
Alternative Flows:	**100.1 View thumbnail snapshots** (branch at step2 in 100.0) 1. The user selects "thumbnail view". 2. The system displays the snapshots for all cameras. 3. The user selects a snapshot from all snapshots. 4. The user selects the "view" button. 5. The system displays a viewing window that is identified by the camera ID. (SR 100.0) 6. The system displays video output within the viewing window at specific frame per second. (SR 100.1)
Exceptions:	**100.0.E.1 A floor plan is not available or has not been configured** (at step 3 in 100.0) 1. System informs the user the error encountered and rolls back the erroneous action. (see use-case "configure the floor plan") **100.0.E.2 Cannot display video output** (at step 7 in 100.0, at step 7 in 100.1) 1. System displays default steal image. 2. System informs the user the error encountered and rolls back the erroneous action.

Includes:	N/A
Priority:	High
Frequency of Use:	Infrequent
Business Rules:	N/A
Special Requirements:	**SR100.1 ID of camera** • ID of camera is assigned by manufacturing company. • There is no duplicated ID. **SR100.2 Frame per second** • Video output displays at one frame per second.
Assumptions:	1. The website for surveillance is always available. 2. There is no disconnection for using.
Notes and Issues:	N/A.

2.4.3.2 Pan and zoom the camera

Use Case ID:	UC101		
Use Case Name:	Pan and zoom the camera		
Created By:	Junsu Kim	Last Updated By:	Junsu Kim
Date Created:	Mar 26th 2009	Date Last Updated:	Mar 29th 2009

Actors:	User Central Processor Camera
Description:	The User can pan viewed cameras to left-side and right-side or zoom in/out current display of camera.
Trigger:	N/A.
Preconditions:	1. Cameras always operate even though the central processor turns out. 2. The surveillance zones are predefined. 3. User has logged into SafeHome Web interface. 4. User has viewed video output within the viewing window,
Postconditions:	N/A
Normal Flow:	**101.0 Pan the camera** 1. The user changes the extent of pan (SR101.2) 2. The system makes camera refocused according to the extent of pan 3. The system displays paned video output within the viewing window. **101.1 Zoom the camera**

	1. The user changes the level of zoom (SR101.2) 2. The system makes camera refocused according to the level of zoom 3. The system displays zoomed video output within the viewing window.
Alternative Flows:	N/A
Exceptions:	**101.0.E.1 the camera does not operate during viewing.** (at step 3 in 101.0, at step 3 in 101.1) 1. System displays default steal image. 2. System informs the user the error encountered and rolls back the erroneous action.
Includes:	N/A
Priority:	Low
Frequency of Use:	Infrequent
Business Rules:	N/A
Special Requirements:	**SR101.1 extent of pan** • The directions of pan are right-side and left-side. • There is limit to pan the camera. **SR101.2 Level of zoom** • There is limit to zoom the camera.
Assumptions:	The website for surveillance is always available.
Notes and Issues:	N/A

2.4.3.3 Record the scenes

Use Case ID:	UC102		
Use Case Name:	Record the scenes		
Created By:	Junsu Kim	Last Updated By:	Junsu Kim
Date Created:	Mar 26th 2009	Date Last Updated:	Mar 29th 2009

Actors:	User Central Processor Camera
Description:	The moving images of whole cameras are recorded separately.
Trigger:	N/A
Preconditions:	1. Cameras always operate even though the central processor turns out. 2. The surveillance zones are predefined. 3. User has logged into SafeHome Web interface

Postconditions:	N/A
Normal Flow:	**102.0. Record display** 1. The cameras capture moving images and send to central processor. 2. The system checks enough space to record. (SR102.1) 3. The system assigns keyword to record for later searching. (SR102.2) 4. The system records moving images.
Alternative Flows:	**102.1. Not enough space to record** (branch at step2 in 102.0) 1. Old records are move to secondary storage. 2. The moving to secondary storage are continuing until obtain enough capacity. 3. The system assigns keyword to record for later searching. (SR102.2) 4. The system records moving images.
Exceptions:	**102.0.E.1 All cameras do not work.** (at step1 in 102.0) 1. System informs the user the error encountered and stop recording.
Includes:	
Priority:	High
Frequency of Use:	Always
Business Rules:	1. If the secondary storage is almost full, the monitoring company changes the secondary storage to empty one. Then keeping the storage for several months.
Special Requirements:	**SR102.2 Enough space to record** • The space should be available for 24 hour recording **SR102.2 Keyword of record** • The keyword is combined by ID of camera and the date that recorded the moving images.
Assumptions:	1. The time to assign keyword is very short so it is not necessary to wait to complete assigning keywords. 2. The backup starts before storage is full so central processor always has the storage to records.
Notes and Issues:	

2.4.3.4 Play back record

Use Case ID:	UC104
Use Case Name:	Playback the record

Created By:	Junsu Kim	Last Updated By:	Junsu Kim
Date Created:	Mar 26th 2009	Date Last Updated:	Mar 29th 2009

Actors:	User Central Processor Camera
Description:	User can play back the records and look the old records.
Trigger:	N/A
Preconditions:	1. Cameras always operate even though the central processor turns out. 2. The surveillance zones are predefined. 3. User has logged into SafeHome Web interface.
Postconditions:	N/A
Normal Flow:	**104.0. Play back record** 1. The user selects "surveillance" from the major function button. 2. The user selects "playback". 3. The system display searching window, 4. The user enters keywords in searching window. 5. The user selects "search" button. 6. The system checks the searching constraints (SR104.1) and searches the records that match for keywords. (SR 104.2) 7. The system displays the results of searching. 8. The user selects one record from the results. 9. The user selects the "view" button. 10. The system displays a selected record within viewing window
Alternative Flows:	N/A
Exceptions:	**104.0.E.1 Violate searching constraint** 1. System informs the user the error encountered and requires user to enter correct keywords again **104.0.E.2 Not matching keyword** (at step 6 in 104.0) 1. The systems shows empty result and requires user to enter other keywords again **104.0.E.3 Cannot display record** (at step 10 in 104.0) 1. System displays default steal image. 2. System informs the user the error encountered and rolls back the erroneous action.
Includes:	N/A.

Priority:	Normal
Frequency of Use:	Infrequent
Business Rules:	N/A
Special Requirements:	**SR104.1 Searching constraint.** • The keyword for searching at least 2 characters or numbers. • The English alpha is available only. **SR104.2 Keyword for searching** • The keywords are only ID of camera or the date that recorded the moving images.
Assumptions:	1. The website for surveillance is always available.
Notes and Issues:	1. How can user playback the records during the records are in back up,

2.4.3.5 Turn on/off some cameras

Use Case ID:	UC105		
Use Case Name:	Turn on/off some cameras		
Created By:	Junsu Kim	Last Updated By:	Junsu Kim
Date Created:	Mar 26th 2009	Date Last Updated:	Mar 29th 2009

Actors:	User Central Processor Camera
Description:	User can turn on/off cameras and surveillance zone. User can see current status of cameras.
Trigger:	N/A
Preconditions:	1. Cameras always operate even though the central processor turns out. 2. The surveillance zones are predefined. 3. User has logged into SafeHome Web interface.
Postconditions:	N/A
Normal Flow:	**105.0. View statuses of cameras** 1. The user selects "surveillance" from the major function button. 2. The user selects "Turn on/off" 3. The system displays statues of cameras within the floor plan of the house.

	4. The user selects a camera icon from the floor plan.
	5. The user selects "turn on" or "turn off"
	6. The system turn camera on or off according to user's selection.
Alternative Flows:	**105.1. Turn on/off surveillance zone** (branch at step4 in 105.0)
	1. The user select surveillance zone.
	2. The user selects "turn on" or "turn off".
	3. The system turn surveillance zone on or off according to user's selection.
Exceptions:	**105.0.E.2 turn off the camera that do recording**
	1. The systems ask to user again for confirmation.
	2. If user confirm the "turn off", stop recording and turn off the camera.
Includes:	N/A
Priority:	Normal
Frequency of Use:	Infrequent
Business Rules:	N/A
Special Requirements:	N/A.
Assumptions:	1. The website for surveillance is always available.
	2. It is possible to communicate to cameras through wireless LAN.
Notes and Issues:	N/A

2.4.4 Swimlane diagrams

2.4.4.1 Turn on/off some cameras
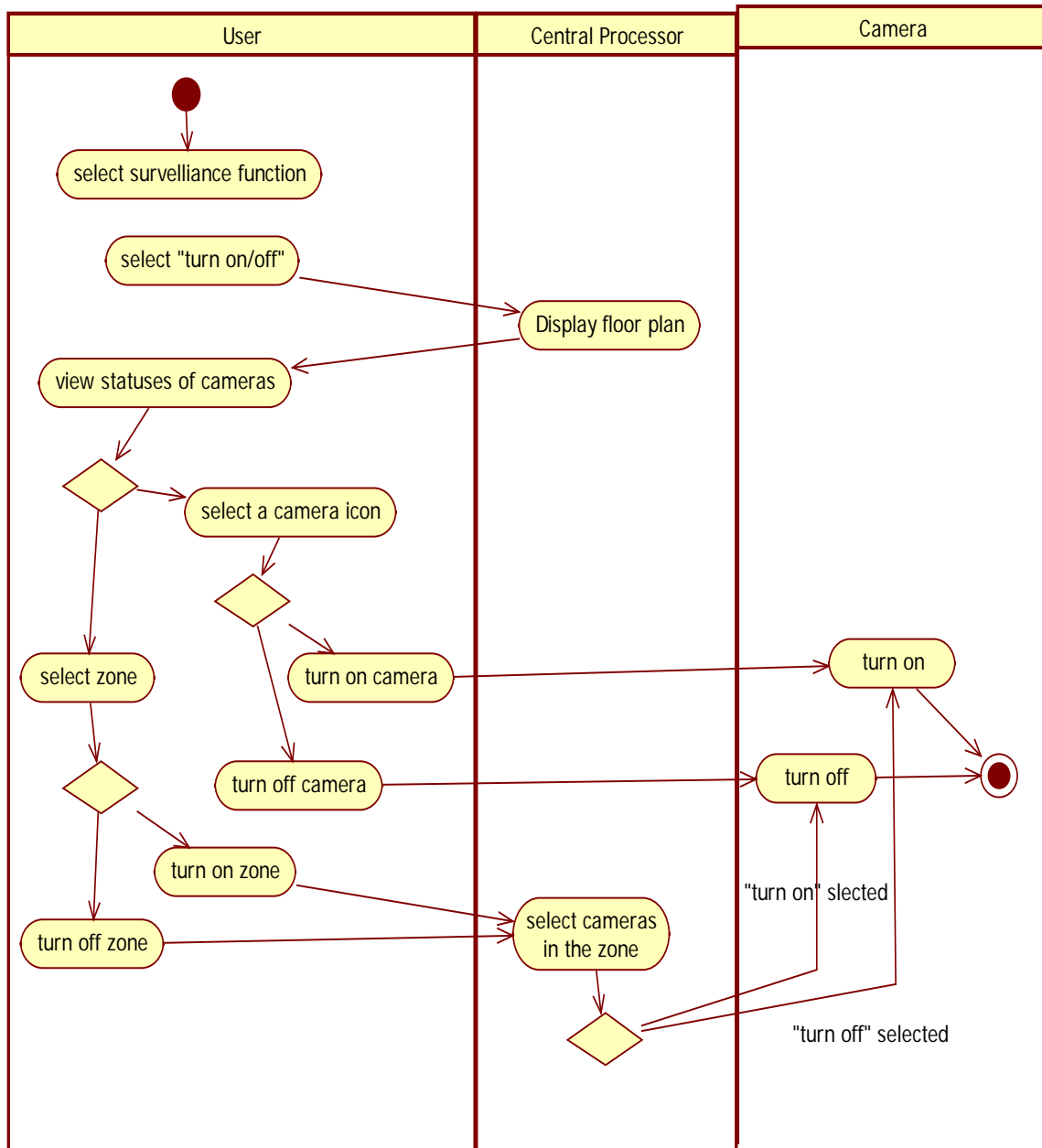
Figure 13 – Swimlane diagram for Turn on/off some cameras

2.4.4.2 View the inside/outside of the house

User	Central Processor	Camera

select survelliance function

select "pick a camera"

select "thunmbnail view"

Display floor plan

Display all snapshots

select a snapshots

select a camera icon

select "view" button

capture images

generate video ouput

encrypt

view camera output
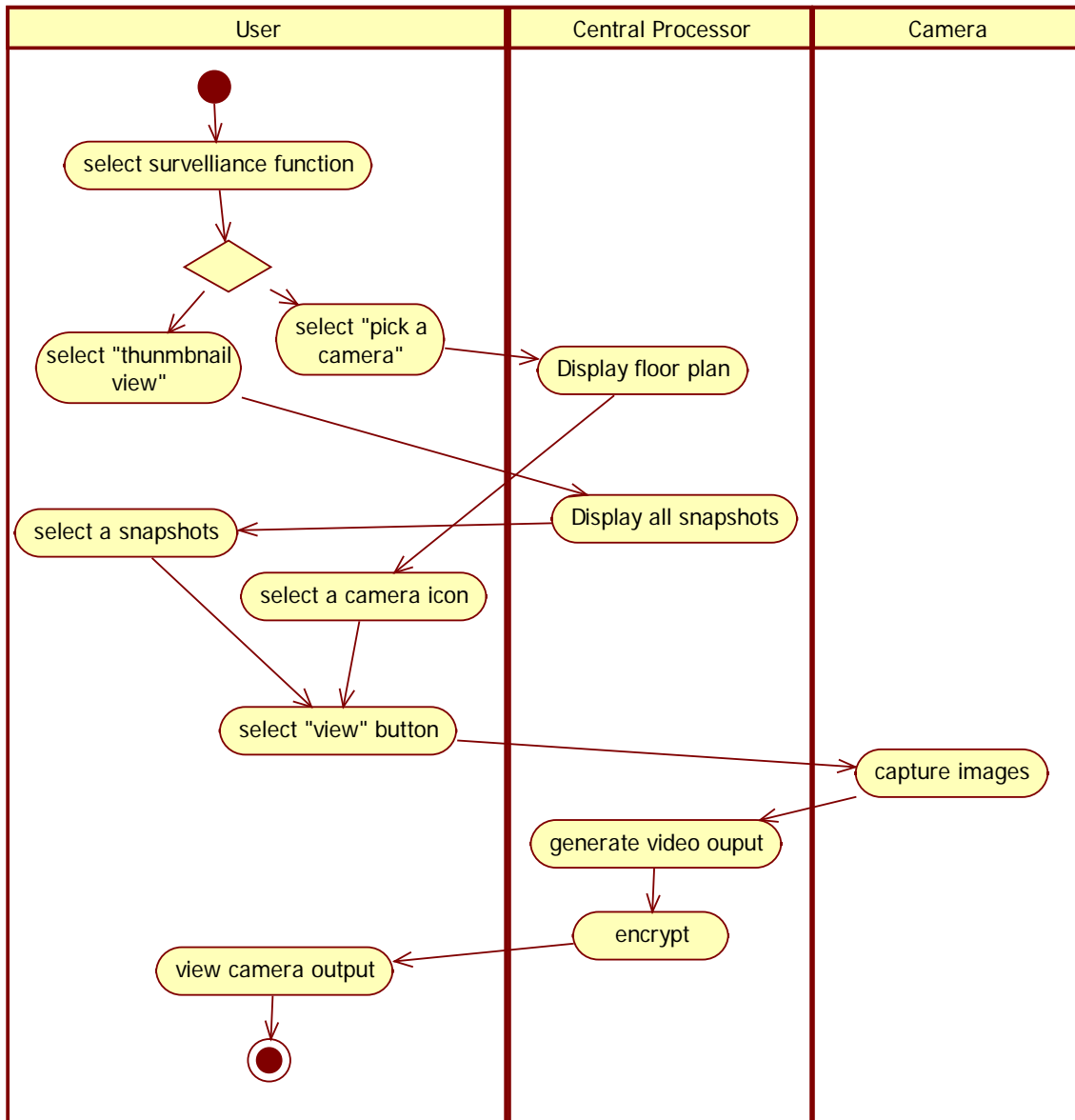
Figure 14 - Swimlane diagram for View the inside/outside of the house

2.4.4.3 Pan and zoom the camera
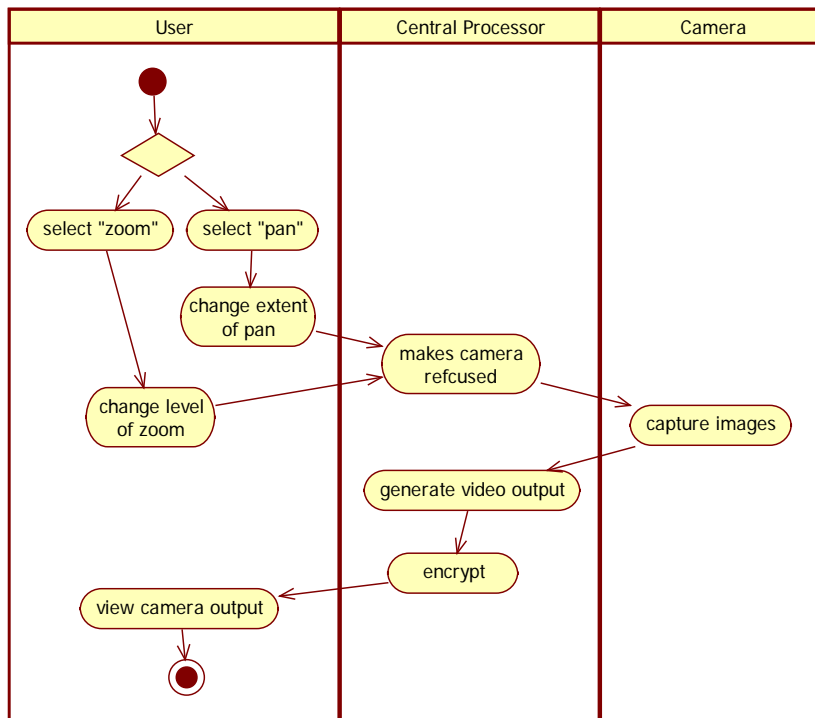
Figure 15 - Swimlane diagram for Pan and zoom the camera

2.4.4.4 Record the scenes
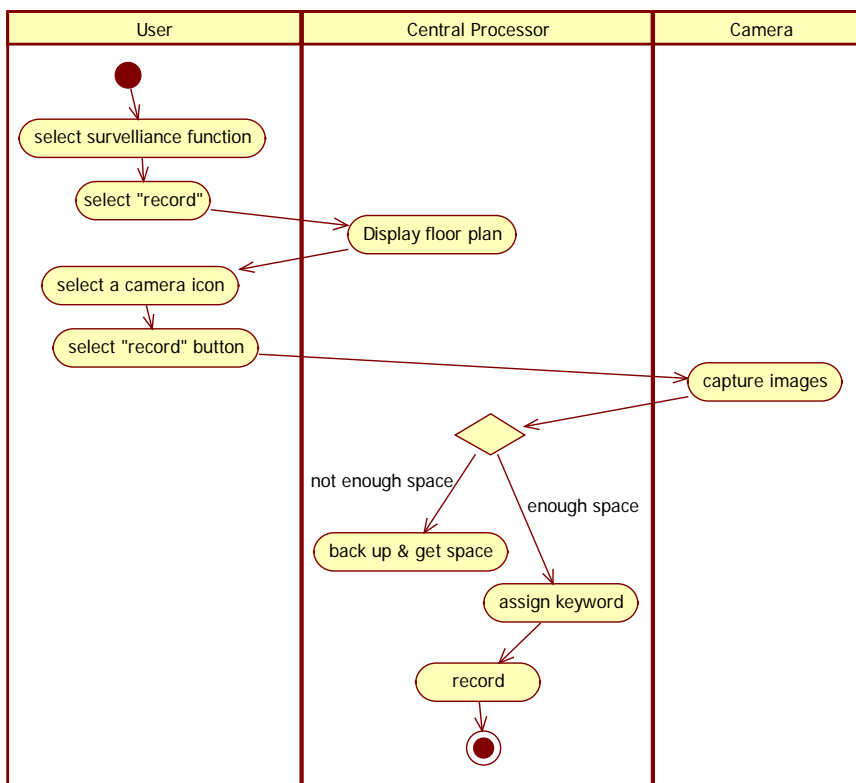
Figure 16 - Swimlane diagram for Record the scenes

2.4.4.5 Playback a record

Figure 17 - Swimlane diagram for Playback a record

2.5 Configure the system

2.5.1 Descriptions

The home owner whose identity has been verified can dynamically reconfigure the floor plan of the house as well as define/redefine the security/surveillance zones. In addition, the home owner can also manage his/her account information and passwords, including web password and control panel password. Control panel password can be changed via either control panel interface or web interface. The other activities can be performed only via Web interface, either locally or remotely.

2.5.2 Use Case Diagram
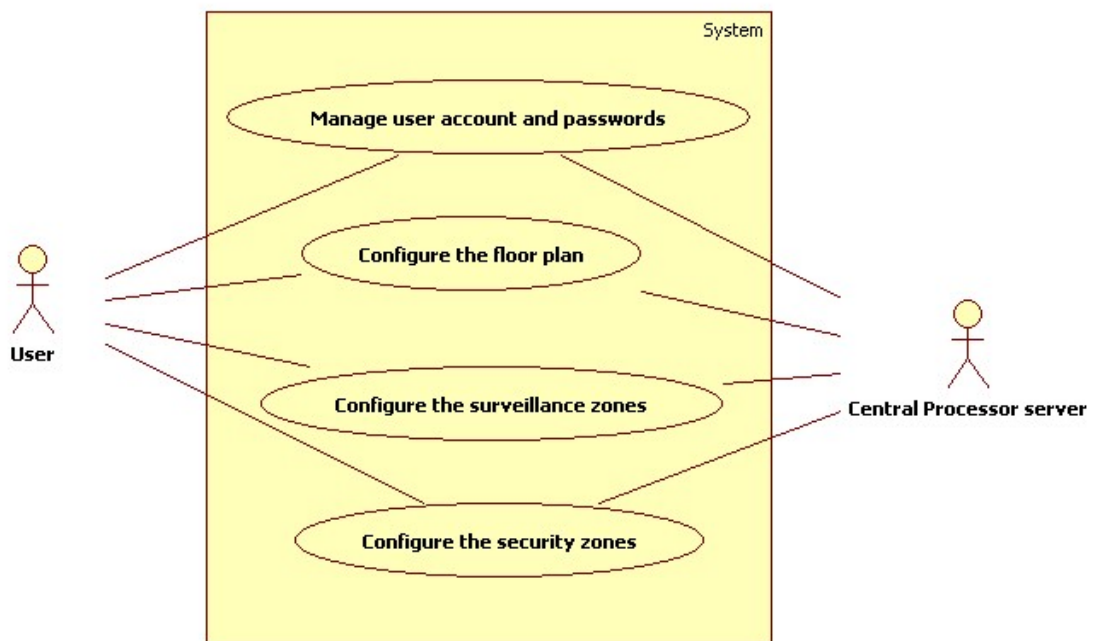
<p align="center">**Figure 18 - Use case diagram for "Configure the system" feature**</p>

2.5.3 Use Case Scenarios

2.5.3.1 Manage user account and passwords

Use Case ID:	UC31		
Use Case Name:	Manage user account and passwords		
Created By:	Khanh	Last Updated By:	Khanh
Date Created:	Mar 25th 2009	Date Last Updated:	Mar 26th 2009

Actors:	User
Description:	Authorized user accesses the SafeHome system via Web interface (locally or remotely) to modify his/her account information, including Control Panel password and web access password. In

	addition, managing the Control Panel password can be performed via Control Panel interface.
Trigger:	User decides to edit his/her account or change the passwords.
Preconditions:	5. User has logged into SafeHome Web interface (not applied for Control Panel interaction).
Postconditions:	1. User account information and passwords shall be changed. 2. Current screen shall be navigated away (not applied for Control Panel interface).
Normal Flow:	**31.0 Manage user account and passwords via Web interface.** 4. User asks to manage the user account and passwords. 5. System displays the user's account information (R31). 6. User asks to edit the account information. 7. System enables the fields that user can change. 8. User changes the information and confirms to submit the changes to the system. 9. System checks the information's constraints (SR31.2) and store to the Central Processor server. 10. Except for control panel password, other information shall be sent and stored to the company's server. 11. System informs change success to user.
Alternative Flows:	**31.1 Change control panel password via Control Panel interface** 1. User asks to change the control panel password. 2. System waits for user to change the password. 3. User enters new password. 4. System checks for the password's constraint (SR31.2). 5. System stores the new password to the Central Processor and informs change success to user.
Exceptions:	**31.0.E.1 No Internet connection** (at step 7 in 31.0) 1. System detects that there is no Internet connection, so no information can be transferred to the company's server. 2. System informs the problem to user. 3. Finish the use case. **31.0.E.2 Web connection times out** (at any step in 31.0) 1. System detects that user hasn't had any interaction with web interface for a period of time (SR31.3), automatically logs the user out and informs him/her the reason. 2. User wants to extend the transaction. 3. Go back to step 1 in 31.0.

	31.1.E.1 Control panel times out (at any step in 31.1)
	1. System detects that there is no input from user for a period of time (SR31.3), automatically cancels the current request (transaction) and informs to the user.
	31.1.E.2 Request denied due to another being executed request (at both steps 1 in 31.0 and 31.1)
	1. System detects that there is another task being executed from another interface, denies the request from user.
	2. User waits until the system is ready for new task.
	3. Go back to step 1 in 31.0.
Includes:	N/A.
Priority:	High.
Frequency of Use:	One a week is suggested.
Business Rules:	**R31 User account information includes**
	R31.1 User id and user name (unchangeable).
	R31.2 User's current address (unchangeable).
	R31.3 User's contact email (changeable).
	R31.4 User's web interface password (changeable).
	R31.5 User's control panel password (changeable).
Special Requirements:	**SR31.1 The password should be changed in this below sequence**
	• Confirm the old password
	• Enter the new password and a re-type for confirmation
	SR31.2 User information's constraints
	• Contact email should be valid.
	• Web interface password should have at least 6 characters.
	• Control Panel password should have exactly 4 digits.
	SR31.3 Time out time
	• Web time out shall be 10 minutes.
	• Control panel time out shall be 5 seconds.
Assumptions:	1. Assume that one user has only one house facilitated with the SafeHome system.
Notes and Issues:	1. The private user's information and passwords sent on the Internet line shall be encoded and transferred safely.
	2. Since there are many interfaces supported by the system, SafeHome system shall pay attention to the consistency and correctness of the user's password changes when receiving several requests from different interfaces.
	3. Safely encrypted data transference and communication

	should be used in the case of remote control.

2.5.3.2 Configure the surveillance zones

Use Case ID:	UC32		
Use Case Name:	Configure the surveillance zones		
Created By:	Khanh	Last Updated By:	Khanh
Date Created:	Mar 26th 2009	Date Last Updated:	Mar 26th 2009

Actors:	User
Description:	Via Web interface, an authorized user can configure the surveillance zones, including adding, modifying and deleting some of the zones. In addition, some combination of surveillance zones can be selected to constitute the "Stay" or "Away" mode.
Trigger:	User decides to configure the surveillance zones.
Preconditions:	1. User has logged into SafeHome Web interface.
Postconditions:	1. Surveillance zones are updated. 2. "Stay" and "Away" modes are updated. 3. Configuration changes are stored to server.

Normal Flow:	**32.0 Configure the surveillance zones.**
	 1. User asks to configure the surveillance zones.
	 2. System visually displays the current effective zones to be configured.
	 3. User configures the surveillance zones.
	    • Adds, removes some surveillance zones (Flow 32.1).
	    • Modifies existed zones (Flow 32.2).
	      o Adds, removes some cameras.
	    • Attaches, detaches some zones to/from the "Stay" or "Away" mode (Flow 32.3).
	 4. System simultaneously checks for the zone's constraints (SR32.1) while user is configuring the surveillance zones.
	 5. System informs change success to user and error detail if an error is encountered.

Alternative Flows:	**32.1 Add, delete surveillance zones** (branch at step 3 in 32.0)
	 1. User asks to add/remove a surveillance zone
	    • Add: user chooses a camera to be included in the new zone.
	    • Delete: user chooses a zone to be deleted.
	 2. System confirms for the every change, applies to the current

	executing system and stores the configuration to the Central Processor server. 3. System informs the change success and go back to step 3 in 32.0. **32.2 Modify existed zones** (branch at step 3 in 32.0) 1. User selects a zone to be modified. 2. User asks to add/remove several cameras to/from the zone. 3. System confirms only after all adding/removing for a zone are finished from the user. 4. System informs the change success and go back to step 3 in 32.0. **32.3 Configure "Stay" or "Away" mode** (branch at step 3 in 32.0) 1. User selects a surveillance zone. 2. System displays the current status of if the zone is in "Stay" or "Away" mode or both or none of the two. 3. User selects/deselects the modes for the zone. 4. System confirms to apply to the current executing system and stores the configuration to the Central Processor server. 5. System informs the change success and go back to step 3 in 32.0.
Exceptions:	**32.0.E.0 Constraint error detected** (at step 4 in 32.0) 1. System detects a constraint error from user's configuring. 2. System informs the user the error encountered and rolls back the erroneous action. 3. Go back to the current branch at step 3 in 32.0. **32.0.E.1 Web connection times out** (at any step in 32.x) 1. System detects that user has had any interaction with web interface for a period of time (SR32.3), automatically logs the user out and informs him/her the reason. 2. User wants to extend the transaction. 3. Go back to the current branch at step 3 in 32.0.
Includes:	N/A.
Priority:	High.
Frequency of Use:	Rarely.
Business Rules:	N/A
Special Requirements:	**SR32.1 Surveillance zone's constraints** - One surveillance zone should contain at least 1 camera. - One camera may be contained in several zones.

	• System shall contain at least 1 surveillance zone.
	SR32.2 Transaction extension
	• Transaction can only be extended with web password's provision from user.
	SR32.3 Time out time
	• Web time out shall be 10 minutes.
	• Control panel time out shall be 5 seconds.
Assumptions:	1. The surveillance zones were initially established satisfying the surveillance zone's constraints (SR32.1).
	2. Cameras placed by floor plan configuration are existent and correctly working.
Notes and Issues:	1. Some cameras may have some problems (e.g. unable to connect to) that should be detected automatically by the system. System shall ignore change requests to such problematic cameras.
	2. Safely encrypted data transference and communication should be used in the case of remote control.

2.5.3.3 Configure the security zones

Use Case ID:	UC33		
Use Case Name:	Configure the security zones		
Created By:	Khanh	Last Updated By:	Khanh
Date Created:	Mar 27th 2009	Date Last Updated:	Mar 27th 2009

Actors:	User
Description:	Via Web interface, authorized user can configure the security zones, including adding, modifying and deleting some of the zones. In addition, some combination of security zones can be selected to constitute the "Stay" or "Away" mode.
Trigger:	User decides to configure the security zones.
Preconditions:	1. User has logged into SafeHome Web interface.
Postconditions:	1. Security zones are updated.
	2. "Stay" and "Away" modes are updated.
	3. Configuration changes are stored to server.
Normal Flow:	**33.0 Configure the security zones.**
	1. User asks to configure the security zones.
	2. System visually displays the current effective zones to be configured.

	3. User configures the security zones. 　• Adds, removes some security zones (Flow 33.1). 　• Modifies existed zones (Flow 33.2). 　　○ Adds, removes some sensors and detectors. 　• Attaches, detaches some zones to/from the "Stay" or "Away" mode (Flow 33.3). 4. System simultaneously checks for the zone's constraints (SR33.1) while user is configuring the security zones. 5. System informs change success to user and error detail if an error is encountered.
Alternative Flows:	**33.1 Add, delete security zones** (branch at step 3 in 33.0) 1. User asks to add/remove a security zone 　• Add: user chooses a sensor or motion detector to be included in the new zone. 　• Delete: user chooses a zone to be deleted. 2. System confirms for the every change, applies to the current executing system and stores the configuration to the Central Processor server. 3. System informs the change success and go back to step 3 in 33.0. **33.2 Modify existed zones** (branch at step 3 in 33.0) 1. User selects a zone to be modified. 2. User asks to add/remove several sensors or motion detectors to/from the zone. 3. System confirms only after all adding/removing for a zone are finished from the user. 4. System informs the change success and go back to step 3 in 33.0. **33.3 Configure "Stay" or "Away" mode** (branch at step 3 in 33.0) 1. User selects a security zone. 2. System displays the current status of if the zone is in "Stay" or "Away" mode or both or none of the two. 3. User selects/deselects the modes for the zone. 4. System confirms to apply to the current executing system and stores the configuration to the Central Processor server. 5. System informs the change success and go back to step 3 in 33.0.
Exceptions:	**33.0.E.1 Constraint error detected** (at step 4 in 33.0)

	1. System detects a constraint error from user's configuring.
	2. System informs the user the error encountered and rolls back the erroneous action.
	3. Go back to the current branch at step 3 in 33.0.
	33.0.E.2 Web connection times out (at any step in 33.x)
	1. System detects that user has had any interaction with web interface for a period of time (SR33.3), automatically logs the user out and informs him/her the reason.
	2. User wants to extend the transaction.
	3. Go back to the current branch at step 3 in 33.0.
Includes:	N/A.
Priority:	High.
Frequency of Use:	Rarely.
Business Rules:	N/A
Special Requirements:	**SR33.1 Security zone's constraints** • One security zone should contain at least 1 sensor or motion detector. • One sensor or detector may be contained in several zones. • System shall contain at least 1 security zone. • "Stay" and "Away" modes contain at least 1 security zone. **SR33.2 Transaction extension** • Transaction can only be extended with web password's provision from user. **SR33.3 Time out time** • Web time out shall be 10 minutes. • Control panel time out shall be 5 seconds.
Assumptions:	1. The security zones were initially established satisfying the surveillance zone's constraints (SR33.1). 2. Sensors and motion detectors placed by floor plan configuration are existent and correctly working.
Notes and Issues:	1. Some sensors or motion detectors may have some problems (e.g. unable to connect to) that should be detected automatically by the system. System shall ignore change requests to such problematic sensors or detectors. 2. Safely encrypted data transference and communication should be used in the case of remote control.

2.5.3.4 Configure the floor plan

Use Case ID:	UC34

Use Case Name:	Configure the floor plan		
Created By:	Khanh	Last Updated By:	Khanh
Date Created:	Mar 27th 2009	Date Last Updated:	Mar 27th 2009

Actors:	User
Description:	Via Web interface, authorized user can configure the floor plan of the house. User can place or move the devices (sensors, motion detectors and cameras) around the house's floor plan, i.e. to some pre-specified attachable positions.
Trigger:	User decides to configure the floor plan of the house.
Preconditions:	1. User has logged into SafeHome Web interface.
Postconditions:	1. Floor plan appearance shall be changed. 2. Floor plan configuration changes shall be stored to server.

Normal Flow:	**34.0 Configure the floor plan.**
	1. User asks to configure the floor plan of the house.
	2. System displays the house's floor plan with attached sensors, motion detectors and cameras.
	3. User shall
	   • Place a device into the floor plan (Flow 34.1).
	   • Move a device inside the floor plan (Flow 34.2).
	   • Remove a device from the floor plan (Flow 34.3).
	4. System simultaneously checks special requirement (SR34.1) while user is interacting with the floor plan configuration.
	5. System asks for confirmation for every user's action and stores the configuration change to Central Processor server.
	6. System informs user for every change success and error detail if an error is encountered.

Alternative Flows:	**34.1 Place a device into the floor plan** (branch at step 3 in 34.0) 1. User selects a device type to place into the floor plan 2. System shows positions in the floor plan that selected type of device can be attached to. 3. User attaches the device to an available slot in the floor plan. 4. System checks for the requirement (SR34.2) and attaches the device to the floor plan. 5. Go back to step 3 in 34.0. **34.2 Move a device inside the floor plan** (branch at step 3 in 34.0)

	1. User selects a device attached in the floor plan to move. 2. System shows positions in the floor plan that selected device can be moved to. 3. User moves the device to an available slot in the floor plan. 4. System checks for the requirement (SR34.2), removes the device from the old position and moves it to the new position in the floor plan. 5. Go back to step 3 in 34.0. **34.3 Remove a device from the floor plan** (branch at step 3 in 34.0) 1. User selects a device attached in the floor plan to remove. 2. User selects to remove the device from the floor plan. 3. System confirms and removes the device from its slot and marks the slot as available.
Exceptions:	**34.0.E.1 Constraint error detected** (at step 4 in 34.0) 1. System detects a constraint error from user's configuring. 2. System informs the user the error encountered and rolls back the erroneous action. 3. Go back to the current branch at step 3 in 34.0. **34.0.E.2 Web connection times out** (at any step in 34.x) 1. System detects that user has had any interaction with web interface for a period of time (SR34.4), automatically logs the user out and informs him/her the reason. 2. User wants to extend the transaction. 3. Go back to the current branch at step 3 in 34.0. **34.1.E.1 Device's connectivity unreachable** (at step 4 in 34.1 and 34.2) 1. System can't connect to the attached device. 2. System informs user to check the device's status and rolls back the user's action. 3. Go back to the current branch at step 3 in 34.0.
Includes:	N/A.
Priority:	High.
Frequency of Use:	Rarely.
Business Rules:	N/A.
Special Requirements:	**SR34.1 House devices and zones' constraints** • A security/surveillance zone shall be removed if no sensor, detector/camera is included in. • System shall contain at least 1 security zone and 1

	surveillance zone.
	• Each type of devices has several predefined positions in the floor plan to be placed into.
	• "Stay" and "Away" modes contain at least 1 security zone and 0 surveillance zone.
	SR34.2 House devices' connectivity
	• Every connected device to the floor plan via floor plan configuration shall be checked for its connectivity.
	SR34.3 Transaction extension
	• Transaction can only be extended with web password's provision from user.
	SR34.4 Time out time
	• Web time out shall be 10 minutes.
	• Control panel time out shall be 5 seconds.
Assumptions:	1. Devices shall be attached to the physical locations before attaching via floor plan configuration.
	2. Devices shall be detached from the physical locations after detaching via floor plan configuration.
	3. This configuration should be performed after the system is disarmed to avoid possible conflicts.
Notes and Issues:	1. Every device shall provide an ID that the system can connect to and check for its connectivity.

2.5.4 Swimlane Diagrams

2.5.4.1 Manage user account and passwords
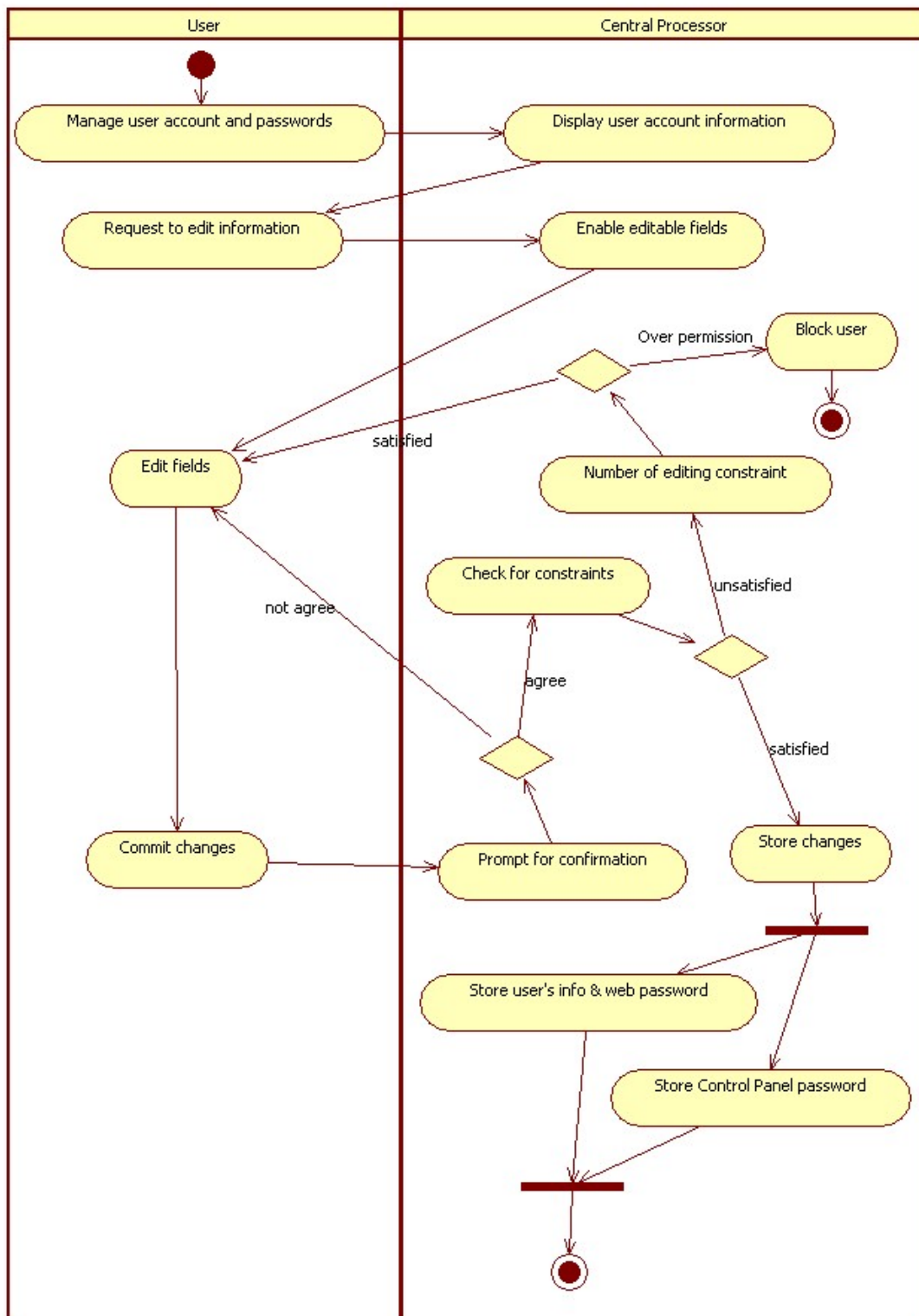
Figure 19 – Swimlane diagram for Manage user account via Web interface
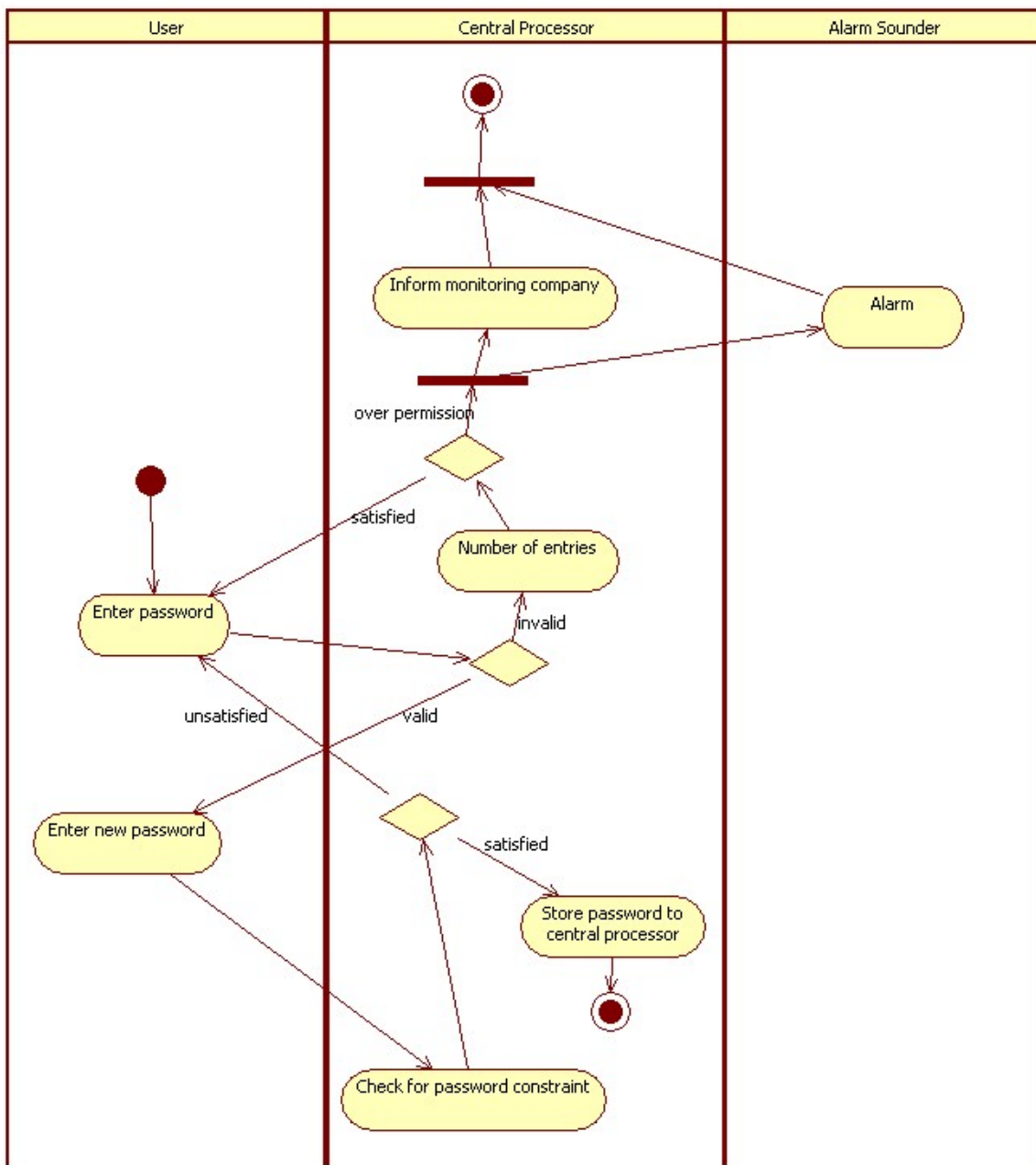
Figure 20 – Swimlane diagram for Manage Control Panel password via Control Panel

2.5.4.2 Configure the surveillance zones

Figure 21 – Swimlane diagram for Configure the surveillance zones

2.5.4.3 Configure the security zones

Figure 22 – Swimlane diagram for Configure the security zones

2.5.4.4 Configure the floor plan

Figure 23 – Swimlane diagram for Configure the floor plan

3 Traceability Matrix

Table 1 – Traceability matrix between use cases

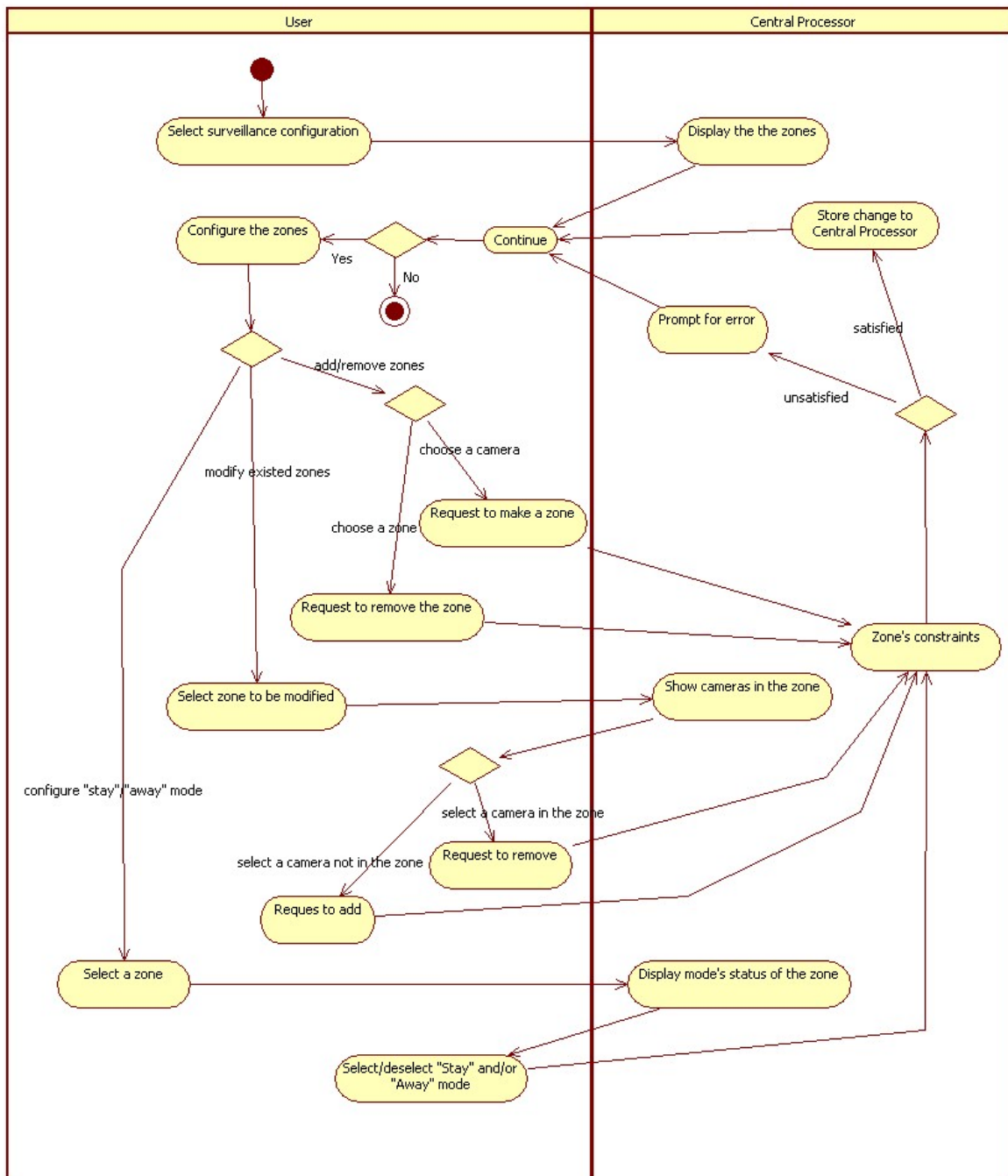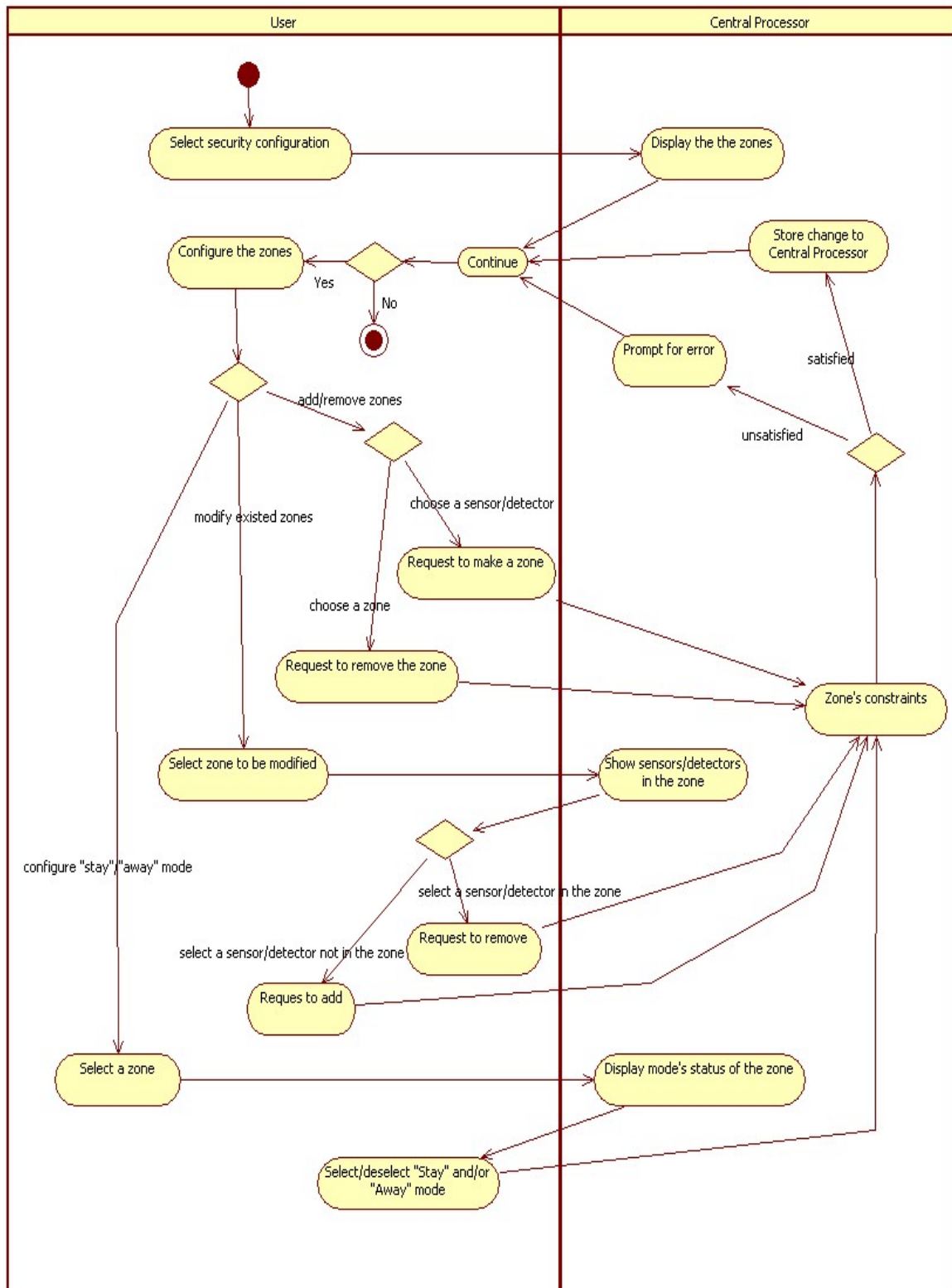| Use cases by system features		Web log-in	Secure the House — Arm the system	Disarm the system	Detect an intruder or accident	Respond to security alarm events	Request help in panic cases	Observe the house — Turn on/off some cameras	Pan and zoom the camera	View the inside /outside of the house	Record the scenes	Playback a record	Configure the system — Manage user account and passwords	Configure the floor plan	Configure the surveillance zones	Configure the security zones
	Web log-in	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Secure the house	Arm the system	✓	✓	✓	✓									✓		✓
	Disarm the system	✓	✓	✓										✓		✓
	Detect an intruder or accident		✓		✓	✓										
	Respond to security alarm events	✓			✓	✓	✓									
	Request help in panic cases					✓	✓									
Observe the house	Turn on/off some cameras	✓						✓		✓	✓				✓	✓	
	Pan and zoom the camera	✓							✓	✓	✓					
	View the inside/outside of the house	✓						✓	✓	✓	✓				✓	✓	
	Record the scenes	✓						✓	✓	✓	✓	✓				
	Playback a record	✓									✓	✓				
Configure the system	Manage user account and passwords	✓											✓			
	Configure the floor plan	✓	✓	✓				✓		✓				✓		
	Configure the surveillance zones	✓						✓		✓					✓	
	Configure the security zones	✓	✓	✓												✓

Appendix A: Term Index

Appendix B: Glossary

Home security: the activities to maintain the safety of the house such as protecting the house from the unauthorized intruders, restricting the house access from authorized visitors and detecting the unexpected dangers (fire) or accidents (heart attack)

Home surveillance: the activities to keep track of the house's status via the cameras placed inside and outside

Control panel: the electronic panel attached on the main door of the house, composing of a small status monitor and a number of control buttons to perform the security functions around the house. A visual illustration of control panel is shown in Chapter 4.2.

Web interface: the user-system's interaction interface that accepts input and provides output by generating web pages which are transmitted via the (Internet or local) network and viewed by the user using a web browser program [Wikipedia].

Security zone: Some of the sensors and motion detectors are grouped together to define a security zone. The security zones regulate the authority and restriction to parts of the house and may overlap each other.

Surveillance zone: Some of the cameras are grouped together to define a surveillance zone. The surveillance zones regulate the home owner's observation to parts of the house and may overlap each other.

"Stay"/"Away" modes: The "Stay"/"Away" modes are the system's configurations in which some of the security zones are enabled and some of the surveillance zones are enabled. Literally, the "Stay" mode provides barely enough security and surveillance to comfort the staying home owner, while "Away" mode provides a standard high level of security and surveillance around the house when the home owner is away.

Sensor: A device that measures a physical quantity and converts it into a signal which can be read by an observer or by an instrument [Wikipedia].

Motion detector: A device that contains a physical mechanism or electronic sensor that quantifies motion that can be either integrated with or connected to other devices that alert the user of the presence of a moving object within the field of view [Wikipedia].

Arm/disarm: The activities to activate/deactivate some predefined sensors and motion detectors

in/out-side of the house. Arm has an abstract meaning which can be set as "Stay" mode, "Away" mode or a complex mode. Whereas, disarm has a single meaning of deactivate all the in-operation sensors and motion detectors.

House condition: The condition of the devices or parts of the houses which are sensor-attached. An opened door or window may cause the house condition an error condition when the home owner wants the system to arm the house.

Central processor: The central processor encompasses the control software (the main part of SafeHome project), which can be accessed via control panel interface or web interface, and a web server to support the wireless network over the house as well as the remote control far away from the house.

Appendix C: Meeting Minutes

1st Meeting – Software Analysis

Minutes   **MAR 16th 2009**   **6:30pm-7:15pm**

NOTE TAKER	Le Do Tuan Khanh
ATTENDEES	Jinho Choi, Junsu Kim, Le Do Tuan Khanh

Agenda topics

6:30PM-7:15PM   Work Allocation

DISCUSSION	

1. The contents need to be delivered for the next phase
2. Work allocation to members

CONCLUSIONS	

1. Fundamental artifacts to be delivered as required
1.1. Use case diagrams and scenarios
1.2. Swimlane diagrams
2. Artifact is in negotiation
2.1. SRS revision
3. Currently, we're going to base on the submitted SRS to derive the use cases and describe use case scenarios. The three features of the system are allocated to our members as in the action items

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
"Secure the house" feature	Jinho Choi	Thu, Mar 19rd 2009
"Observe the house" feature	Junsu Kim	Thu, Mar 19th 2009
"Configure the system" feature	Khanh	Thu, Mar 19th 2009
Analysis presentation	Junsu Kim	Tue, Mar 24th 2009

7:015PM-   Next Meeting

DISCUSSION	NEXT MEETING WILL BE HELD : Thu, Mar 19th 2009, 6:30pm

1. Analyze the SRS's comments and prepare for a modification if necessary
2. Review the assigned work
3. Allocate new tasks to members

SPECIAL NOTES	N/A

2nd Meeting – Software Analysis

Minutes   **MAR 19th 2009   7:00pm-7:50pm**

NOTE TAKER	Jinho Choi
ATTENDEES	Jinho Choi, Junsu Kim, Le Do Tuan Khanh

Agenda topics

7:00PM-7:30PM   Work Allocation

DISCUSSION	

1. Discuss use case of surveillance
2. Progress status by now.

CONCLUSIONS	

1. Solve question about "Observe.Record.Key"
2. Revise SRS document
   - Modify Record the display -> Record the scene
   - Modify the use case diagram
3. Write in use case template
4. Change the work and team presentation deadline

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
"Secure the house" feature	Jinho Choi	Thu, Mar 26th 2009
"Observe the house" feature	Junsu Kim	Thu, Mar 26th 2009
"Configure the system" feature	Khanh	Thu, Mar 26th 2009
Analysis presentation	Junsu Kim	Tue, Mar 30th 2009

7:015PM-   Next Meeting

DISCUSSION	NEXT MEETING WILL BE HELD : Thu, Mar 26th 2009, 7:00pm

1. Analyze the SRS's comments and prepare for a modification if necessary
2. Discuss the use case, use case diagram, and swimlane diagram of each feature
3. Prepare team presentation of "Analysis Model"

SPECIAL NOTES	Do our best about the project and examination of Software Engineering Class

----

3rd Meeting – Software Analysis

Minutes   **MAR 27th 2009   7:00pm-8:50pm**

NOTE TAKER	Jinho Choi
ATTENDEES	Jinho Choi, Junsu Kim, Le Do Tuan Khanh

Agenda topics

7:00PM-8:30PM   Work Allocation

DISCUSSION	
1. Discuss what team members did until now.	
2. How to remove the inconsistency of document	

CONCLUSIONS	
1. Remove the inconsistency the actor name	
2. Junsu must redraw the swinlane diagram with StarUML tool.	
3. Write use case and draw swimlane diagram clearly.	

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
Elaborate "Secure the house" feature	Jinho Choi	Thu, Mar 26th 2009
Elaborate "Observe the house" feature	Junsu Kim	Thu, Mar 26th 2009
Elaborate "Configure the system" feature	Khanh	Thu, Mar 26th 2009
Analysis presentation	Junsu Kim	Tue, Mar 30th 2009

8:30PM-   Next Meeting

DISCUSSION	NEXT MEETING WILL BE HELD : Thu, Mar 26th 2009, 7:00pm
4. Analyze the SRS's comments and prepare for a modification if necessary	
5. Discuss the use case, use case diagram, and swimlane diagram of each feature	
6. Prepare team presentation of "Analysis Model"	

SPECIAL NOTES	

Appendix D: Who did what List

Task	Jinho Choi	Junsu Kim	Le Do Tuan Khanh
SRS revision for "Secure the house"	✓		
SRS revision for "Observe the house"		✓	
SRS revision for "Configure the system"			✓
SRS revision for traceability matrix	✓	✓	✓
Introduction (Chapter 1)	✓		
Overall system (Chapter 2.1)			✓
Secure the house feature (Chapter 2.2)	✓		
Observe the house feature (Chapter 2.3)		✓	
Configure the house (Chapter 2.4)			✓
Traceability matrix (Chapter 3)	✓	✓	✓
Meeting minutes	✓		✓
Document review	✓	✓	✓
Analysis model presentation		✓	

Appendix E: Reference Materials

Managing Software Requirements A Unified Approach, Dean Leffingwell, Don Widrig, Addison-Wesley, 1999.

Software Requirements: Styles and Techniques, Soren Lauesen, Addison-Wesley, 2002.

Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development - 3rd Edition, Craig Larman, Prentice Hall, 2005.

UML Distilled 3rd Edition: A Brief Guide to The Standard Object Modeling Language, Martin Fowler, Addison Wesley, 2003.

Software Engineering A practitioner's Approach sixth edition, Roger S. Pressman, McGraw-Hill, 2005.

Applying Use Cases A Practical Guide, Geri Schneider, Jason P. Winters, Addison-Wesley, 1998.