**CS350 2015 Spring**

**Introduction to Software Engineering**

***SafeHome* Project**

**Team 9**

Junwoo Park 20121034

Eojin Rho 20130218

Yiru Jeon 20153540

**Project #2: Software Requirement Specification &  
Software Analysis Models**

|  |
| --- |
| **Contents** |

**List of Table** 4

**List of Figures** 4

**List of Swimlane Diagrams** 4

**List of Use-cases** 6

**List of Interface Diagrams** 7

**List of Use-case Diagrams** 7

**1.** **Introduction** 8

**1.1.** **Background** 8

**1.2.** ***SafeHome* Overview** 8

**1.3.** **Purpose and Structure** 9

**2.** **Overall Description** 10

**2.1.** **Functionalities and Future Plans** 10

**2.2.** **Product Perspective** 13

**2.3.** **User Class and Description** 13

**2.4.** **Operating Environment** 14

**2.5.** **Assumptions** 14

**3.** **System Features** 15

**3.1.** **SafeHome Boot-up/shutdown service** 15

**3.2.** **Configuration Services** 19

**3.3.** **Real-time security service** 34

**3.4.** **User-requested information retrieval service** 54

**3.5.** **Authentication** 61

**3.6.** **User Interface** 65

**4.** **Non-functional Requirements** 72

**4.1.** **Performance Requirements** 72

**4.2.** **Safety Requirements** 73

**4.3.** **Security Requirements** 73

**5.** **Traceability** 73

**5.1.** **Relationships between use cases and non-functional requirements** 73

**5.2.** **Relationships between interface diagrams and non-functional requirements** 74

**6.** **Project Management** 75

**6.1.** **Project Life Cycle** 75

**6.2.** **Development Method** 76

**6.3.** **Roles and Responsibility** 76

**6.4.** **Risk management** 77

**6.5.** **Staff member** 78

**6.6.** **Schedule** 78

**7.** **Project Tools** 78

**7.1.** **Development Environment** 78

**7.2.** **Development Tools** 79

**Appendix**. 80

**Appendix A. List of Glossary** 80

**Appendix B. List of Acronyms** 81

**Appendix C. Term Index** 82

**Appendix D. Who-did-what List** 83

**List of Swimlane diagrams** 85

**List of Use-cases** 86

**List of Interface diagrams** 87

**Appendix E. References** 88

**Appendix F. Revision History** 88

# **List of Table**

Table 1. Traceability matrix for use-case scenarios 73

Table 2. Traceability Matrix for Interface Diagram 74

Table 3. UP description 76

Table 4. Method for development activity 76

Table 5. Roles and Responsibility 76

Table 6. Risk management 77

# **List of Figures**

Figure 1. SafeHome overview 8

Figure 2. Thumbnail View Example 9

Figure 3. *SafeHome* Product Perspective 13

Figure 17. UP overview 75

# **List of Swimlane Diagrams**

SL 1. Self-diagnosis : check whether connected sensors and cameras are okay 16

SL 2. Initialize cameras 17

SL 3. Finish cameras 17

SL 4. Initialize sensors 18

SL 5. Finish sensors 18

SL 6. ControlPanelPassword Change 21

SL 7. WebpagePassword change 22

SL 8. Design floor plan 24

SL 9. Assign security zone 26

SL 10. Backup plan for power off 28

SL 11. Factory reset 29

SL 12. Manage logged-in devices 31

SL 13. Firmware update 33

SL 14. Arm system 37

SL 15. Disarm system 38

SL 16. Arm device 39

SL 17. Disarm device 40

SL 18. Display alarm 41

SL 19. Set travel mode 43

SL 20. View camera through floor plan window 45

SL 21. View camera through thumbnail 47

SL 22. Pan the camera 48

SL 23. Zoom in/out a camera 49

SL 24. Panic 50

SL 25. Cancel task and return 52

SL 26. Display status 53

SL 27. Pet angst sensor 54

SL 28. Finding ID 56

SL 29. Finding password 57

SL 30. Reporting system usage pattern 58

SL 31. Reporting web page access history 59

SL 32. Replay the record 61

SL 33. Deny concurrent user accesses 63

SL 34. Authentication-control panel 64

SL 35. Authentication-web page 65

# **List of Use-cases**

UC 1. ControlPanelPassword change 20

UC 2. WebpagePassword change 21

UC 3. Design floor plan 23

UC 4. Assign security zone 24

UC 5. Backup plan for power off 27

UC 6. Factory reset 28

UC 7. Manage logged-in devices 30

UC 8. Firmware update 31

UC 9. Arm/disarm system 36

UC 10. Arm/disarm devices 38

UC 11. Display alarm 40

UC 12. Set travel mode 42

UC 13. View camera through floor plan window 43

UC 14. View camera through thumbnail 45

UC 15. Pan the camera 47

UC 16. Zoom in/out a camera 48

UC 17. Panic 50

UC 18. Cancel task and return 50

UC 19. Display status 52

UC 20. Pet angst sensor 53

UC 21. Finding ID 55

UC 22. Finding password 56

UC 23. Reporting system usage pattern 57

UC 24. Reporting web page access history 58

UC 25. Replay the record 60

UC 26 . Deny concurrent user accesses 62

UC 27. Authentication-ControlPanel 63

UC 28. Authentication-Webpage 64

# **List of Interface Diagrams**

ID 1. Web interface - login page 66

ID 2. Web interface - Accessing Security Function 67

ID 3. Web interface - Main page with list of functions 67

ID 4. Web interface - Security Control Panel 68

ID 5. Web interface - viewing camera 69

ID 6. Web interface - Single-camera view 69

ID 7. Web interface - Thumbnail view 70

ID 8. Web interface - Configuration menu 71

ID 9. Control panel interface 72

# **List of Use-case Diagrams**

UCD 1. Configuration 19

UCD 2. Sensor-related Security 35

UCD 3. Camera-related Security 35

# **Introduction**

* 1. **Background**

In these days, many home devices are starting to be controlled by unified method. Many homes are equipped with systems, which control heating system, air conditioner, lights, automobile tracking system, security camera, security sensor and so on. People can control all gadgets consistently using these centralized controlling systems. Moreover, many service providers started to implement Web interface to access controlling system because (1) people want to control their own home while they are away and (2) many mobile devices accessing Internet are available, such as smartphones and tablet-PCs.

* 1. ***SafeHome* Overview**

Therefore, we propose *SafeHome*. *SafeHome* is a centralized system for controlling home gadgets. *SafeHome* focuses on security. *SafeHome* controls security devices as well as home appliances.



Figure . SafeHome overview

*SafeHome* monitors security sensors which can detect intruders, and dangerous situations such as fire, toxin gases. Also, *SafeHome* controls security cameras. A homeowner can see overall cameras in thumbnail view (see Figure 2.). The homeowner also, can zoom a camera, and pan a camera to see what he or she wants to see. While homeowner travels away, *SafeHome* controls lights to imitate that there are people inside the building so that trespassers are reluctant to invade the building.

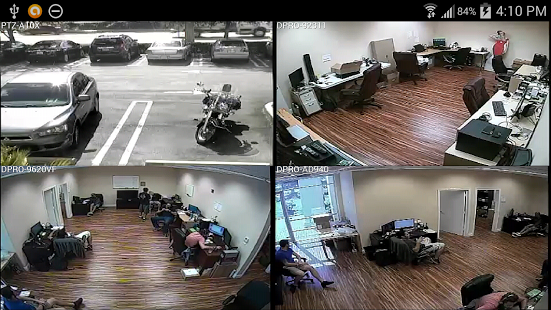


Figure . Thumbnail View Example

*SafeHome* provides flexibility to homeowners. Homeowner can order additional devices through Internet and attach the new devices to one’s *SafeHome* system. *SafeHome* is adaptable to any home floor structure. A homeowner can design a floor plan for the home with layout tools provided by *SafeHome*. Then homeowner may place sensors, cameras, and other gadgets to the floor plan in *SafeHome*.

* 1. **Purpose and Structure**

The SRS (Software Requirement Specification) describes the requirements that must be met by the *Safehome* product. The organization of the document is following:

* *Chapter 1. Introduction* provides an overview of *SafeHome* project, project’s environment, and the SRS.
* *Chapter 2. Overall Description* describes *SafeHome* project and its environment in detail.
* *Chapter 3. System Features* explains technical details of the project features in terms of security, surveillance, and configuration functionalities.
* *Chapter 4. Non-functional Requirements* explains *SafeHome* system requirements which is not included in functional requirements.

# **Overall Description**

* 1. **Functionalities and Future Plans**
     1. **Functionalities**

1. Boot-up/shutdown services
   1. *SafeHome* system should do self-diagnosis to find problems in the system itself or in *SafeHome* devices (cameras and sensors).
   2. The system can initialize/finalize sensors when the system boots/shutdowns.
   3. The system can initialize/finalize cameras when the system boots/shutdowns.
2. Configuration services
   1. A homeowner can change passwords
      1. 4-digit password used in control panel
      2. 2 passwords used in web page; each has at least 8 characters.
   2. A homeowner can configure *SafeHome* floor plan.
      1. The homeowner can redraw floor plan.
         * When the building is remodeled.
         * When the floor structure is changed due to additional furniture.
      2. Floor plan contains distance scale.
      3. Floor plan contains information about walls and doors.
      4. The homeowner can register new devices.
      5. The homeowner can rearrange devices.
   3. A homeowner can group specific sensors into a *security zone*.
   4. A homeowner can configure backup plan for power off.
      1. The homeowner can inform the system devices that could be turned off.
      2. The homeowner can inform the system devices that must be turned on.
3. Real-time security services
   1. A homeowner can arm/disarm *SafeHome* system.
   2. A homeowner can arm/disarm parts of *SafeHome* devices.
      1. e.g. arming/disarming only sensors or a specific sensor.
      2. e.g. arming/disarming sensors that belong to specific *security zone*.
   3. A homeowner can temporality disarm parts of the system to allow a housekeeper to enter when the homeowner is away.
   4. *SafeHome* control panel contains a speaker to generate alarming sounds.
   5. *SafeHome* can turn on lights and other gadgets to deceive outsiders when the home owner is away.
   6. *SafeHome* sensors respond to *SafeHome* system using binary value; true or false.
      1. e.g. functional or not
      2. e.g. something is detected or not.
      3. e.g. enabled or not
   7. A homeowner can record cameras.
      1. Video format is MPEG.
      2. Video resolution is bigger than 640 \* 480.
      3. Video FPS (frame per second) should be bigger than 1.
   8. A homeowner can watch cameras.
      1. The homeowner can watch all cameras in thumbnail view.
      2. The homeowner can select a specific camera and control it: panning camera or zooming camera.
   9. A homeowner can control cameras.
      1. The homeowner can zoom a camera.
      2. The homeowner can pan a camera.
   10. *SafeHome* records videos for at least a month.
       1. The system storage should have proper capacity to store videos of a month.
4. User-requested information retrieval services
   1. A homeowner can find his or her lost ID or passwords.
   2. A homeowner can inspect his or her system usage patterns.
   3. A homeowner can inspect *SafeHome* web page access history to check Internet security.
   4. A homeowner can playback a past video.
5. Authentication
   1. The *SafeHome* system manages session to handle concurrent accesses. See [2.5. Assumption](#_Assumptions).
      1. Timeout: 20 seconds in control panel, 1 minute in web page
   2. A homeowner can control SafeHome system using control panel after authentication in control panel.
      1. 4-digits password is required.
      2. Access permission is granted to only one session. See [2.5. Assumption](#_Assumptions).
   3. A homeowner can control SafeHome system using web browser after authentication in web page.
      1. Two passwords are required; each password has at least 8 characters.
      2. Access permission is granted to only one session. See [2.5. Assumption](#_Assumptions).
6. User interface
   1. A homeowner can access *SafeHome* system using control panel in house. [See 3.6.3. Hardware User Interface](#_Hardware_User_Interface)
   2. A homeowner can access *SafeHome* system through Internet with web browser.
      1. Remote PC or smartphones that have network device and web browser applications can access *SafeHome* system.
      2. Web page should be designed mobile-friendly.
      3. **Future Plans**

* *SafeHome* system can control not only security devices but also general home appliances such as, heating system, air conditioner, vents, telephones, and so on.

## **Product Perspective**

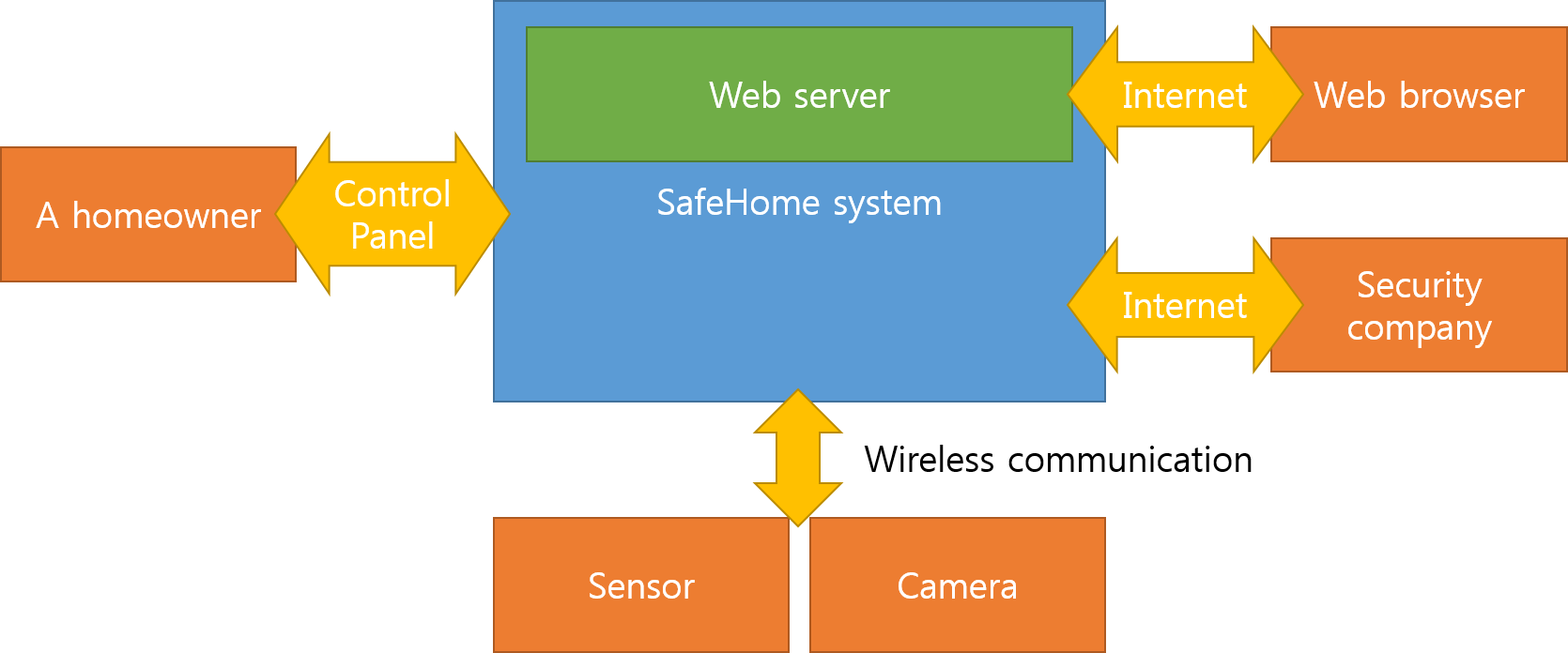


Figure . *SafeHome* Product Perspective

*SafeHome* has 4 different kinds of actors. First of all, (1) a homeowner can manage *SafeHome* system through control panel. Control panel is hardware based interface. Such control panel is a necessary interface when Internet connection is unavailable. (2) The homeowner can access *SafeHome* using web browsers through Internet. (3) *SafeHome* devices interact with *SafeHome*. The devices report intrusion and dangerous situation. *SafeHome* cameras transfer camera feed. (4) When *SafeHome* detects the homeowner is in danger, it informs a security company, CPI corporation, so that the corporation can make actions to protect clients.

## **User Class and Description**

* A homeowner: A homeowner can manage *SafeHome* system through control panel. Control panel interface should be available in case Internet connection is not available.
* A web browser: A homeowner can manage *SafeHome* system using web browser. Therefore, the homeowner can control home using web browser application in a PC or a smartphone.
* A device (sensor / camera): A *SafeHome* device that has a protocol to interact with *SafeHome* system; *SafeHome* system can request *SafeHome* devices something. A *SafeHome* device responds to *SafeHome* system.
* A security company: CPI corporation; When *SafeHome* detects an intruder or dangerous situation, it raises alarm and notifies CPI corporation that a homeowner is in danger. Then, CPI corporation sends private securities and reports law enforcers to protect clients.

## **Operating Environment**

* Webpage interface of *SafeHome* system should have structure that is proper to mobile devices. A homeowner may access to *SafeHome* system using a smartphone.

## **Assumptions**

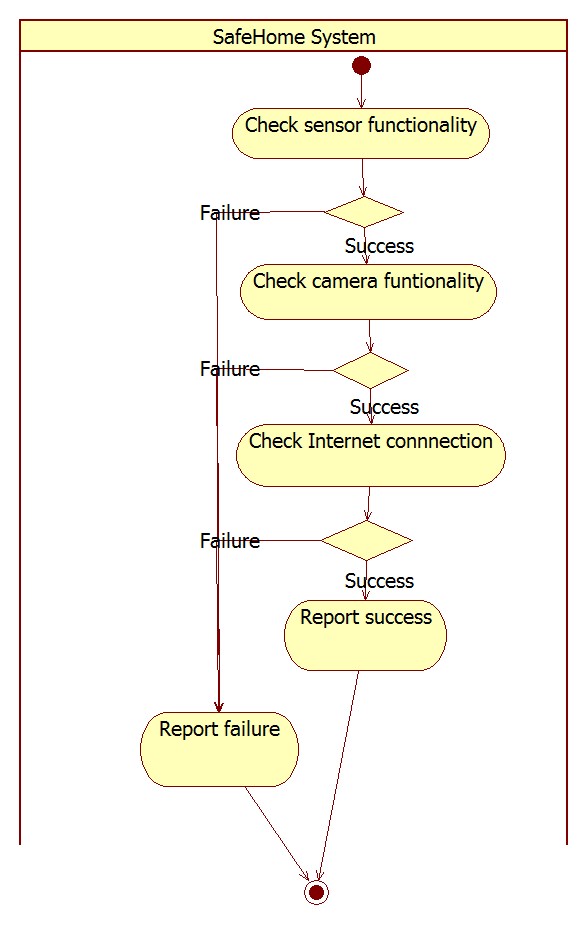
* *SafeHome* hardware devices and prepared and ready to be assembled.
* *SafeHome* devices use secure wireless communication.
  + No attacker can intercept camera video.
  + No attacker can forge signal of a sensor and prevent alarm to activate.
* TCP/IP is used on top of wireless communication; contents of communication between *SafeHome* devices and *SafeHome* system are not lost nor re-ordered.
* A homeowner has overall authority on *SafeHome* system. He or she can inspect the system, watch system’s report, and customize the system.
* Physical security is accomplished; Attacker cannot break physical communication materials and disable Internet connection of *SafeHome* system.
* *SafeHome* main device contains enough computation power to execute web server application.
* *SafeHome* system has a file system to store video records. Video feeds are not broken nor corrupted. *SafeHome* can assume that physical failure in file system does not happen.
* No concurrent user has access to the device.
  + (web-control panel exclusive) Access through web and access through control panel are exclusive.
  + (web access exclusive) Web control access can take place in only one client.
  + (control panel exclusive) There is only one control panel in the house.
* (Internet Connectivity) Internet connection is always available for the SafeHome system.
* All devices including cameras, sensors and the Safehome system communicate using IEEE 802.11x protocol.

# **System Features**

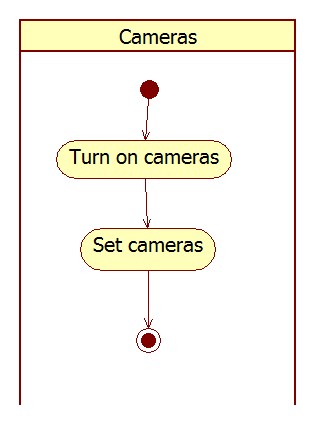
## **SafeHome Boot-up/shutdown service**

* + 1. **Future Descriptions**

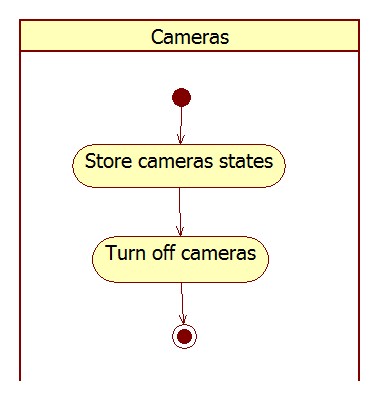
*SafeHome* provides home security system. To ensure *SafeHome* system is fully functional, *SafeHome* system must check the functionality itself. If *SafeHome* system is not functioning well, it should report the failure of the system. Moreover, sensors and cameras must initialize for their functionality. In addition, sensors and cameras must be finish in right sequence.



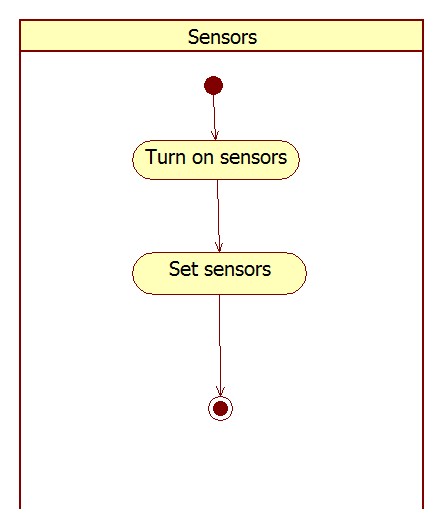
SL . Self-diagnosis : check whether connected sensors and cameras are okay



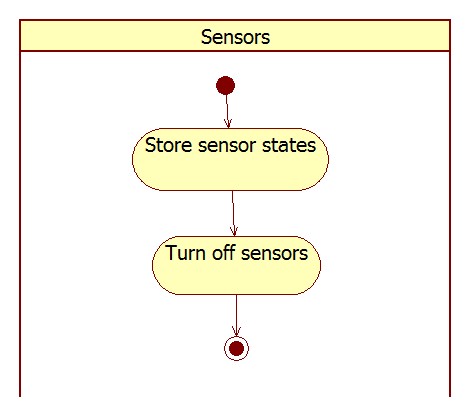
SL . Initialize cameras



SL . Finish cameras



SL . Initialize sensors



SL . Finish sensors

## **Configuration Services**

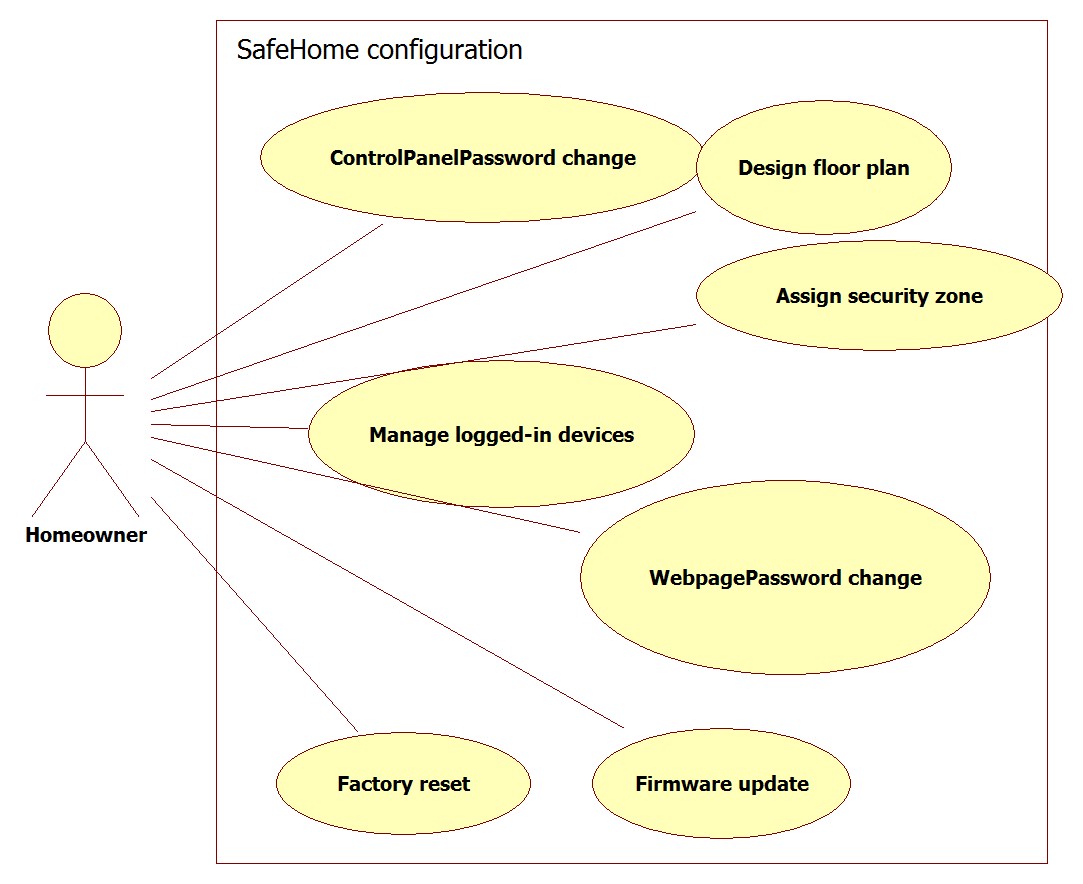
* + 1. **Description**

*SafeHome* is a security system and it should support customization features to provide a homeowner best security. Security sensors and cameras can be relocated for this purpose. In addition, floor structure could be changed; new wall is assembled or new furniture is installed.

*SafeHome* provides Internet access interface to a homeowner. To prevent outsider attacker from controlling a home, *SafeHome* requires personal identification procedure based on ID and password system. However, a homeowner might lost his or her mobile devices which are already authenticated. Hence, *SafeHome* should be able to show which devices are logged in and to force a device to be logged off.

Because *SafeHome* system contains a firmware software that could be updated by system developers, homeowner should be able to update his or her *SafeHome* system through Internet.

* + 1. **Use case diagram**

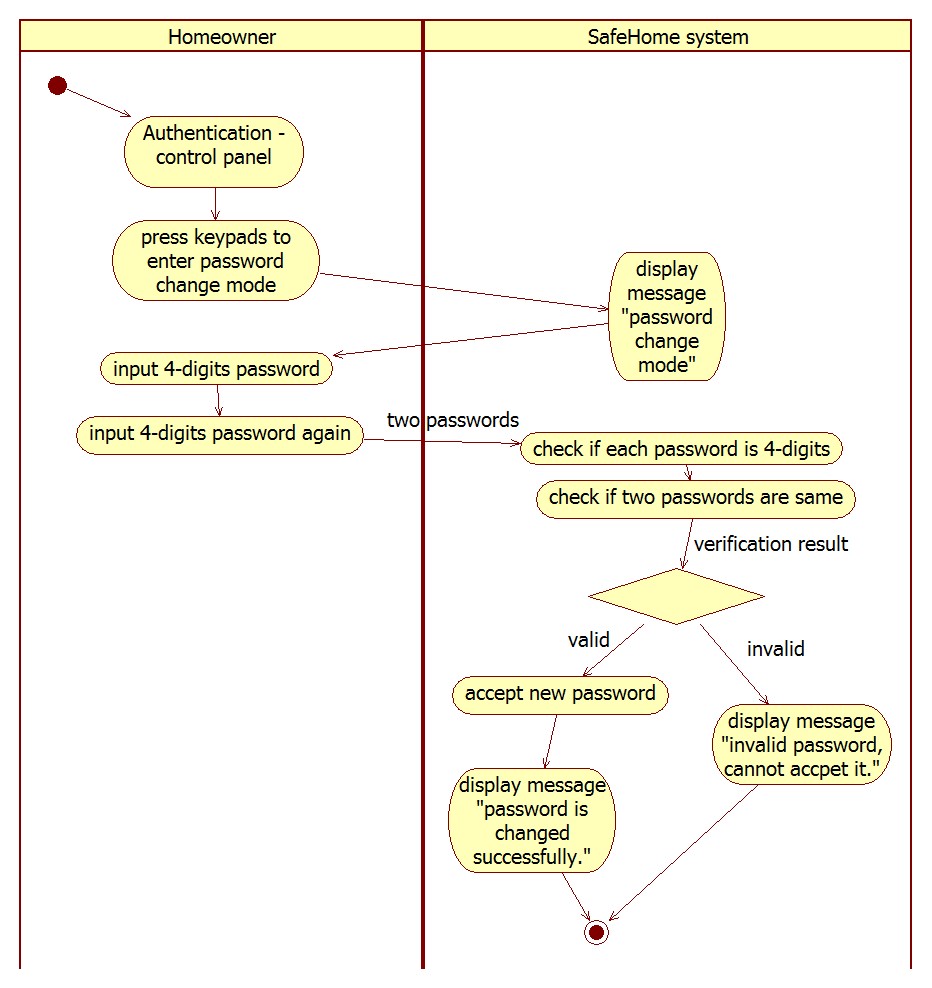


UCD . Configuration

* + 1. **Use cases**
       1. **Password**

UC . ControlPanelPassword change

|  |  |
| --- | --- |
| Name | ControlPanelPassword change |
| Primary actor | Homeowner |
| Goal in context | To allow the homeowner to change 4-digit password of control panel. |
| Preconditions | 1. Homeowner authentication is completed. |
| Trigger | The homeowner wants to change password for control panel. |
| Scenario | 1. The homeowner gets to control panel. 2. The homeowner does authentication using 4-digit password. 3. The homeowner presses sequence of numbers in keypad to change password. 4. The system asks new password. 5. The homeowner enters new 4-digit password. 6. The system asks the homeowner to enter 4-digit password again. 7. The homeowner enters the same password. (sanity checking) 8. If both input are same, the system displays that password is changed successfully. |
| Exception | 1. Sanity checking fails – The system displays that password is not changed and goes to initial state. |
| Priority | High |
| Channel to actor | Control panel |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | 1. Initial password: 0000 2. What should be “sequence of numbers” to enter password change mode? |



SL . ControlPanelPassword Change

UC . WebpagePassword change

|  |  |
| --- | --- |
| Name | WebpagePassword change |
| Primary actor | Homeowner |
| Goal in context | To allow the homeowner to change two passwords of web page. |
| Preconditions | 1. Homeowner authentication is completed. |
| Trigger | The homeowner wants to change password for web page login. |
| Scenario | 1. The homeowner enter configuration menu in web page. 2. The homeowner selects “change password”. 3. The system asks new password. 4. The homeowner enters two new passwords. 5. The system asks the homeowner to enter the two passwords again. 6. The homeowner enters the same passwords. (sanity checking) 7. If both input are same, the system displays that passwords are changed successfully. |
| Exception | 1. Sanity checking fails – The system displays that password is not changed and goes to main menu web page. |
| Priority | High |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | 1. How the homeowner create initial web page account? |

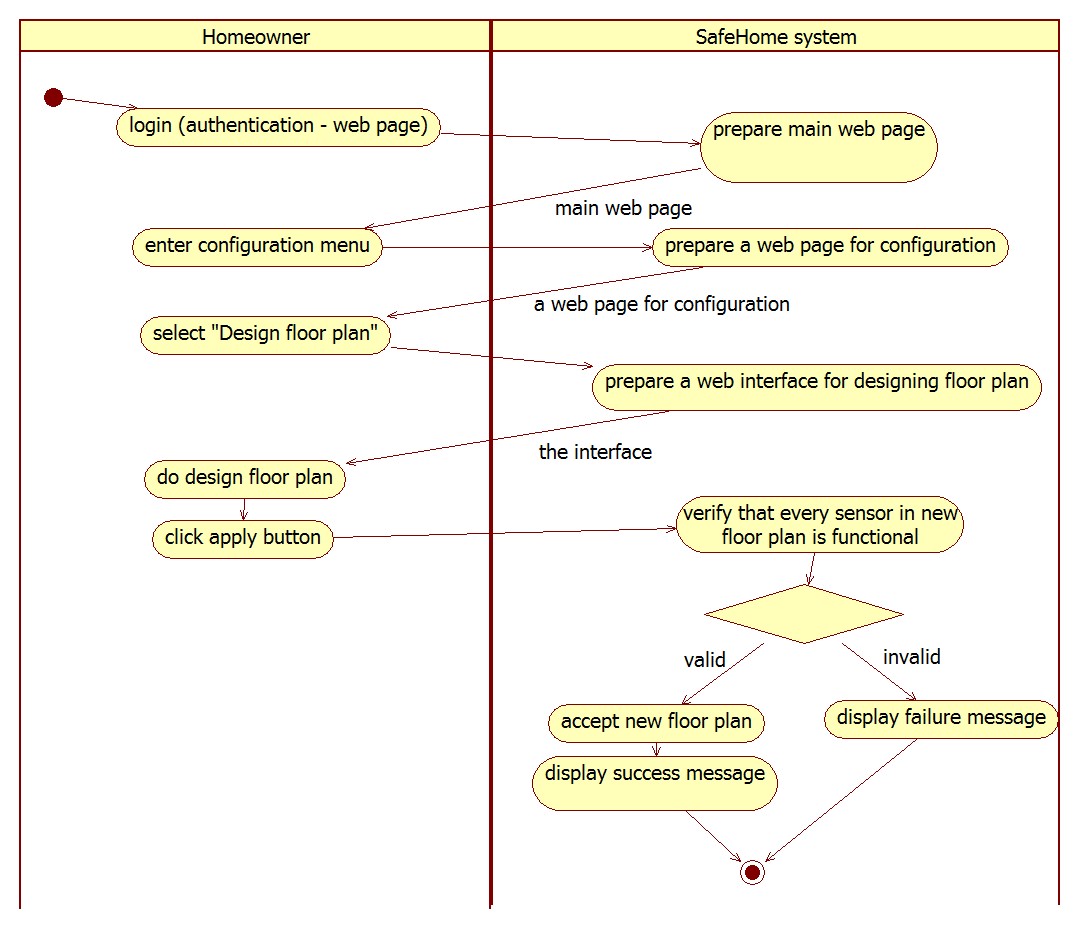


SL . WebpagePassword change

* + - 1. **Floor Plan**

UC . Design floor plan

|  |  |
| --- | --- |
| Name | Design floor plan |
| Primary actor | Homeowner |
| Goal in context | To design *SafeHome* floor plan |
| Preconditions | 1. Homeowner authentication is completed. 2. *SafeHome* must be disarmed. |
| Trigger | The homeowner changed floor plan and decides to apply changes to *SafeHome*. |
| Scenario | 1. The homeowner changes floor plan: new wall, furniture, or etc. 2. The homeowner decides to apply changes to *SafeHome*. 3. The homeowner goes to *SafeHome* control panel. 4. The homeowner selects configuration menu. 5. The homeowner selects “Design floor plan”. 6. The system shows current floor plan if it has, empty plan otherwise. 7. The homeowner can change distance scale. 8. The homeowner can change floor plan with the system aided layout tool. 9. After the homeowner finishes designing, the system verifies that *SafeHome* devices are functional. 10. If verification is done successfully, the system displays main menu. |
| Exception | 1. Failed to load current floor plan. 2. Distance scale is negative. 3. Some devices are not functional in verification procedure. |
| Priority | High |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | - |

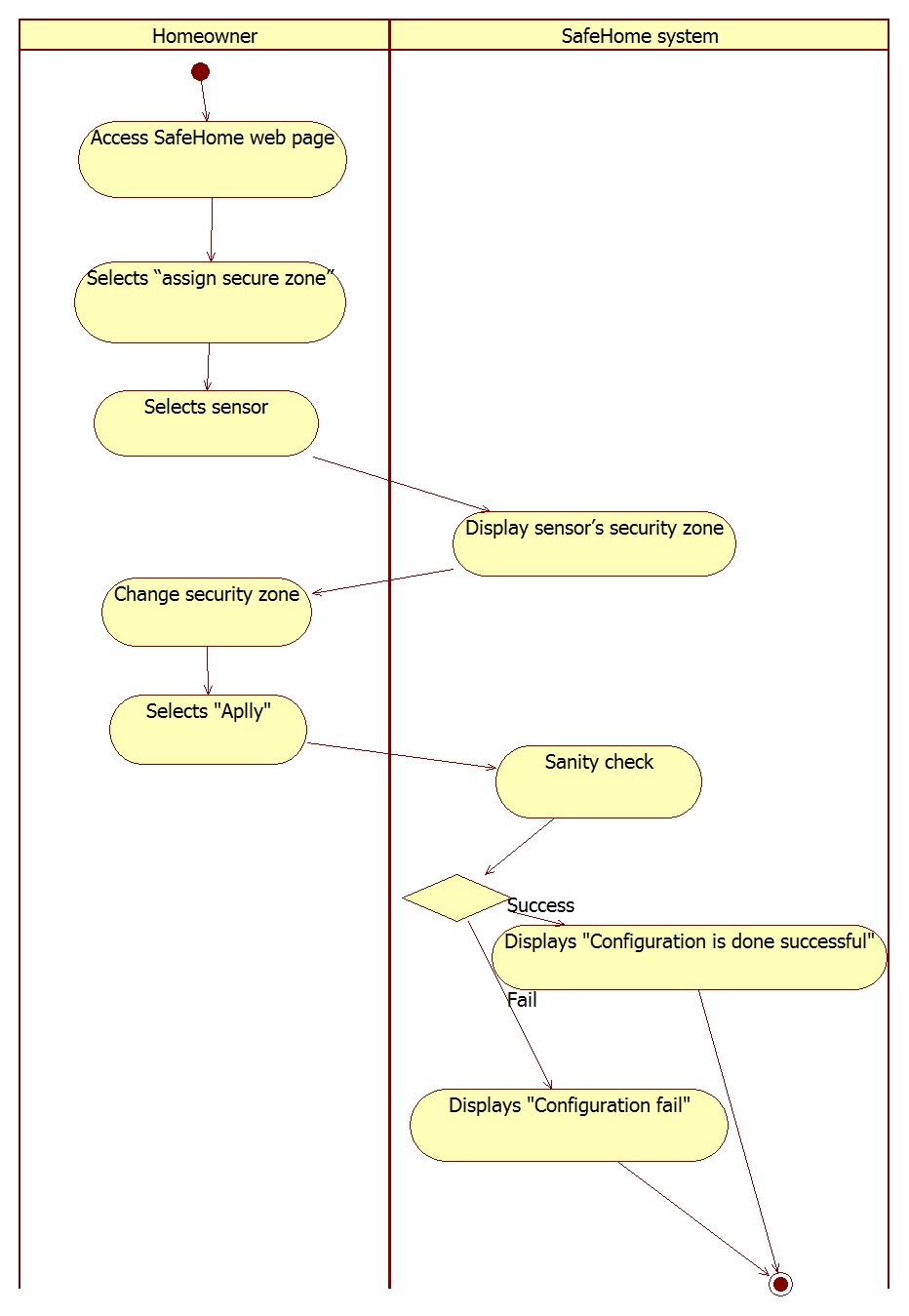
****

SL . Design floor plan

* + - 1. **Security Zone**

UC . Assign security zone

|  |  |
| --- | --- |
| Name | Assign security zone |
| Primary actor | Homeowner |
| Goal in context | To assign *SafeHome* devices into a security zone. |
| Preconditions | 1. Homeowner authentication is completed. 2. *SafeHome* must be disarmed. |
| Trigger | The homeowner decides to configure security zones. |
| Scenario | 1. The homeowner access *SafeHome* web page. 2. The homeowner selects “assign secure zone”. 3. The homeowner selects a sensor. 4. The system shows the sensor’s current security zone. 5. The homeowner can change the security zone. 6. The homeowner selects “apply” 7. The system does sanity check. 8. The system displays message “configuration is done successfully.”. |
| Exception | Sensors became nonfunctional in sanity checking process. |
| Priority | Low priority |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | - |

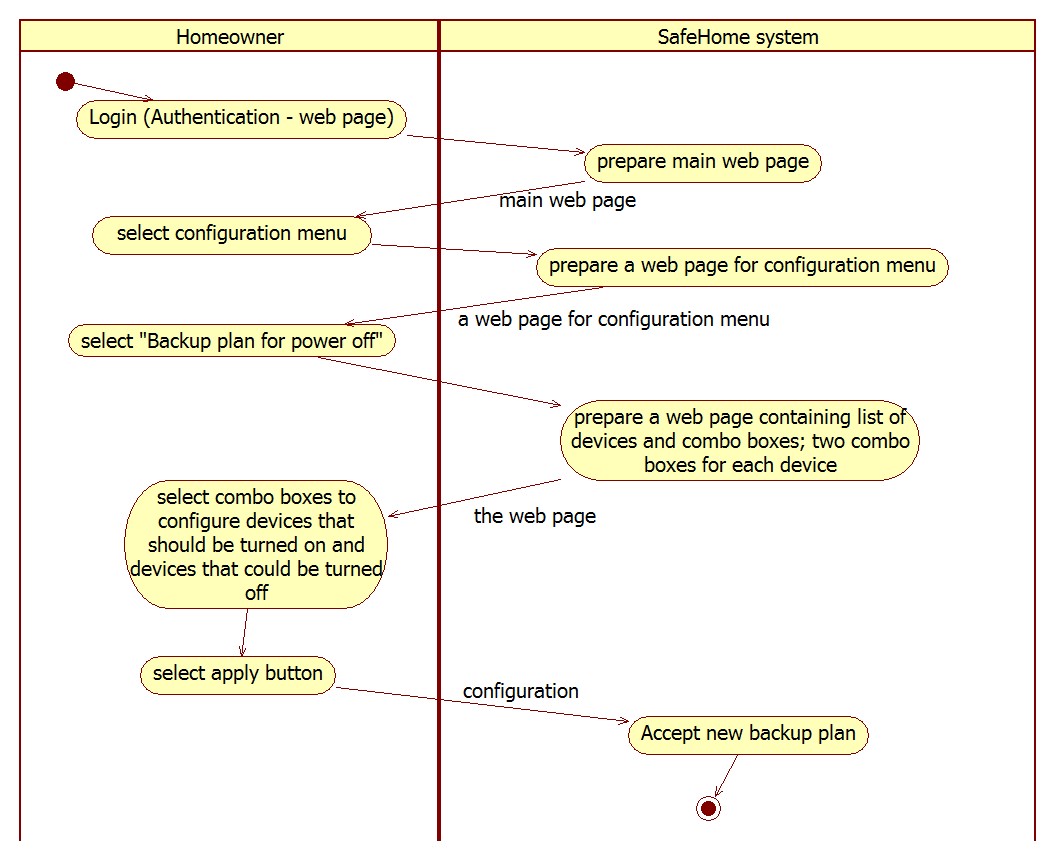


SL . Assign security zone

* + - 1. **Backup plan for power off**

UC . Backup plan for power off

|  |  |
| --- | --- |
| Name | Backup plan for power off |
| Primary actor | Homeowner |
| Goal in context | To allow the homeowner to configure the backup plan |
| Preconditions | 1. Homeowner authentication must be done. 2. Internet connection is available. |
| Trigger | The homeowner decided to configure the backup plan. |
| Scenario | 1. The homeowner access *SafeHome* webpage. 2. The homeowner selects configuration menu. 3. The homeowner selects “Backup plan for power off”. 4. The system shows list of devices. 5. The homeowner selects which devices should be turned on and which devices could be turned off using combo box interface. 6. The homeowner selects apply button. 7. The system stores new backup plan. |
| Exception | - |
| Priority | Medium |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | - |

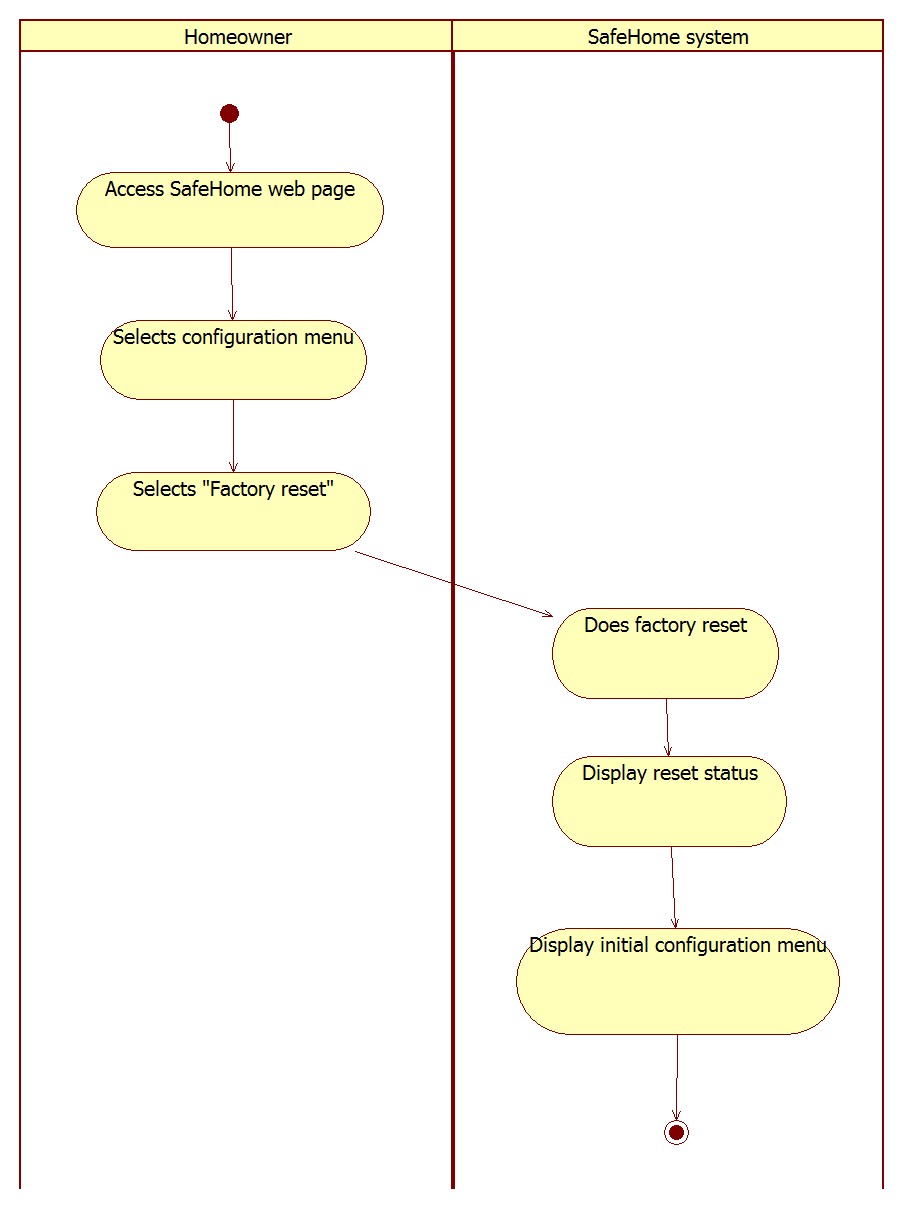
****

SL . Backup plan for power off

* + - 1. **Others**

UC . Factory reset

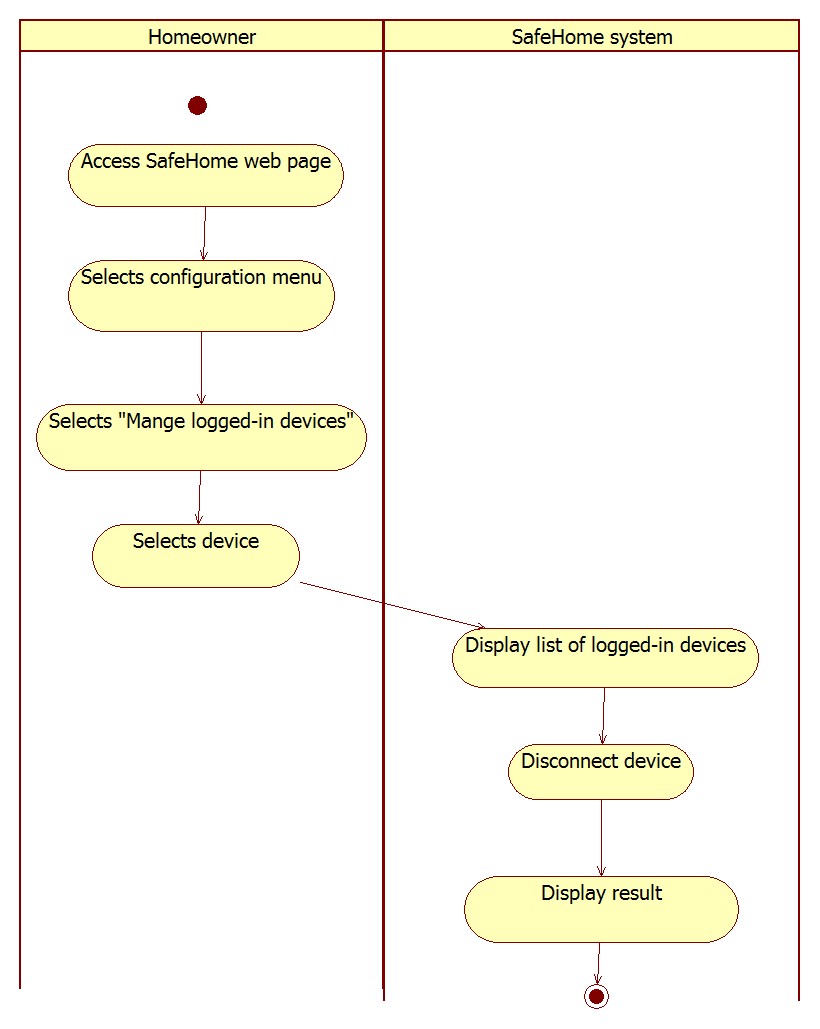
|  |  |
| --- | --- |
| Name | Factory reset |
| Primary actor | Homeowner |
| Goal in context | To reset entire *SafeHome* configuration |
| Preconditions | 1. Homeowner authentication is completed. 2. *SafeHome* must be disarmed. |
| Trigger | The homeowner decides to reset *SafeHome* configuration. |
| Scenario | 1. The homeowner access to *SafeHome* web page. 2. The homeowner selects configuration menu. 3. The homeowner selects “Factory reset” 4. The system does factory reset. 5. The system displays reset status. 6. The system displays initial configuration menu. |
| Exception | - |
| Priority | Low priority |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | Unexpected power down during factory reset |



SL . Factory reset

UC . Manage logged-in devices

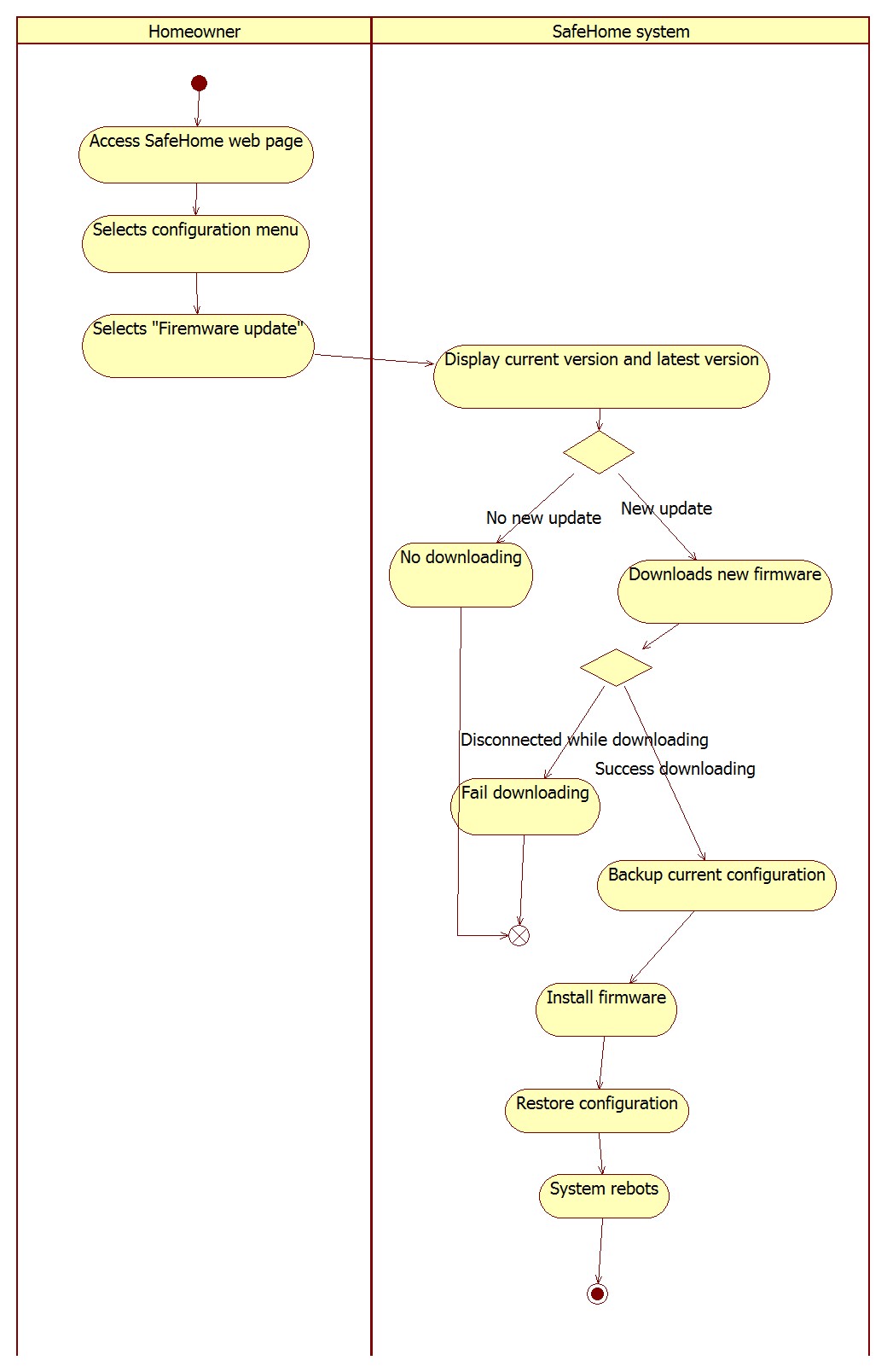
|  |  |
| --- | --- |
| Name | Manage logged-in devices |
| Primary actor | Homeowner |
| Goal in context | To allow the homeowner to force a device to be logged off |
| Preconditions | 1. Homeowner authentication must be done. |
| Trigger | The homeowner decides to force a device to be logged off. |
| Scenario | 1. The homeowner lost a mobile device that is permitted to access *SafeHome* system. 2. The homeowner decides to force the device to be logged off. 3. The homeowner access *SafeHome* web page. 4. The homeowner selects configuration menu. 5. The homeowner selects “Manage logged-in devices” 6. The system shows list of devices that are logged-in. 7. The homeowner selects one of devices. 8. The system disconnect the device. 9. The system displays result of the request. |
| Exception | - |
| Priority | Medium |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | - |



SL . Manage logged-in devices

UC . Firmware update

|  |  |
| --- | --- |
| Name | Firmware update |
| Primary actor | Homeowner |
| Goal in context | To allow the homeowner to update *SafeHome* system |
| Preconditions | 1. Homeowner authentication must be done. 2. Internet connection is available. |
| Trigger | The homeowner decided to update *SafeHome* system. |
| Scenario | 1. The homeowner decide to update the system. 2. The homeowner access *SafeHome* webpage. 3. The homeowner selects configuration menu. 4. The homeowner selects “Firmware update” 5. The system displays current version and latest version. 6. The system downloads new firmware software. 7. The system backs up current configuration. 8. The system installs new firmware. 9. The system restores configuration. 10. The system reboots. |
| Exception | 1. Internet access becomes unavailable while downloading new firmware. |
| Priority | Low |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | Unexpected power down during firmware update |



SL . Firmware update

## **Real-time security service**

* + 1. **Description**

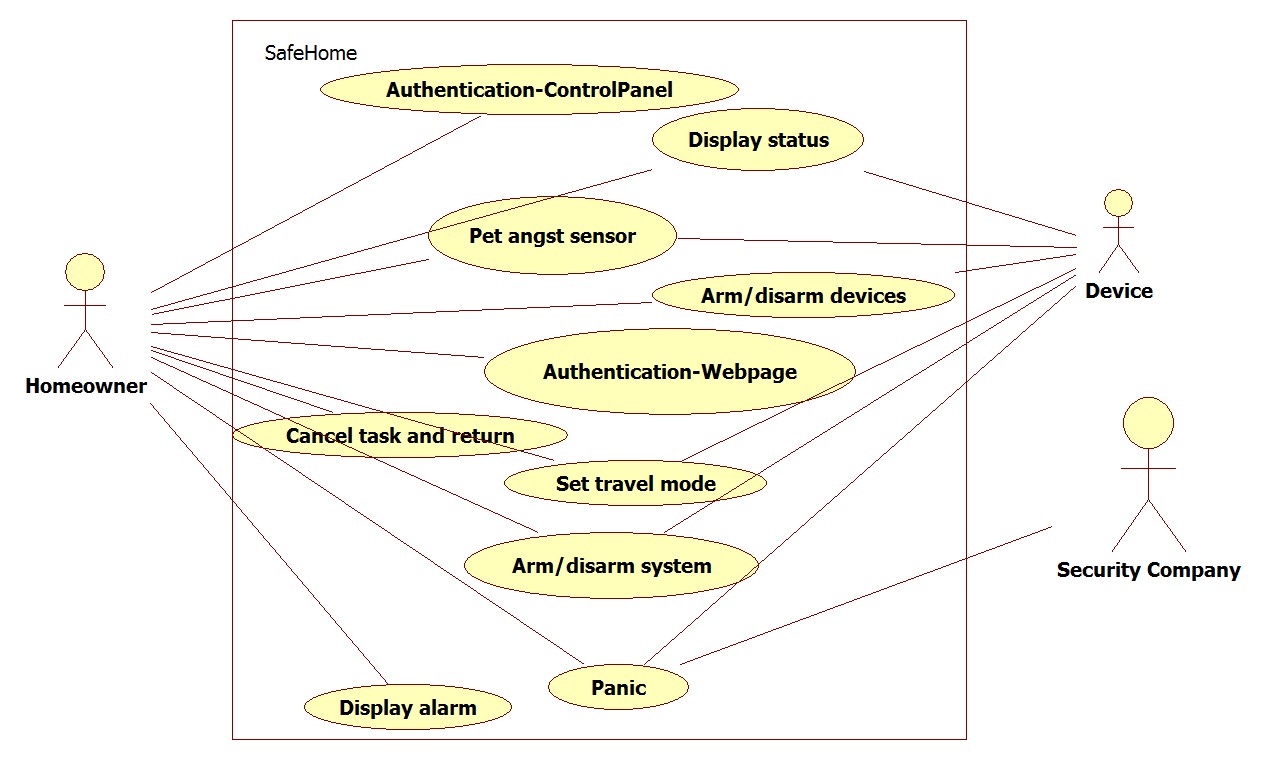
The real-time security service is the main component of *Safehome* system. It includes controlling and utilizing various types of sensors including:

1. door and window sensors for determining if they are open/closed
2. motion detectors to see if there is any intruder
3. fire sensor for fire alarm
4. gas sensor for carbon monoxide level detection
5. smoke level sensors

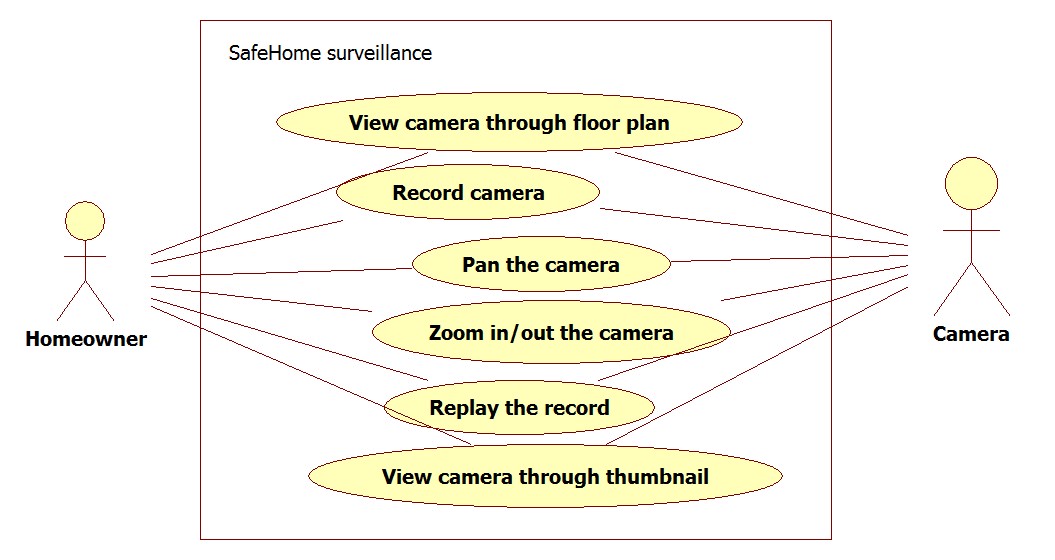
All these sensors can trigger emergency alarm. The home owner can also arm/disarm the house and each sensors using the control panel (hardware) or web interface.

Another aspect of security service that *Safehome* system provides is the surveillance of the house by accessing the camera through Internet e.g. web browser. The homeowner can see the view of a camera by selecting the camera in floor plan or thumbnails. Also, The homeowner can zoom in/out and pan the camera’s view. Moreover, The homeowner can record the camera’s view and replay it later.

* + 1. **Use case diagram**

****

UCD . Sensor-related Security

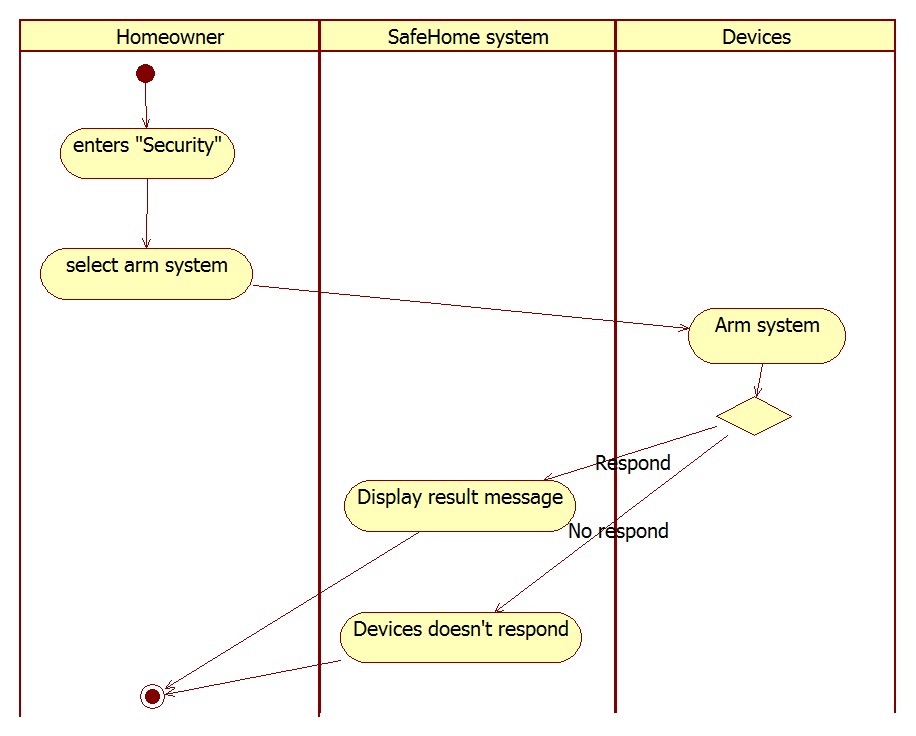


UCD . Camera-related Security

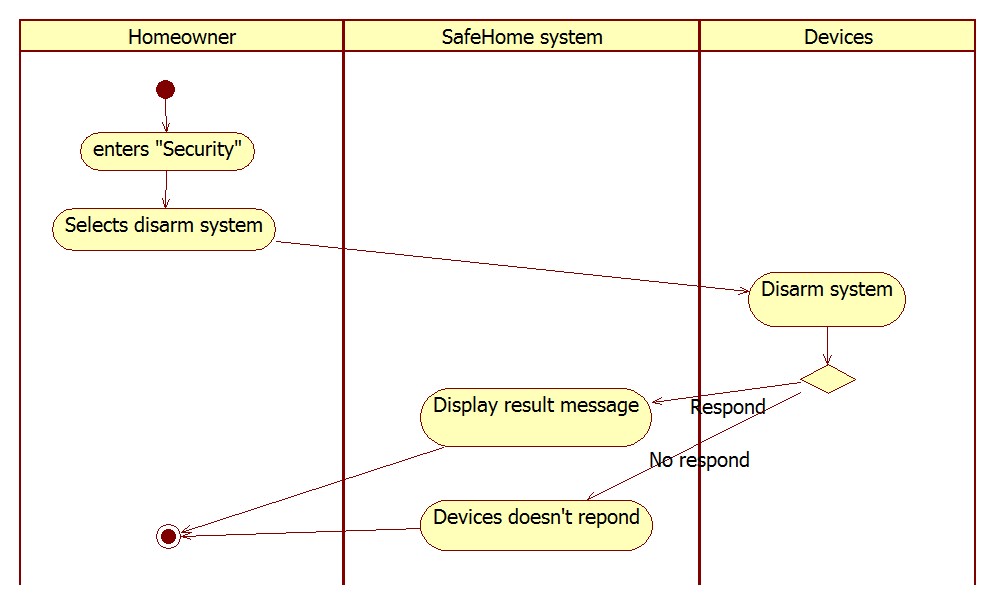
* + 1. **Use cases**
       1. **Arming the system**

UC . Arm/disarm system

|  |  |
| --- | --- |
| Name | Arm/disarm system |
| Primary actor | Homeowner |
| Goal in context | To allow the homeowner to arm/disarm *SafeHome* system: all devices. |
| Preconditions | 1. *SafeHome* system is fully functional. 2. Homeowner authentication is done. |
| Trigger | The homeowner wants to arm/disarm entire *SafeHome* devices. |
| Scenario | 1. The homeowner enters “Security” menu in web page. 2. The homeowner selects “arm/disarm the system”. 3. The system displays result message. |
| Exception | 1. Some devices does not repond. |
| Priority | High |
| Channel to actor | Internet |
| Secondary actors | Device |
| Channels to secondary actors | Device: wireless communication |
| Open issues | - |



SL . Arm system

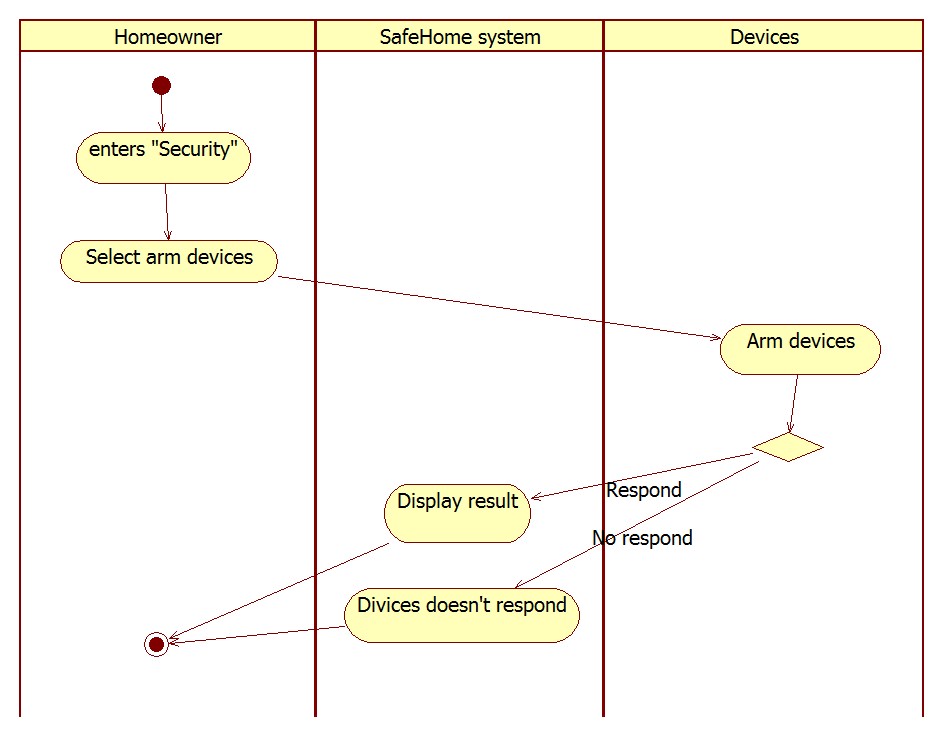
****

SL . Disarm system

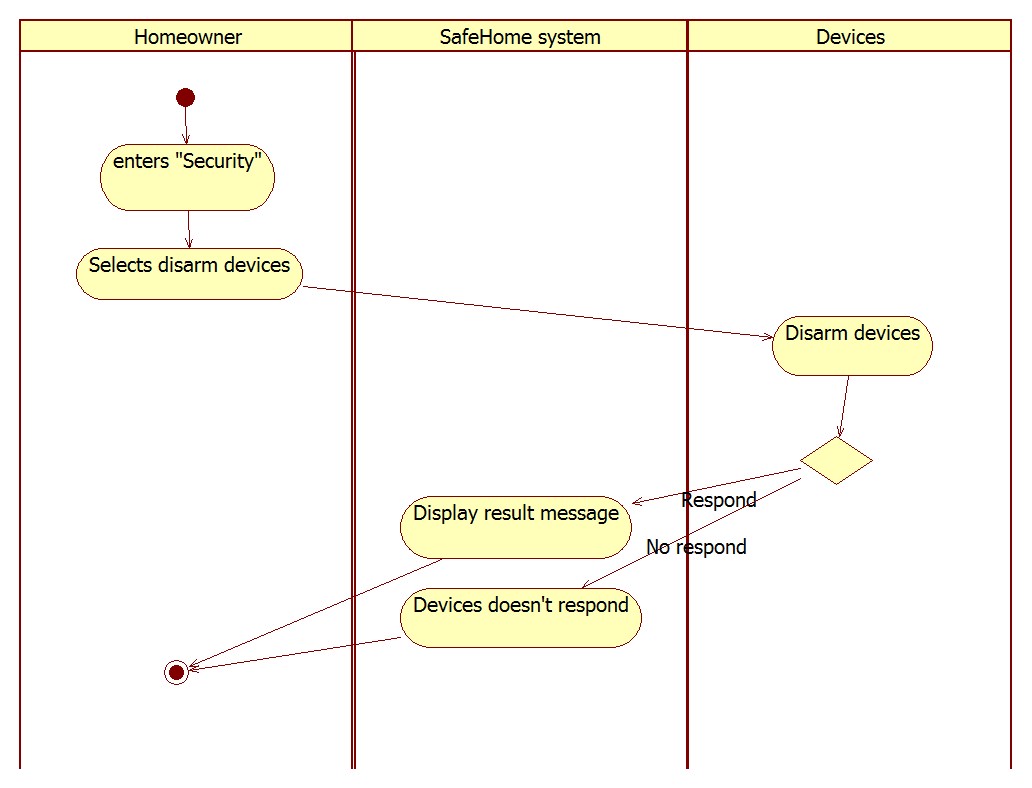
* + - 1. **Arming/Disarming devices**

UC . Arm/disarm devices

|  |  |
| --- | --- |
| Name | Arm/disarm devices |
| Primary actor | Homeowner |
| Goal in context | To allow the homeowner to arm/disarm *SafeHome* devices |
| Preconditions | 1. *SafeHome* system is fully functional. 2. Homeowner authentication is done. |
| Trigger | The homeowner wants to arm/disarm some devices in a security zone or a specific device. |
| Scenario | 1. The homeowner enters “Security” menu in web page. 2. The homeowner selects “arm/disarm devices”. 3. The system displays result message. |
| Exception | 1. Some devices does not respond. |
| Priority | Medium |
| Channel to actor | Internet |
| Secondary actors | Device |
| Channels to secondary actors | Device: wireless communication |
| Open issues | *SafeHome* should allow the homeowner to arm/disarm devices temporarily. When housekeeper visits the home, the homeowner wants to disarm devices temporarily. |

****

SL . Arm device

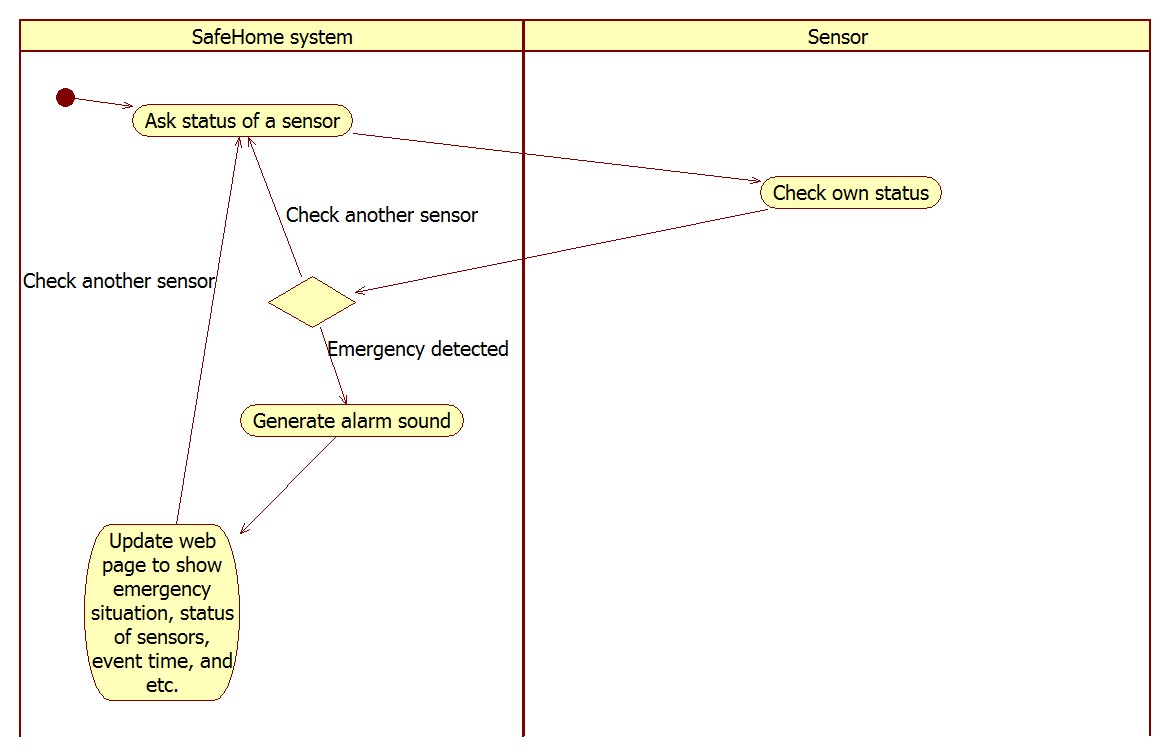
****

SL . Disarm device

* + - 1. **Alarm**

UC . Display alarm

|  |  |
| --- | --- |
| Name | Display alarm |
| Primary actor | Homeowner |
| Goal in context | The homeowner should be notify when an intruder breaches. |
| Preconditions | 1. *SafeHome* system is fully functional. 2. The homeowner arms the security. |
| Trigger | An intruder invaded the house. |
| Scenario | 1. An invader activates a sensor. 2. The sensor reports incident to *SafeHome* system. 3. Control panel displays alarm situation 4. Control panel generates alarm sound. 5. Web page displays alarm situation. 6. System sends emergency call to security company through Internet. 7. Security company sends private security to handle the problem. |
| Exception | - |
| Priority | High |
| Channel to actor | 1. Control panel 2. Web page |
| Secondary actors | 1. Sensors 2. Security company |
| Channels to secondary actors | * Sensors: wireless connection * Security company: Internet |
| Open issues | - |

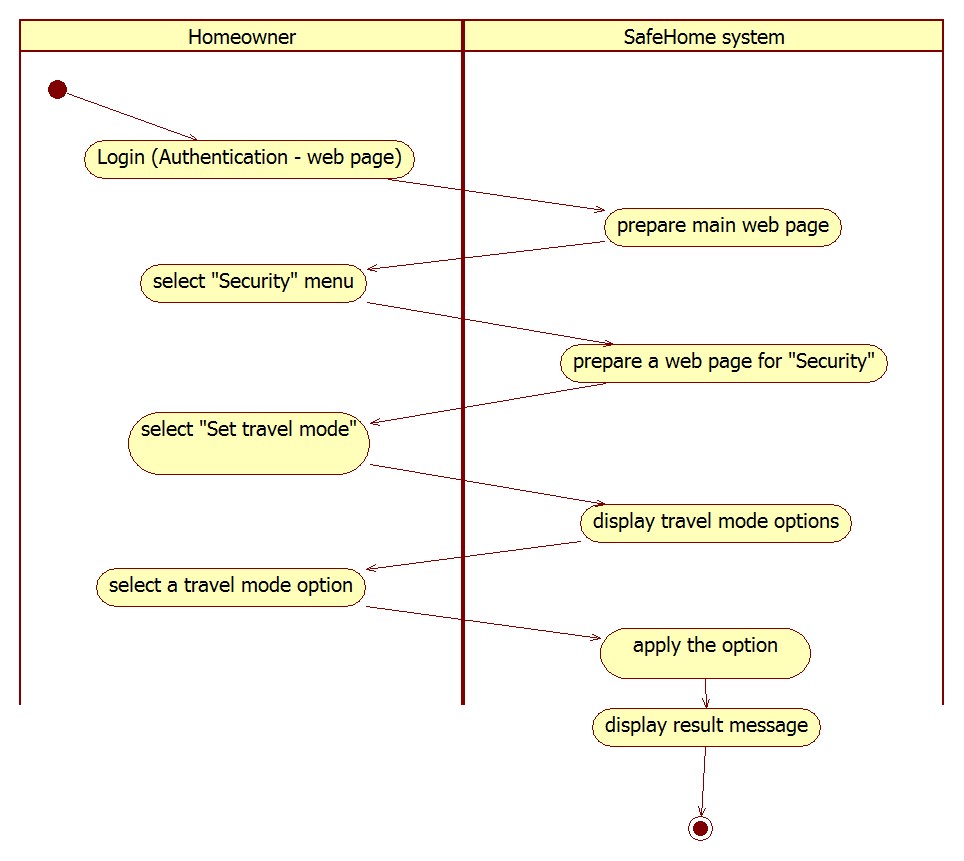
****

SL . Display alarm

* + - 1. **Set travel mode**

UC . Set travel mode

|  |  |
| --- | --- |
| Name | Set travel mode |
| Primary actor | Homeowner |
| Goal in context | To allow the homeowner to set travel mode |
| Preconditions | 1. *SafeHome* system is fully functional. 2. Homeowner authentication is done. |
| Trigger | The homeowner changes travel mode. |
| Scenario | 1. The homeowner enters “Security” menu in webpage. 2. The homeowner selects “Set travel mode”. 3. The system displays 4 options: *home*, *away*, *overnight travel*, and *extended travel*. 4. The homeowner selects one of them. 5. The system configures devices accordingly. 6. The system displays result message. |
| Exception | - |
| Priority | Medium |
| Channel to actor | Internet |
| Secondary actors | Device |
| Channels to secondary actors | Device: wireless communication |
| Open issues | - |

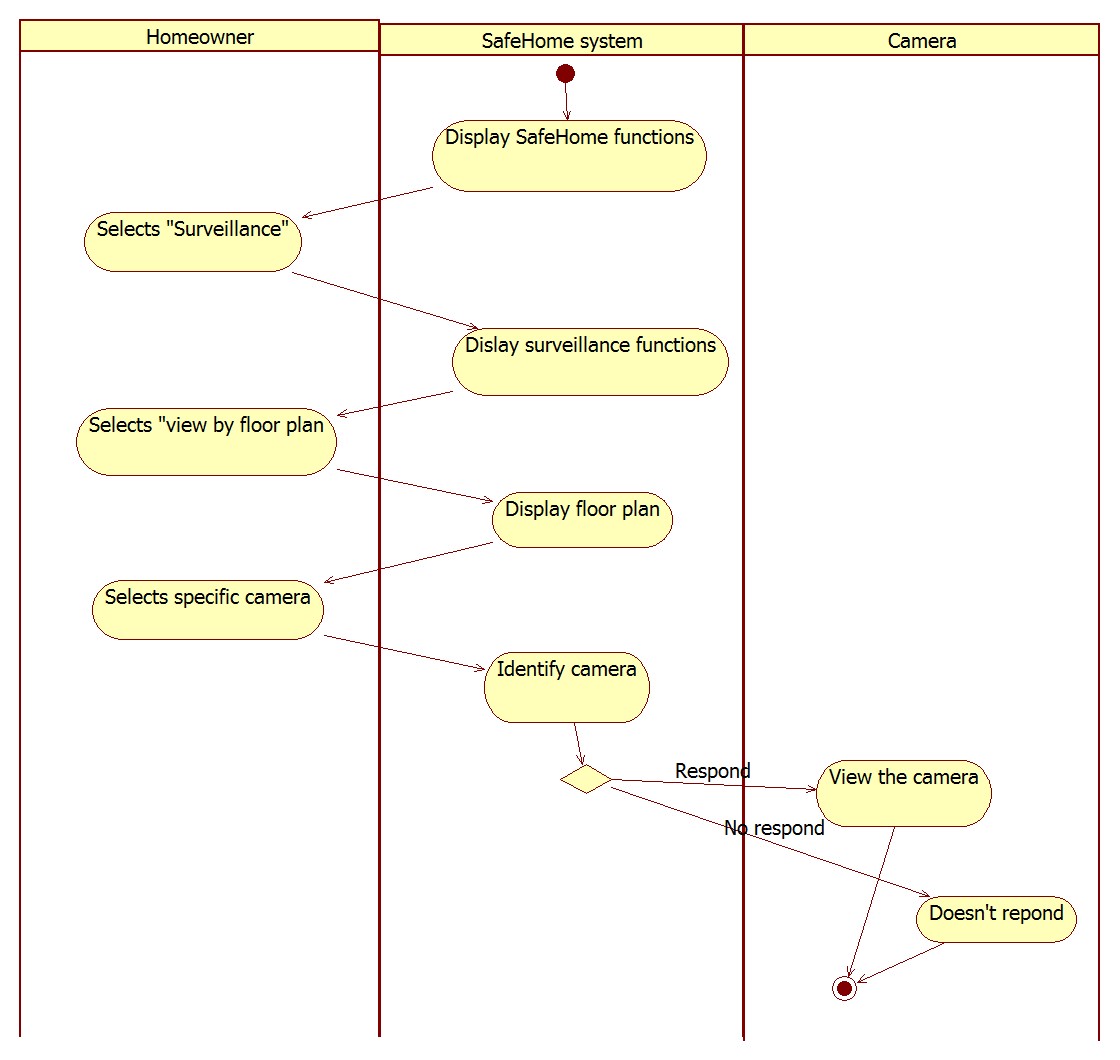
****

SL . Set travel mode

* + - 1. **Camera**

UC . View camera through floor plan window

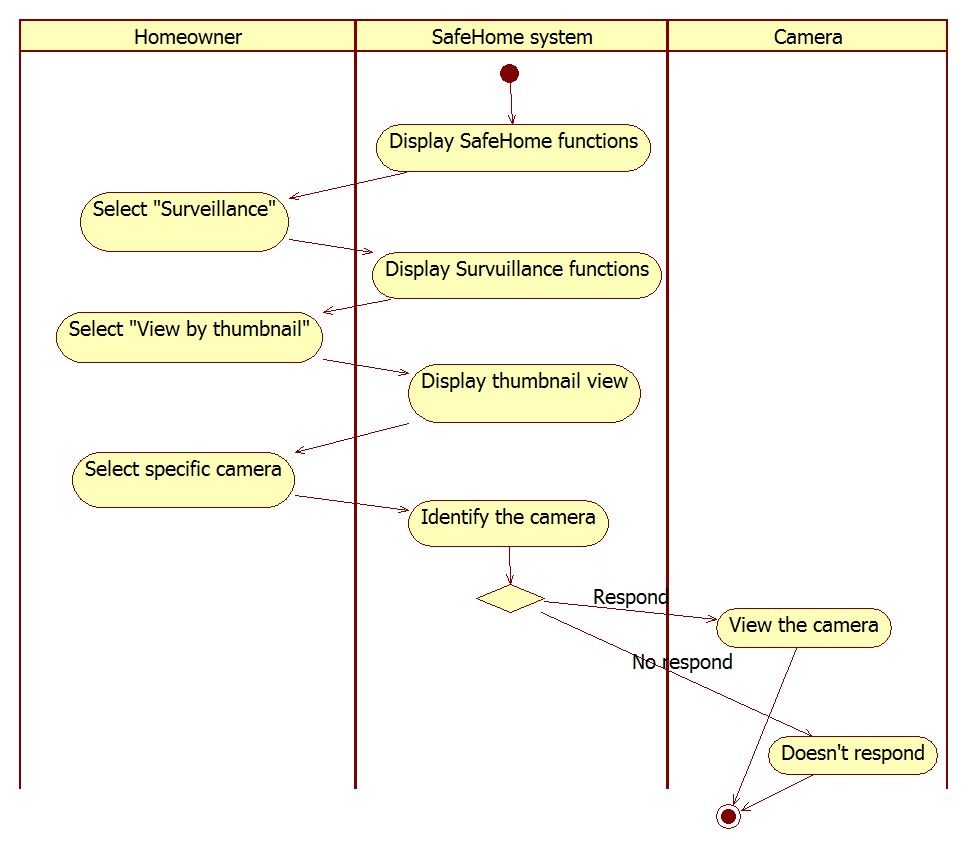
|  |  |
| --- | --- |
| Name | View camera through floor plan window |
| Primary actor | Homeowner |
| Goal in context | The homeowner can access to the *SafeHome* website and view home by selecting a camera in floor plan. |
| Preconditions | 1. *SafeHome* system is fully functional. 2. The homeowner authentication is completed. |
| Trigger | The homeowner enters surveillance menu in webpage. |
| Scenario | 1. Webpage shows all SafeHome functions. 2. The homeowner selects “Surveillance”. 3. Webpage shows all Surveillance functions. 4. The homeowner selects “View by Floor plan”. 5. Webpage shows floor plan of house. 6. The homeowner selects a camera in floor plan. 7. *SafeHome* system identifies the camera by Camera ID. 8. *SafeHome* System displays camera’s view. |
| Exception | The selected camera does not respond. |
| Priority | Medium |
| Channel to actor | Internet |
| Secondary actors | Camera |
| Channels to secondary actors | Camera: Wireless connection |
| Open issues | - |



SL . View camera through floor plan window

UC . View camera through thumbnail

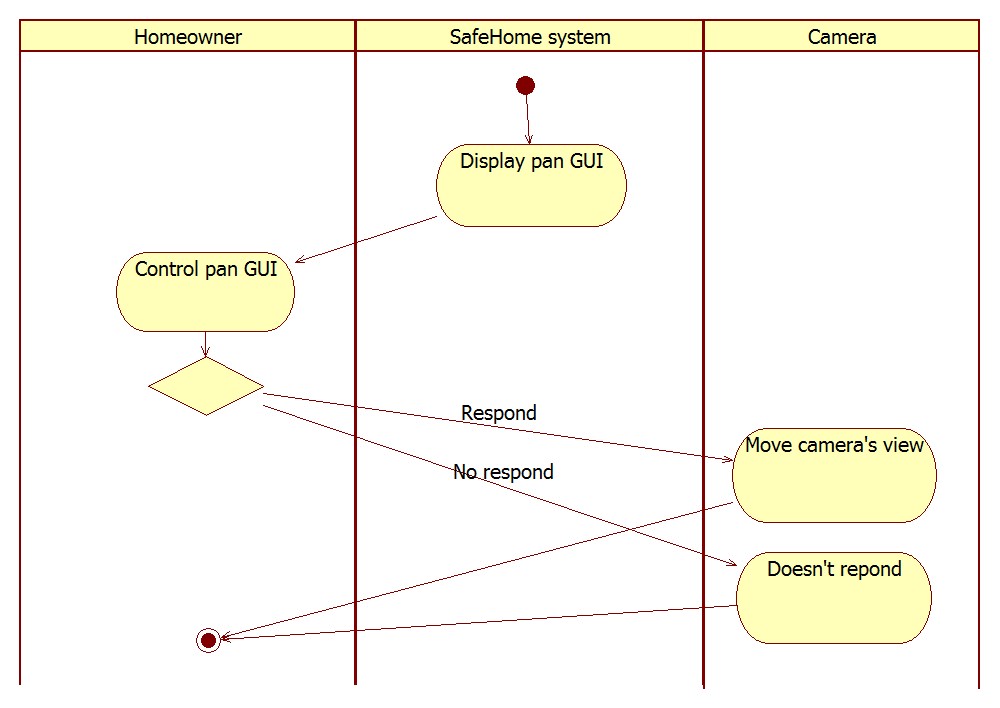
|  |  |
| --- | --- |
| Name | View camera through thumbnail |
| Primary actor | Homeowner |
| Goal in context | The homeowner can access to the *SafeHome* website, view the house through thumbnails. Then, the homeowner select a view in thumbnail and view the house through selected camera. |
| Preconditions | 1. *SafeHome* system is fully functional. 2. Homeowner authentication is completed. |
| Trigger | The homeowner wants to access a camera by thumbnail |
| Scenario | 1. Webpage shows all *SafeHome* functions. 2. The homeowner selects “Surveillance”. 3. Webpage shows all Surveillance functions. 4. The homeowner selects “View by thumbnail”. 5. *SafeHome* system displays thumbnail view from all the cameras. 6. The homeowner selects a specific camera to enlarge. 7. The system identifies the camera by Camera ID. 8. The system enlarges specific camera’s view. |
| Exception | The selected camera does not respond. |
| Priority | Medium |
| Channel to actor | Internet |
| Secondary actors | Camera |
| Channels to secondary actors | Camera : Wireless connections |
| Open issues | 1. How to display the thumbnails depending on number of cameras in system. |



SL . View camera through thumbnail

UC . Pan the camera

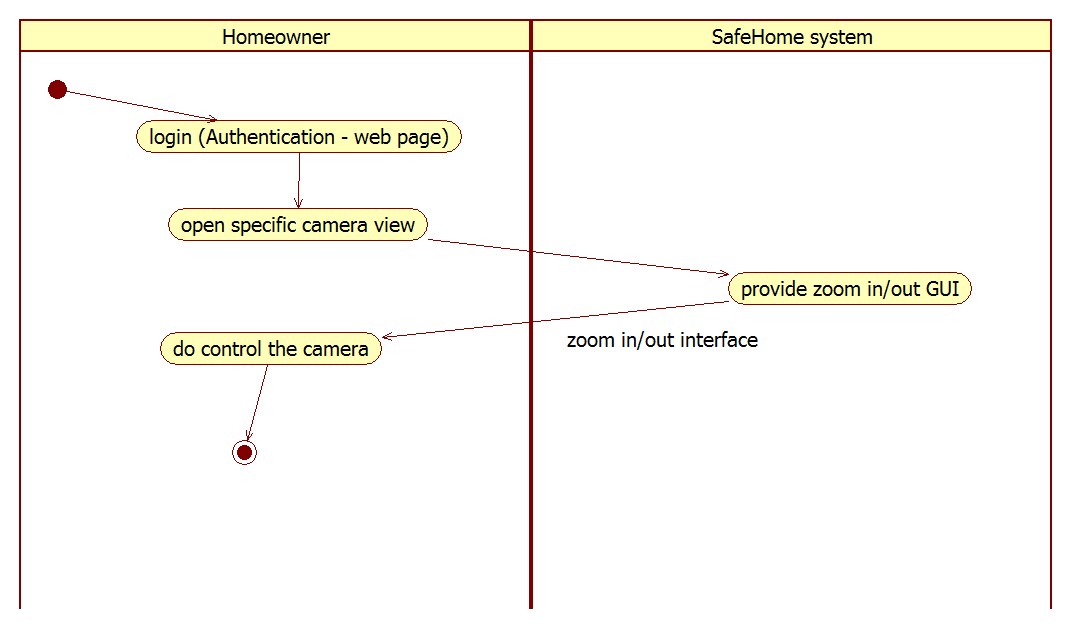
|  |  |
| --- | --- |
| Name | Pan the camera |
| Primary actor | Homeowner |
| Goal in context | The homeowner can pan the selected camera. |
| Preconditions | 1. *SafeHome* system is fully functional. 2. The homeowner opened a specific camera view. |
| Trigger | The homeowner wants to pan the camera. |
| Scenario | 1. Webpage displays pan GUI. Refer [Chapter 5](#_External_Interface_Requirements). 2. The homeowner controls camera using pan GUI. 3. The *SafeHome* system moves the camera’s view according to the homeowner’s command. |
| Exception | The selected camera does not repond. |
| Priority | Low |
| Channel to actor | Internet |
| Secondary actors | Camera |
| Channels to secondary actors | Camera : Wireless connection |
| Open issues | 1. How fast the camera should move? Refer [Chapter 4.1](#_Performance_Requirements). 2. How could the system handle when homeowner wants camera state to initial state? 3. When homeowner wants to move camera to other direction while camera is still moving, how the system should handle this? |



SL . Pan the camera

UC . Zoom in/out a camera

|  |  |
| --- | --- |
| Name | Zoom in/out a camera |
| Primary actor | Homeowner |
| Goal in context | The homeowner can zoom in/out the selected camera. |
| Preconditions | 1. *SafeHome* system is fully functional. 2. The homeowner opened specific camera view |
| Trigger | The homeowner wants to zoom in/out the camera |
| Scenario | 1. Webpage shows zoom in/out GUI. Refer [Chapter 5](#_External_Interface_Requirements). 2. The homeowner controls camera using zoom in/out GUI. 3. The system zooms in/out the camera’s view according to homeowner’s command. |
| Exception | - |
| Priority | Low |
| Channel to actor | Internet |
| Secondary actors | Camera |
| Channels to secondary actors | Camera : Wireless connection |
| Open issues | 1. How fast should camera must zoom in/out? Refer [Chapter 4.1](#_Performance_Requirements). 2. How could the system handle if the homeowner wants to set camera into initial state? |

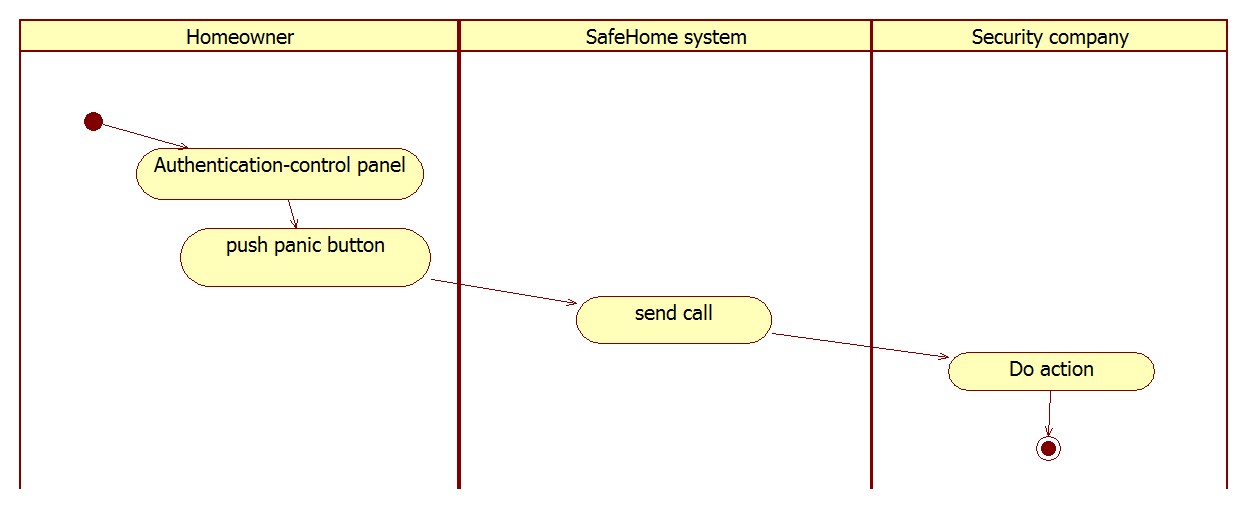


SL . Zoom in/out a camera

* + - 1. **Others**

UC . Panic

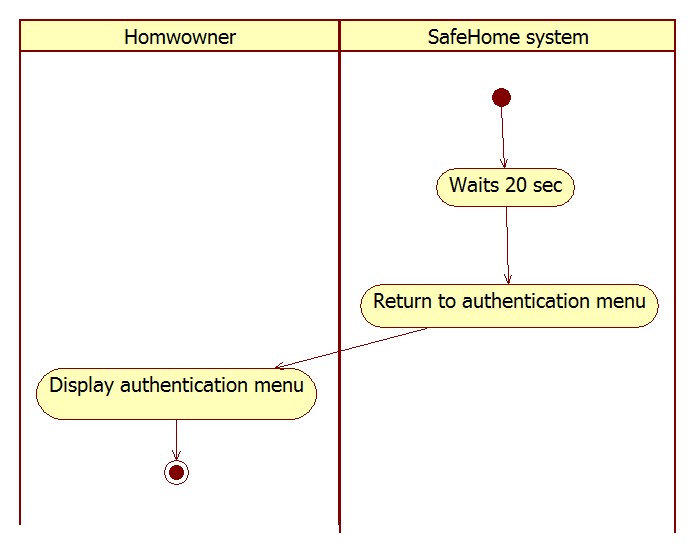
|  |  |
| --- | --- |
| Name | Panic |
| Primary actor | Homeowner |
| Goal in context | The homeowner can send emergency situation to the security company. |
| Preconditions | 1. *SafeHome* system is fully functional. 2. Homeowner authentication is completed. |
| Trigger | The homeowner wants to send emergency situation to security company |
| Scenario | 1. The homeowner pushes panic button in control panel. 2. System sends emergency call to security company through Internet. 3. Security company sends private security to handle the problem. |
| Exception | - |
| Priority | High |
| Channel to actor | Control panel |
| Secondary actors | Security company |
| Channels to secondary actors | Internet |
| Open issues | Homeowner may accidentally push the panic button and want to cancel it. |



SL . Panic

UC . Cancel task and return

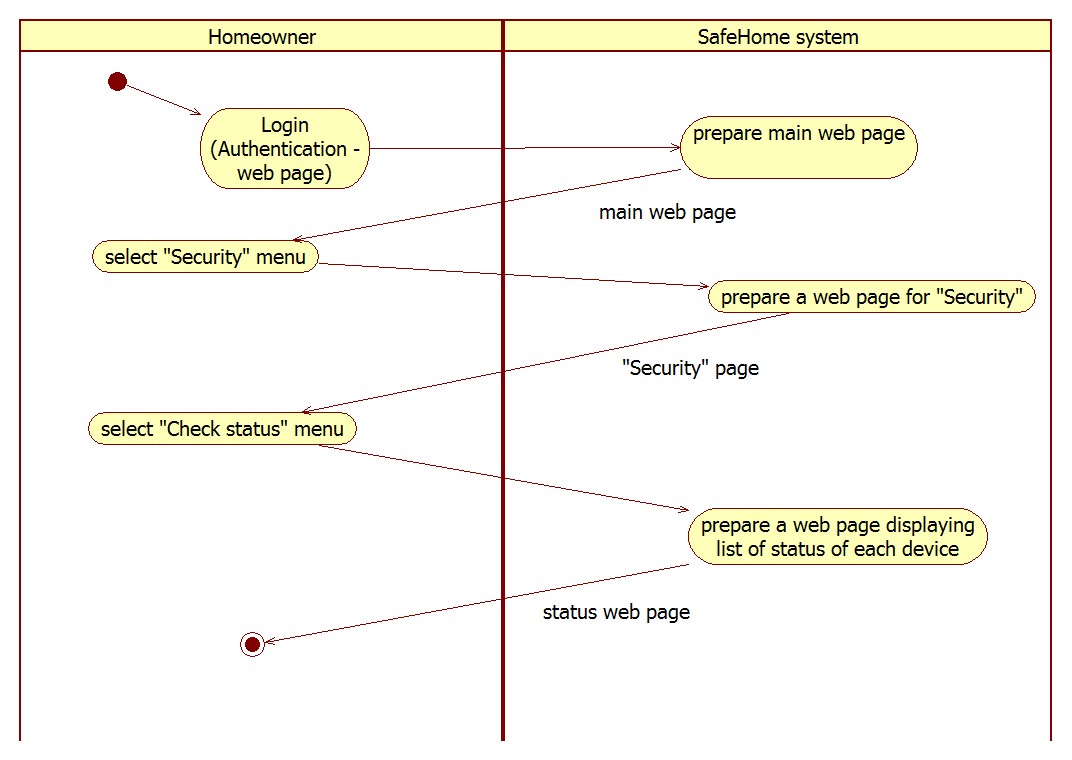
|  |  |
| --- | --- |
| Name | Cancel task and return |
| Primary actor | Homeowner |
| Goal in context | *SafeHome* control panel displays main menu if the homeowner doesn’t respond to request in a certain amount of time. |
| Preconditions | 1. *SafeHome* system is fully functional 2. Homeowner authentication in control panel is done. 3. *SafeHome* system requests an input to the homeowner. |
| Trigger | The homeowner doesn’t respond to request. |
| Scenario | 1. Control panel waits at most 20 seconds for user to input. 2. Control panel returns back to authentication menu. |
| Exception | - |
| Priority | Low |
| Channel to actor | Control panel |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | The homeowner could configure duration of the timeout. |



SL . Cancel task and return

UC . Display status

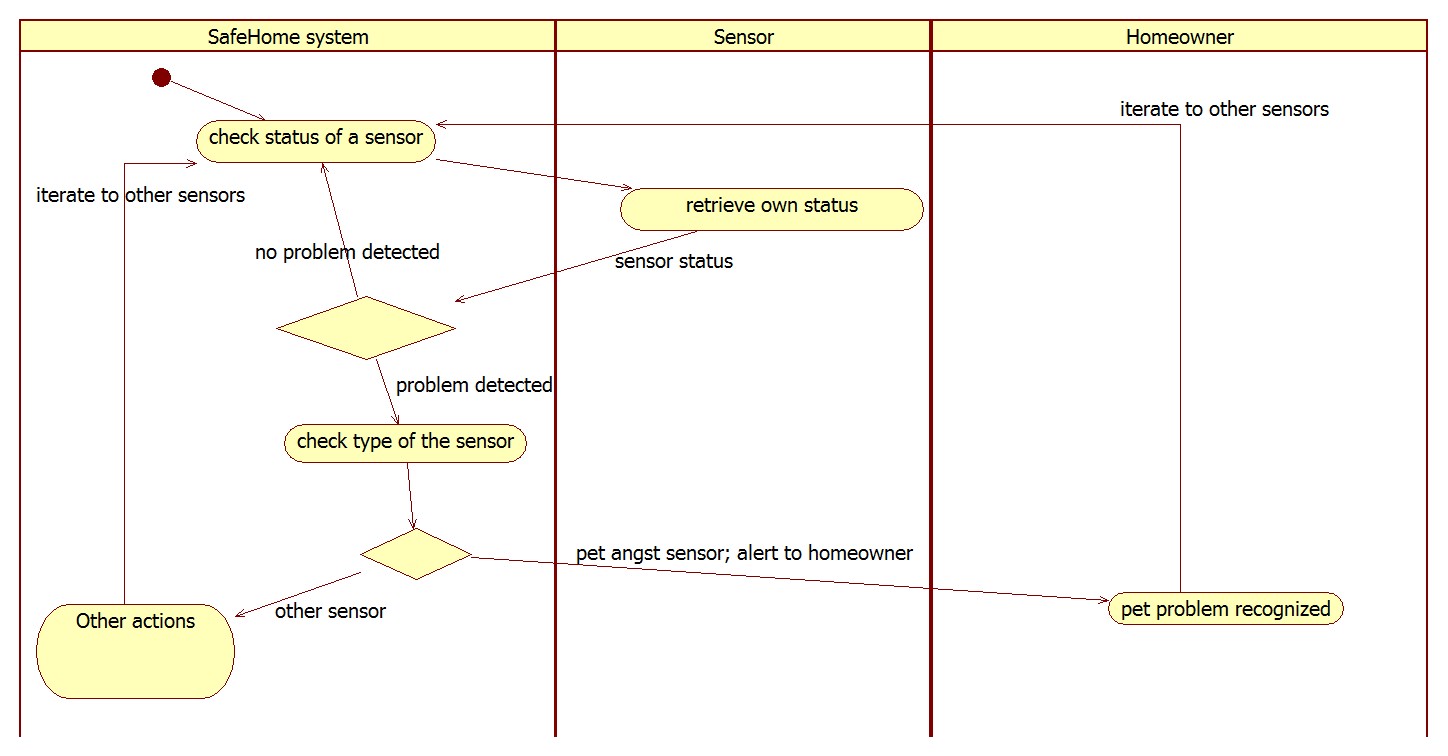
|  |  |
| --- | --- |
| Name | Display status |
| Primary actor | Homeowner |
| Goal in context | To allow the homeowner to inspect every device’s status |
| Preconditions | 1. *SafeHome* system is fully functional. 2. Homeowner authentication is done. |
| Trigger | The homeowner wants to inspect every device’s status. |
| Scenario | 1. The homeowner enters “Security” menu in web page. 2. The homeowner selects “Check status”. 3. The system displays list of status of each device. |
| Exception | - |
| Priority | Medium |
| Channel to actor | Internet |
| Secondary actors | Device |
| Channels to secondary actors | Device: wireless communication |
| Open issues | - |



SL . Display status

UC . Pet angst sensor

|  |  |
| --- | --- |
| Name | Pet angst sensor |
| Primary actor | Pet angst sensor |
| Goal in context | To allow the homeowner that his or her pets have a trouble. |
| Preconditions | 1. *SafeHome* system is fully functional. |
| Trigger | Pet angst sensor raises pet problem signal to *SafeHome* system. |
| Scenario | 1. A homeowner’s pet has problem. 2. The pet starts to bark. 3. Pet angst sensor detects the situation. 4. The sensor sends signal to *SafeHome* system. 5. *SafeHome* system notifies the situation to the homeowner through Internet. |
| Exception | - |
| Priority | Low |
| Channel to actor | Wireless communication |
| Secondary actors | Homeowner |
| Channels to secondary actors | Homeowner: Internet |
| Open issues | - |



SL . Pet angst sensor

## **User-requested information retrieval service**

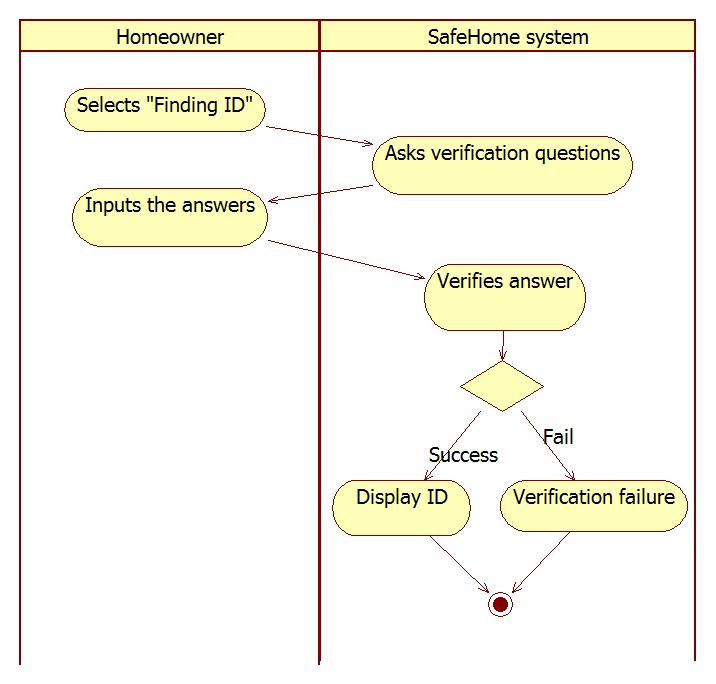
* + 1. **Description**

SafeHome system stores various data such as, ID, passwords, system usage, web page access, and recorded video files. Therefore, homeowner should retrieve these data when homeowner needs it. Moreover, homeowner should retrieve ID or passwords when he/she lost ID and passwords.

* + 1. **Use cases**
       1. **Finding ID/Password**

UC . Finding ID

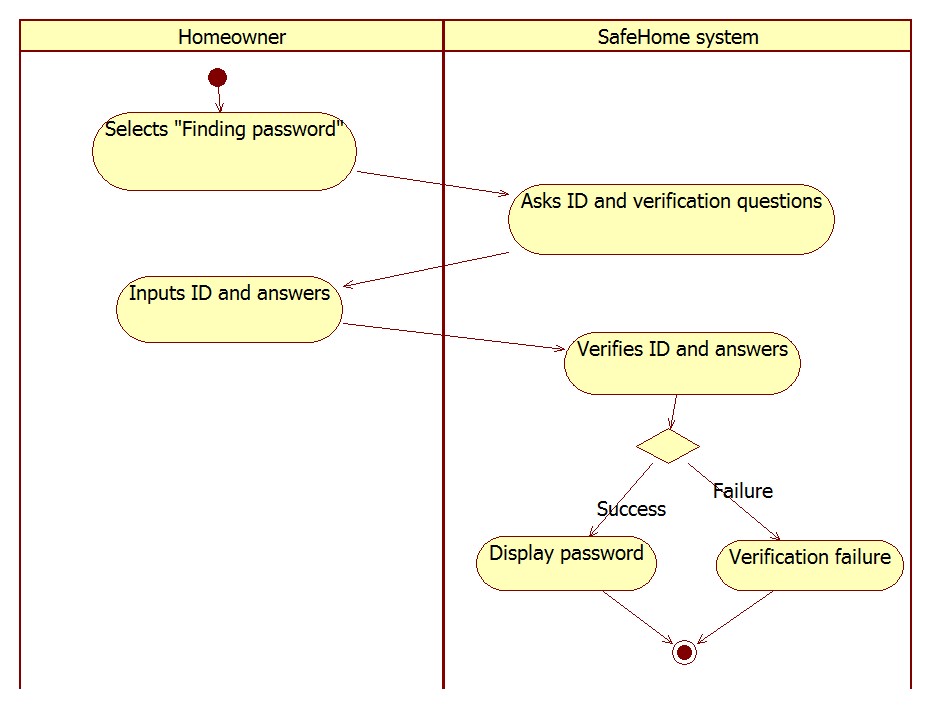
|  |  |
| --- | --- |
| Name | Finding ID |
| Primary actor | Homeowner |
| Goal in context | Homeowner gets the lost ID. |
| Preconditions | *SafeHome* system is fully functional. Homeowner tries to access *SafeHome web page*. |
| Trigger | Homeowner forgets the ID and wants to find ID. |
| Scenario | 1. Homeowner selects “Finding ID” 2. Webpage asks verification questions such as homeowner’s name and phone number. 3. Homeowner inputs the answers. 4. *SafeHome* system verifies answers. 5. *SafeHome* system displays the ID. |
| Exception | 1. Homeowner inputs wrong answer to verification questions. |
| Priority | High |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | - |



SL . Finding ID

UC . Finding password

|  |  |
| --- | --- |
| Name | Finding password |
| Primary actor | Homeowner |
| Goal in context | Homeowner gets the lost password. |
| Preconditions | *SafeHome* system is fully functional. Homeowner tries to access *SafeHome web page*. |
| Trigger | Homeowner forgets the password and wants to find password. |
| Scenario | 1. Homeowner selects “Finding password” 2. Webpage asks homeowner’s ID and verification questions such as homeowner’s name and phone number. 3. Homeowner inputs ID and answers. 4. *SafeHome* system verifies the ID and answers. 5. *SafeHome* system displays the password. |
| Exception | 1. Homeowner inputs wrong ID or wrong answer to verification questions. |
| Priority | High |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | - |

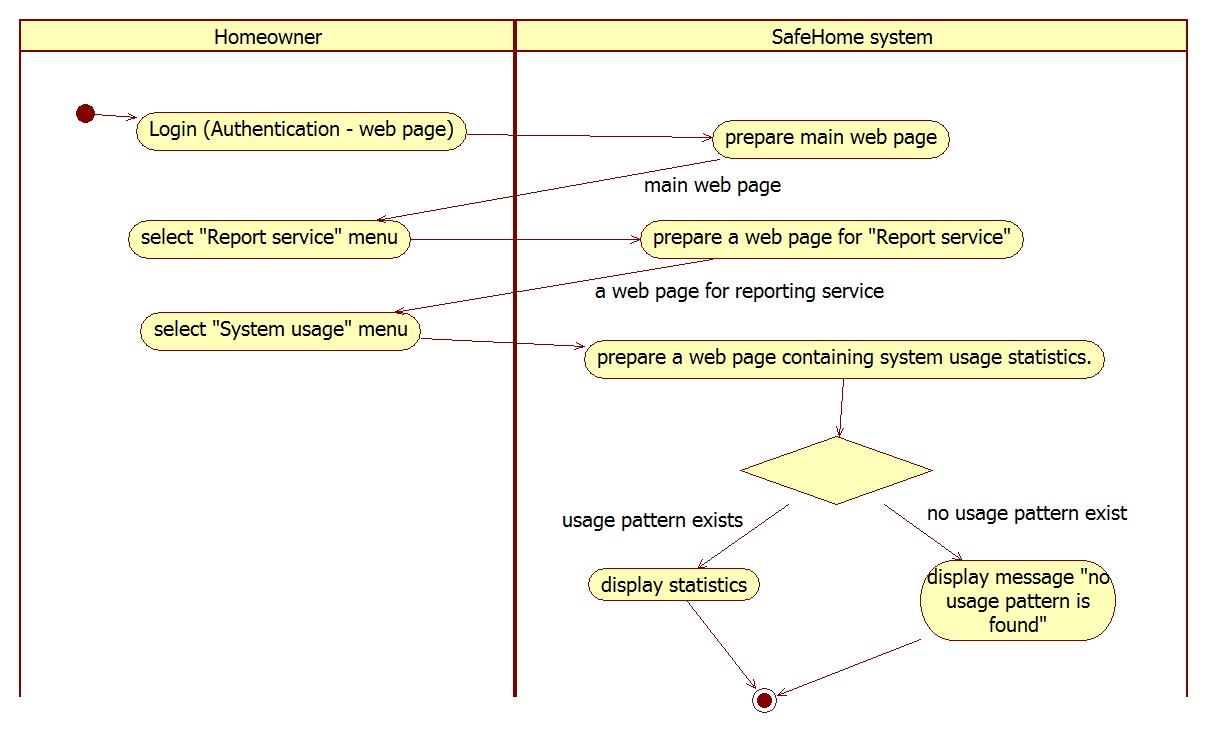
****

SL . Finding password

* + - 1. **Reporting system usage pattern**

UC . Reporting system usage pattern

|  |  |
| --- | --- |
| Name | Reporting system usage pattern |
| Primary actor | Homeowner |
| Goal in context | To allow the homeowner to check his or her usage pattern on *SafeHome* system |
| Preconditions | 1. Homeowner authentication must be done. 2. Internet connection is available. |
| Trigger | The homeowner decided to check his or her usage pattern. |
| Scenario | 1. The homeowner access *SafeHome* webpage. 2. The homeowner selects “Report service” menu. 3. The homeowner selects “System usage” menu. 4. The system displays usage statistics up to now. |
| Exception | 1. No usage pattern exists; when the system is newly installed.  * Print “No usage pattern is found”. |
| Priority | Low |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | - |

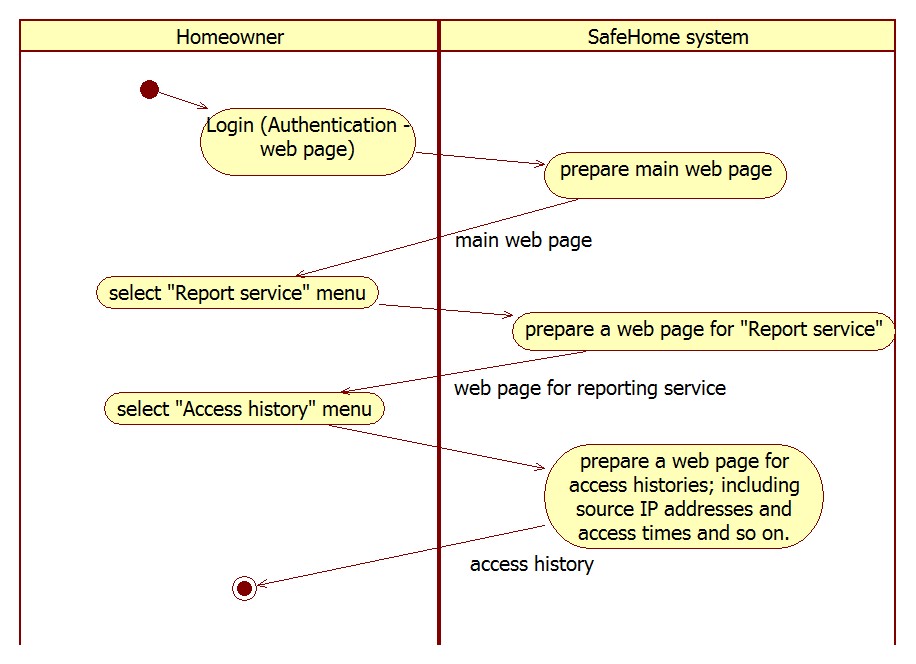
****

SL . Reporting system usage pattern

* + - 1. **Reporting web page access history**

UC . Reporting web page access history

|  |  |
| --- | --- |
| Name | Reporting web page access history |
| Primary actor | Homeowner |
| Goal in context | To allow the homeowner to inspect web page access history |
| Preconditions | 1. Homeowner authentication must be done. 2. Internet connection is available. |
| Trigger | The homeowner decided to inspect access history for security. |
| Scenario | 1. The homeowner access *SafeHome* webpage. 2. The homeowner selects “Report service” menu. 3. The homeowner selects “Access history” menu. 4. The system displays list of access information up to now. List includes source IP address, access time, and so on. |
| Exception | - |
| Priority | Low |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | - |

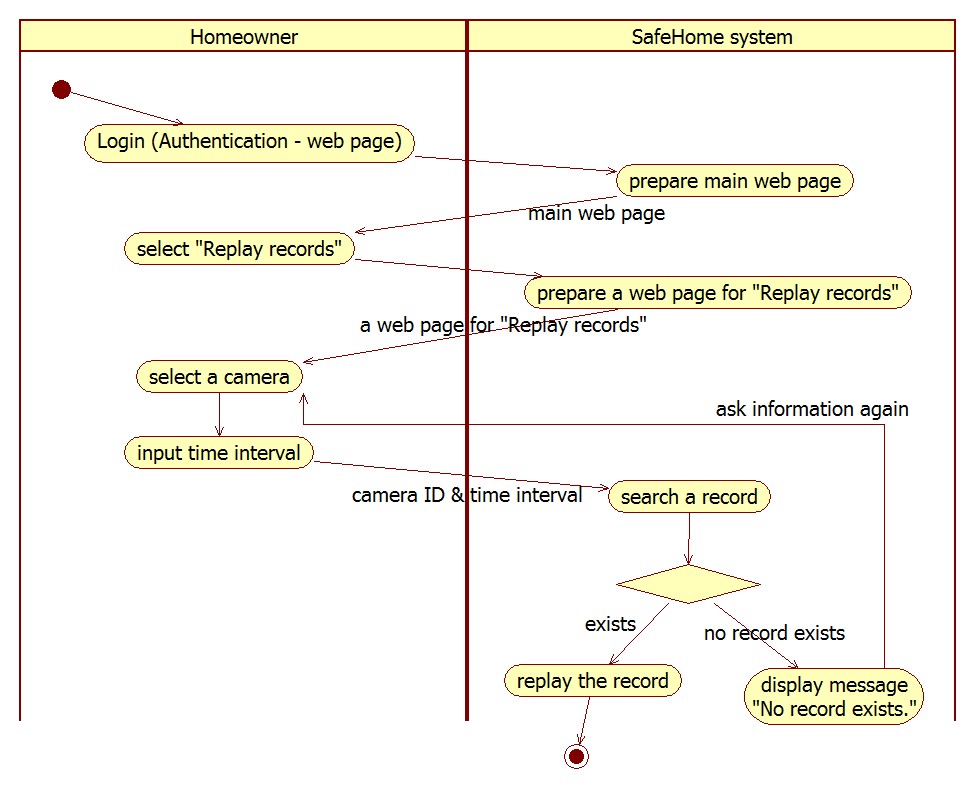
****

SL . Reporting web page access history

* + - 1. **Replaying recorded movie**

UC . Replay the record

|  |  |
| --- | --- |
| Name | Replay the record |
| Primary actor | Homeowner |
| Goal in context | The homeowner can select a camera record and replay the record. |
| Preconditions | 1. *SafeHome* system is fully functional. 2. The homeowner accessed to Surveillance functions. |
| Trigger | The homeowner wants to replay the camera record |
| Scenario | 1. Webpage shows all Surveillance functions. 2. The homeowner selects “Replay the record”. 3. Webpage shows the list of records. 4. The homeowner selects the record. 5. System displays the record by identifying the record by Camera ID. |
| Exception | 1. No record exist – display message “No record exist”. |
| Priority | High |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | 1. The homeowner should be able to move video forward or backward. |



SL . Replay the record

## **Authentication**

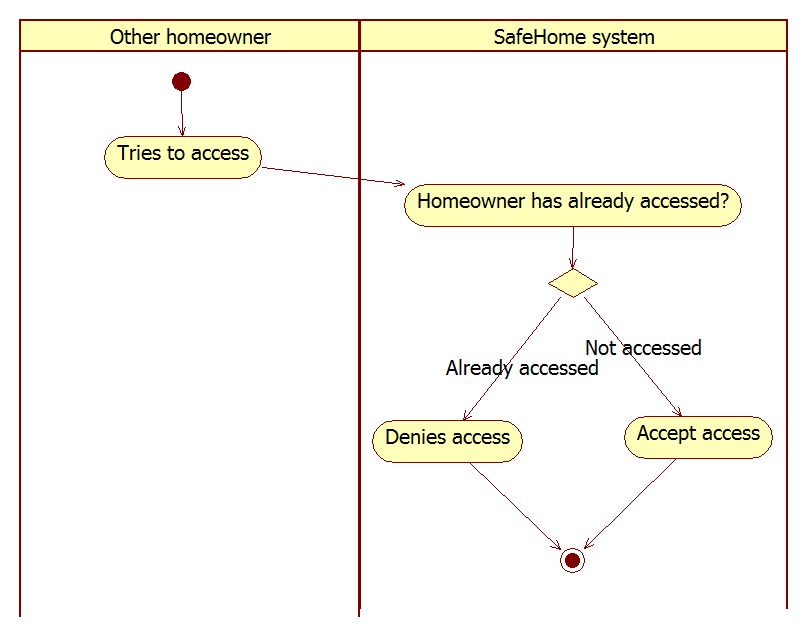
* + 1. **Description**

*SafeHome* system should be managed by legal homeowners. Therefore, *SafeHome* system requires authentication before the system grants a permission to access. In control panel, the system asks 4-digits password which can be typed using 12-buttons keypad. The system asks two passwords in web interface.   
 Moreover, the system should handle concurrent accesses because there are two interfaces and Internet allows more than one accesses. The system allows only one session at any time to avoid any confliction. Because a homeowner could forget to logoff the system, the system closes the session after certain fixed timeout (20 seconds in control panel, 1 minute in web page).

* + 1. **Use case diagram**
    2. **Use cases**
       1. **Session**

UC . Deny concurrent user accesses

|  |  |
| --- | --- |
| Name | Deny concurrent user accesses |
| Primary actor | Other homeowner |
| Goal in context | Other homeowner can’t access to the *SafeHome web page* or control panel when homeowner already accessed to one of *SafeHome web page* or control panel. |
| Preconditions | *SafeHome* system is fully functional. Homeowner accessed to one of *SafeHome web page* or control panel. |
| Trigger | Other homeowner tries to access *SafeHome* system through Internet or control panel. |
| Scenario | 1. Other homeowner tries to access *SafeHome web page* or control panel 2. *SafeHome* system checks whether homeowner has already accessed to the system. 3. *SafeHome* system denies the access. |
| Exception | - |
| Priority | Medium |
| Channel to actor | Internet or control panel |
| Secondary actors | Homeowner |
| Channels to secondary actors | Homeowner : Internet or control panel |
| Open issues | 1. When homeowner forgets to logout after accessing *SafeHome web page*, and homeowner tries to access concurrently, how can system classify between Other homeowner and homeowner. |

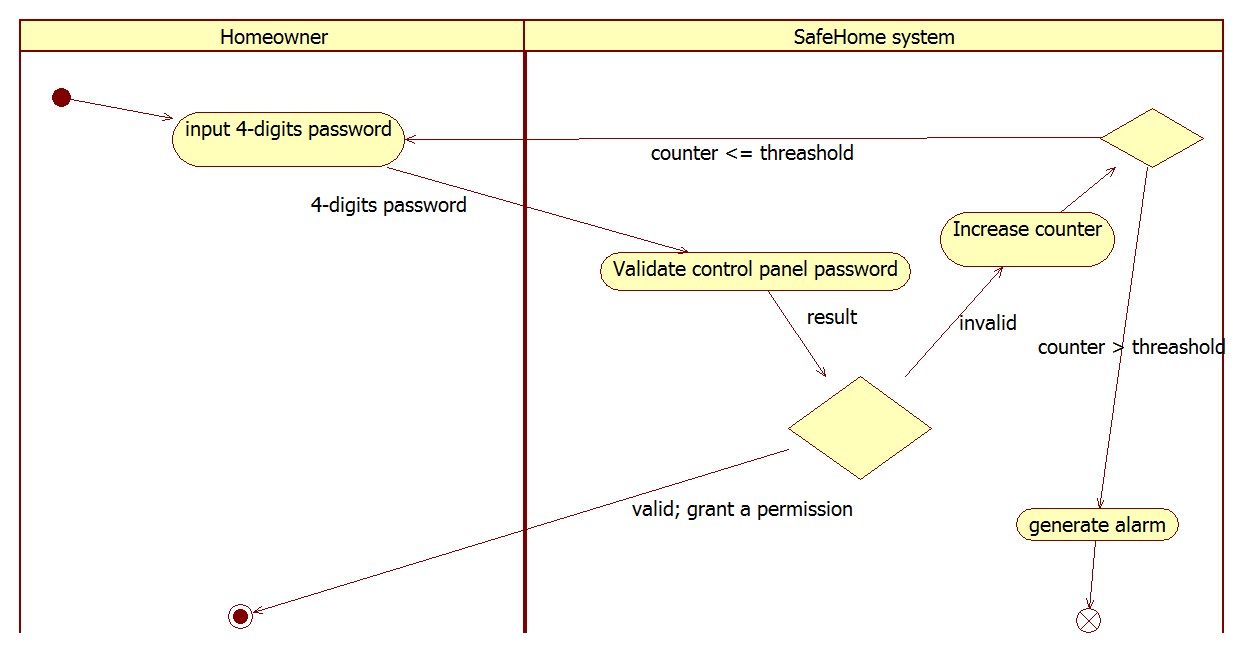
****

SL . Deny concurrent user accesses

* + - 1. **Control panel**

UC . Authentication-ControlPanel

|  |  |
| --- | --- |
| Name | Authentication-ControlPanel |
| Primary actor | Homeowner |
| Goal in context | The homeowner can control *SafeHome* system through control panel. |
| Preconditions | *SafeHome* system is fully functional. |
| Trigger | The homeowner wants to access *SafeHome* system through control panel |
| Scenario | 1. The homeowner gets to control panel in a home. 2. The system asks 4-digit password. 3. The homeowner inputs the password. 4. Now the system is controllable. |
| Exception | 1. Incorrect input password |
| Priority | High |
| Channel to actor | Control panel |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | 1. How should system act when homeowner inputs too many incorrect password? Generate alarming sound. |

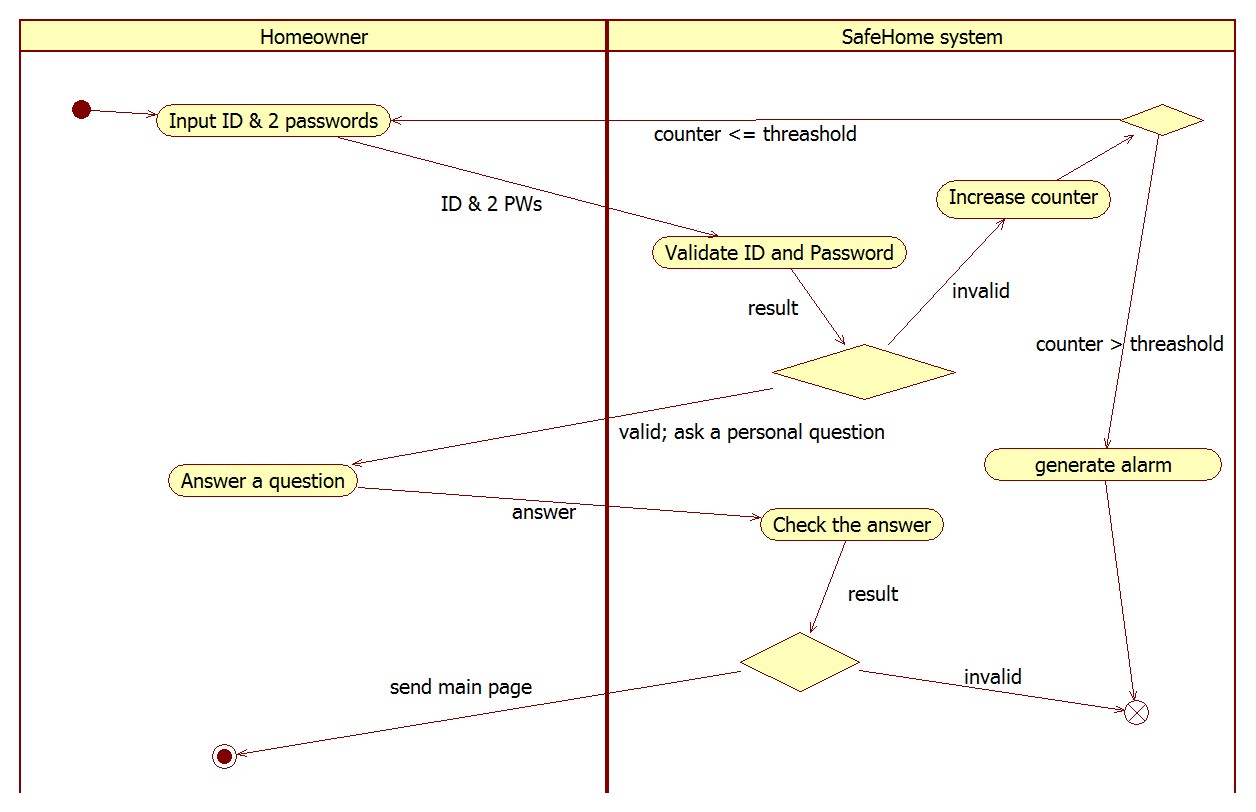


SL . Authentication-control panel

* + - 1. **Webpage**

UC . Authentication-Webpage

|  |  |
| --- | --- |
| Name | Authentication-Webpage (UC-AW) |
| Primary actor | Homeowner |
| Goal in context | The homeowner can access to the *SafeHome* system through web site interface and view *SafeHome* functions. |
| Preconditions | *SafeHome* system is fully functional. |
| Trigger | The homeowner wants to access *SafeHome* system through Internet. |
| Scenario | 1. The homeowner accesses *SafeHome* web page. 2. The homeowner enters ID and two passwords (each password should be 8 characters or longer). 3. Web page asks verification question such as a phone number or address. 4. The homeowner answers an additional question correctly. 5. Webpage shows all *SafeHome* functions. |
| Exception | 1. Incorrect input of ID or password will 2. Incorrect input of verification question |
| Priority | High |
| Channel to actor | Internet |
| Secondary actors | - |
| Channels to secondary actors | - |
| Open issues | 1. How should system act when homeowner inputs too many incorrect password? Refer [Chapter 4.3](#_Security_Requirements). 2. How should system handle when homeowner forgets the password or ID? |



SL . Authentication-web page

## **User Interface**

* + 1. **Description**

The homeowner may access the *SafeHome* system via two different interface: 1. control panel hardware interface and 2. Web Interface on a web browser.

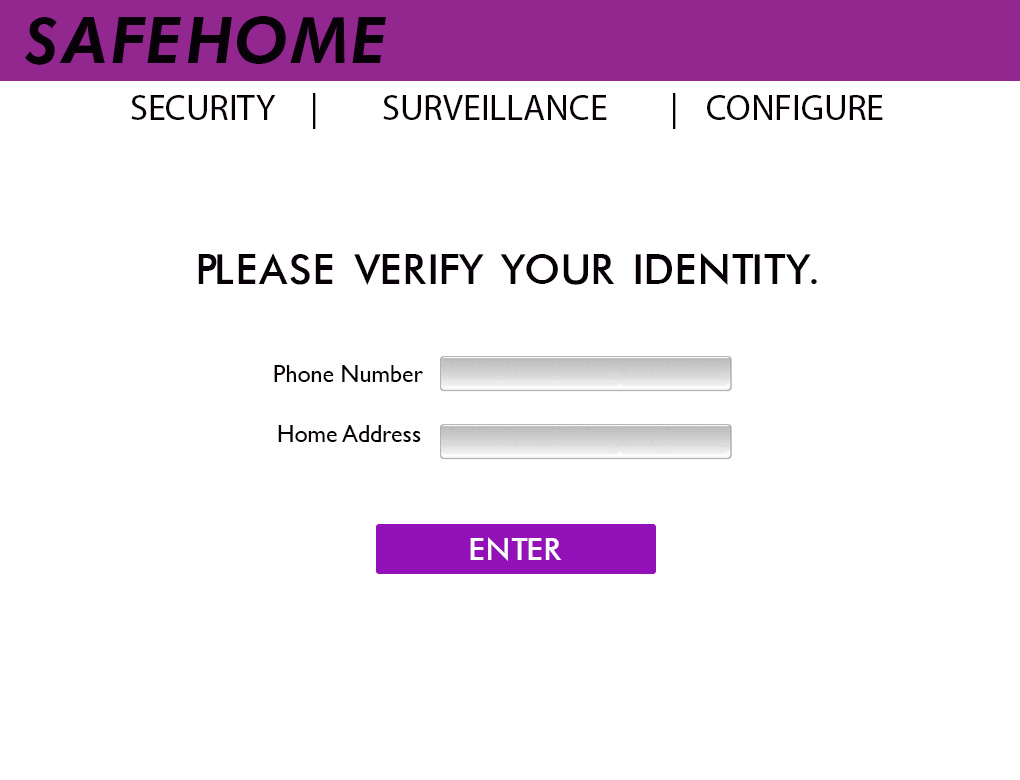
* + 1. **Web User Interface**

The homeowner accesses the *SafeHome* system from the web by the IP address of the *SafeHome* server. The main page guides the user to sign in with the username and the two passwords. The user will enter the username and passwords to move on to the next page.



ID . Web interface - login page

To access the *SafeHome* system, the homeowner has to verify his/her identity by entering his/her address or phone number.



ID . Web interface - Accessing Security Function

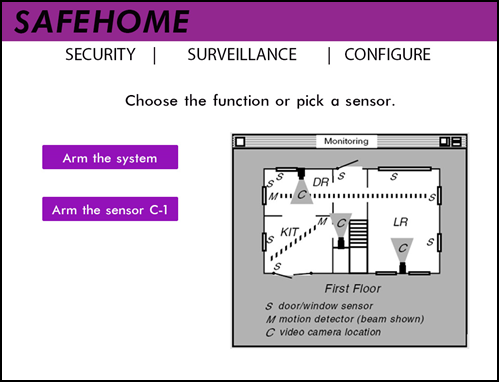
When the verification has completed, the following interface will be shown. The interface shows the list of all categories of *SafeHome* functions.



ID . Web interface - Main page with list of functions

* + - 1. **Security Function**

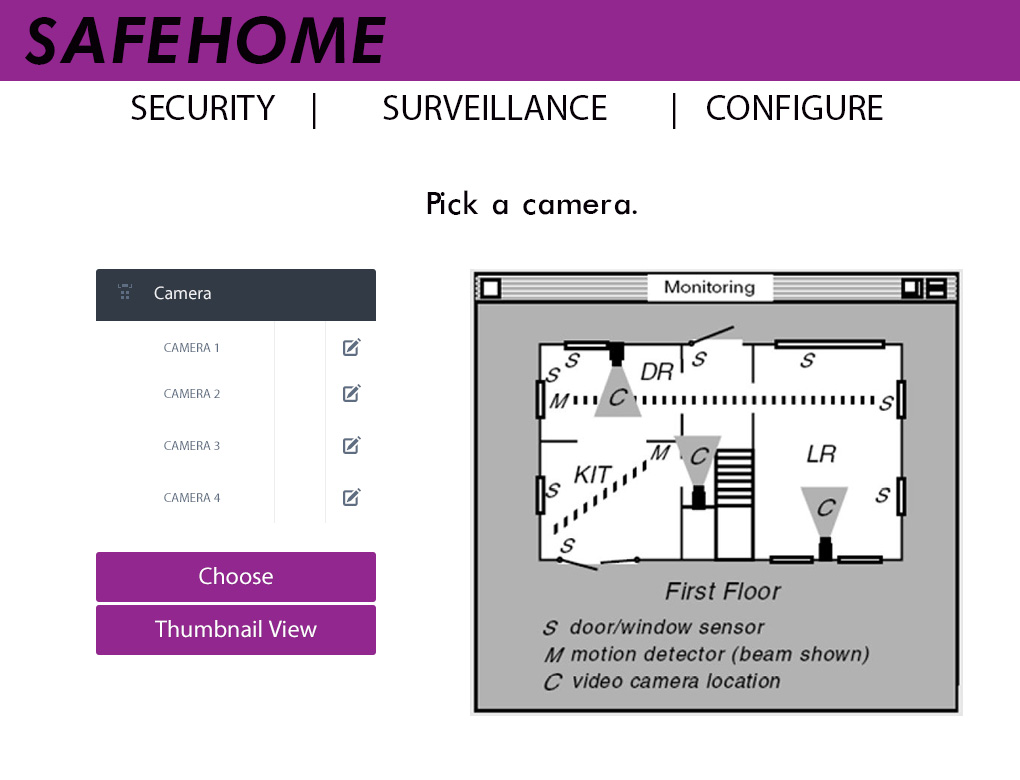
When the homeowner enters security menu, the homeowner can arm/disarm *SafeHome* or other security features.



ID . Web interface - Security Control Panel

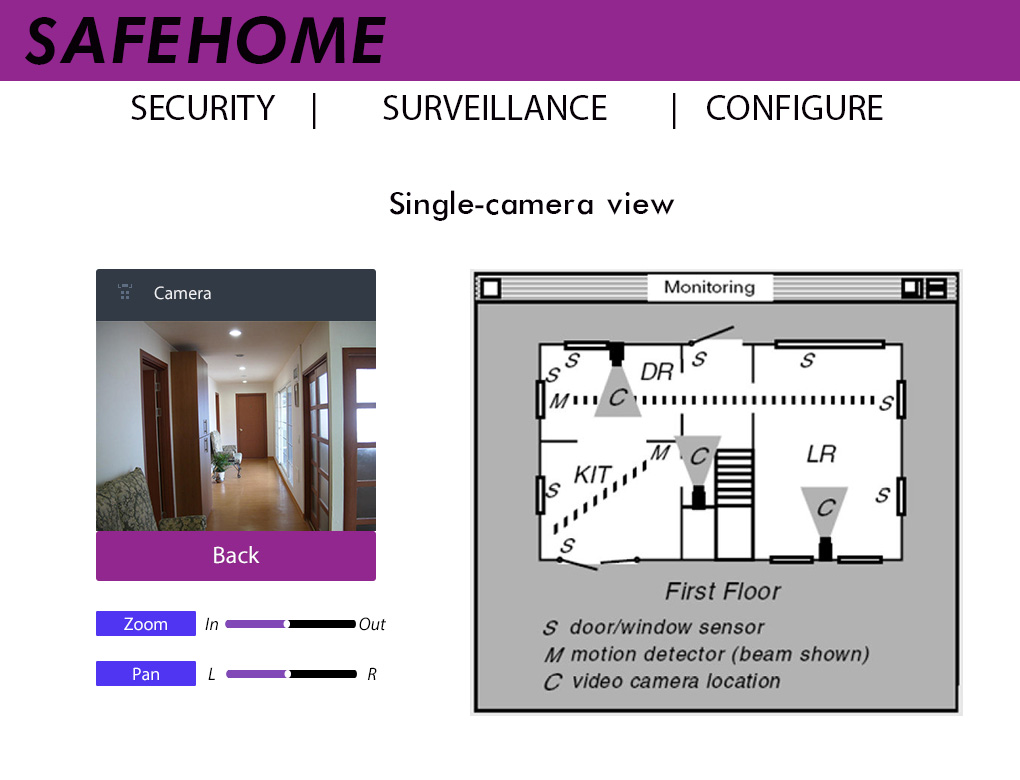
* + - 1. **Surveillance Functions**

The surveillance function provides the homeowner with an interface showing the floor plan and the list of cameras to choose from.



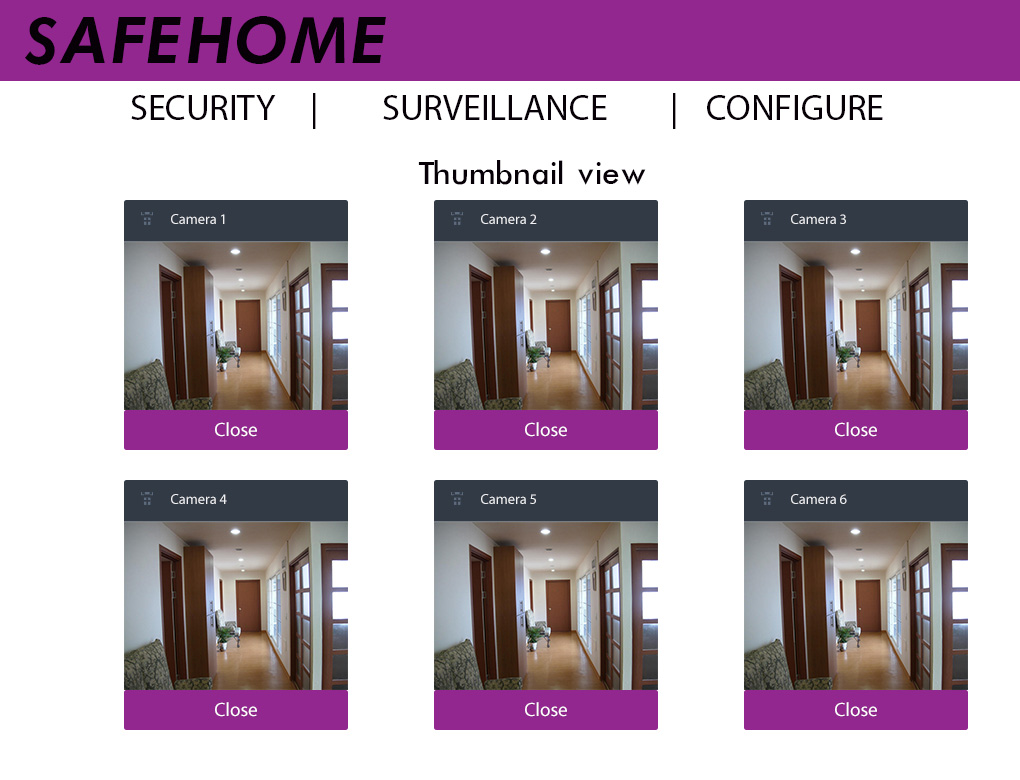
ID . Web interface - viewing camera

Once the user chooses a camera, the system will play the real-time camera view. The zoom and pan interface will allow the user to alter the camera perspective.



ID . Web interface - Single-camera view

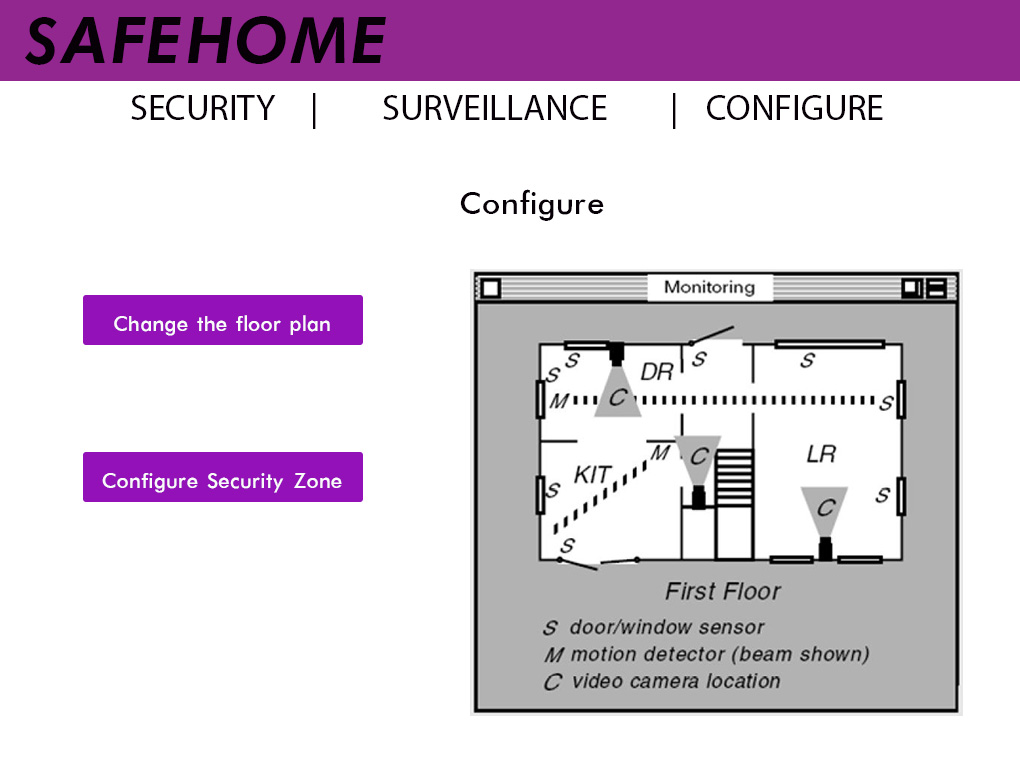
The homeowner can also choose to watch the thumbnail view of all cameras, provided in grid view.



ID . Web interface - Thumbnail view

* + - 1. **Configuration Functions**

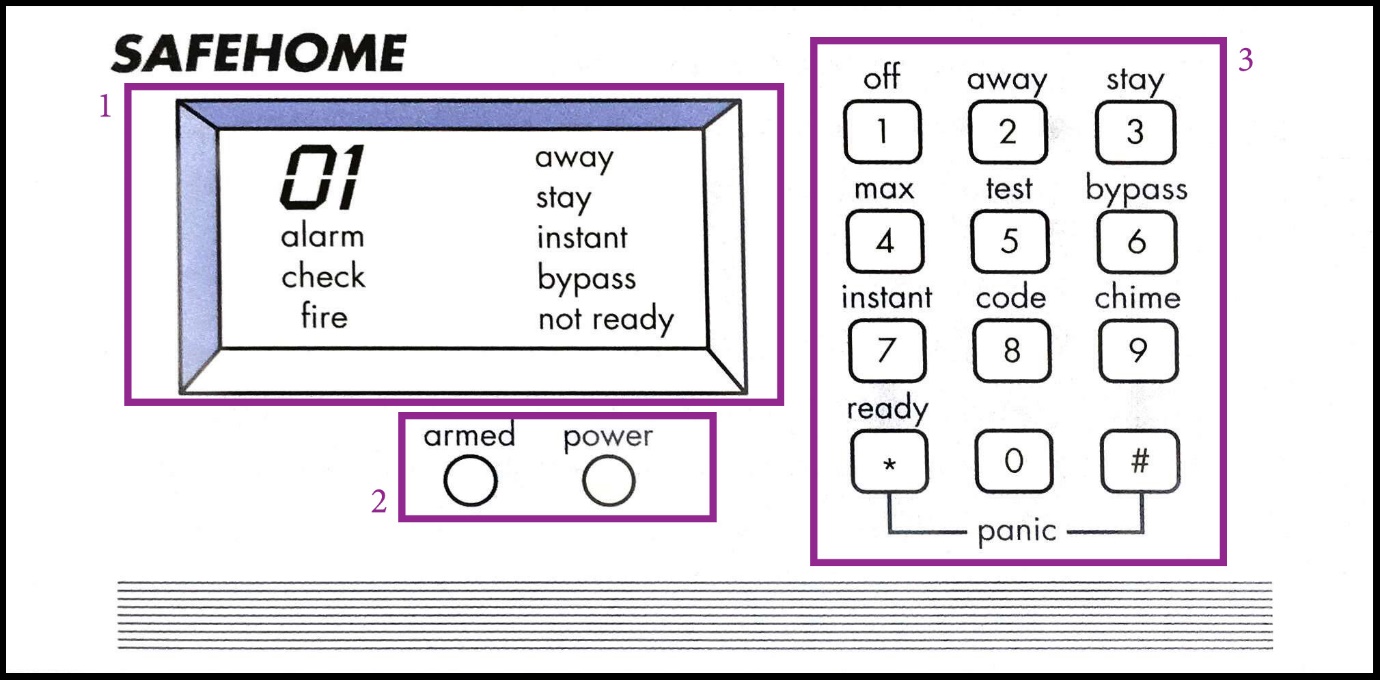
The homeowner can configure the security zone and change the floor plan using the configure menu.



ID . Web interface - Configuration menu

* + 1. **Hardware User Interface**

The hardware provided in the *SafeHome* system is rather antique. It has small black-and-white LCD (labelled 1), and telephone-style push-button keypad (labelled 3). It also has two LED lights (labelled 2) for signaling the power status and armed status.



ID . Control panel interface

The default page shows states of the system (not-ready state means that the doors/windows are open). The user can manually set stay or away mode by pressing the button. Before the user makes any command, he/she must put in the four-digit password. The panel signals an error if the password is wrong. If correct, the user can proceed to another command.

# **Non-functional Requirements**

## **Performance Requirements**

* + 1. *SafeHome* must be real-time system to detect trespassers anytime. *SafeHome* must retrieve all sensor status in real time and notifies a homeowner if there is anything suspiciousness. In addition, to provide quality video feed from security cameras, *SafeHome* should be able to display videos, all of which have at least 1 frame per second.
    2. A *SafeHome* camera must move with proper speed when a homeowner pans the camera.
    3. A *SafeHome* camera must zoom in/out with proper speed when a homeowner zooms the camera in/out.

## **Safety Requirements**

* + 1. If any of devices becomes wrong, *SafeHome* should notify homeowner, so that the homeowner can inspect and handle suspicious devices.
    2. *SafeHome* must contain UPS (Uninterruptible Power Supply) to manage unexpected electricity shortage. UPS must have enough capacity to keep *SafeHome* running for 3 days. We assumed that homeowner is away less than 3 days in most cases.

## **Security Requirements**

* + 1. When a user inputs wrong password for specified number of time, the user could be intruder instead of a homeowner. Therefore, *SafeHome* system asks simple questions such as phone number and address.
    2. Webpage data must be encrypted and sent to network.
    3. Camera’s wireless connection must be secured and not viewed from outside of a homeowner.
    4. Webserver program uses secured HTTP protocol e.g. HTTPS, SSH, etc.

# **Traceability**

## **Relationships between use cases and non-functional requirements**

The following table describes relationships between each use case and non-functional requirements. Non-functional requirement is described as PR<#>, SaR<#> and SeR<#>. Each represents #-th Performance Requirement, Safety Requirement, and Security Requirement respectively.

Table . Traceability matrix for use-case scenarios

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | [PR1](#_SafeHome_must_be) | [PR2](#_A_SafeHome_camera) | [PR3](#_A_SafeHome_camera_1) | [SaR1](#_If_any_of) | [SaR2](#_SafeHome_must_contain) | [SeR1](#_When_a_user) | [SeR2](#_Webpage_data_must) | [SeR3](#_Camera’s_wireless_connection) | [SeR4](#_Webserver_program_uses) |
| [UC1](#UC1) |  |  |  |  |  |  | O |  |  |
| [UC2](#UC2) |  |  |  |  |  |  | O |  | O |
| [UC3](#UC3) |  |  |  | O |  |  | O |  | O |
| [UC4](#UC4) |  |  |  | O |  |  | O |  | O |
| [UC5](#UC5) |  |  |  |  | O |  |  |  |  |
| [UC6](#UC6) |  |  |  |  | O |  |  |  |  |
| [UC7](#UC7) |  |  |  |  |  |  | O |  |  |
| [UC8](#UC8) |  |  |  |  | O |  |  |  | O |
| [UC9](#UC9) | O |  |  | O | O |  | O |  | O |
| [UC10](#UC10) | O |  |  | O | O |  | O |  | O |
| [UC11](#UC11) | O |  |  |  | O |  | O |  | O |
| [UC12](#UC12) |  |  |  | O | O |  | O |  | O |
| [UC13](#UC13) | O |  |  |  | O |  | O | O | O |
| [UC14](#UC14) | O |  |  |  | O |  | O | O | O |
| [UC15](#UC15) | O | O |  |  | O |  |  |  |  |
| [UC16](#UC16) | O |  | O |  | O |  |  |  |  |
| [UC17](#UC17) | O |  |  |  | O |  |  |  |  |
| [UC18](#UC18) | O |  |  |  | O |  |  |  |  |
| [UC19](#UC19) | O |  |  | O | O |  | O |  | O |
| [UC20](#UC20) | O |  |  | O | O |  | O |  | O |
| [UC21](#UC21) |  |  |  |  |  | O |  |  |  |
| [UC22](#UC22) |  |  |  |  |  | O |  |  |  |
| [UC23](#UC23) |  |  |  | O |  |  |  |  |  |
| [UC24](#UC24) |  |  |  | O |  |  |  |  |  |
| [UC25](#UC25) |  |  |  |  |  |  | O |  | O |
| [UC26](#UC26) |  |  |  |  | O |  |  |  |  |
| [UC27](#UC27) |  |  |  |  | O | O |  |  |  |
| [UC28](#UC28) |  |  |  |  | O | O | O |  | O |

## **Relationships between interface diagrams and non-functional requirements**

Table . Traceability Matrix for Interface Diagram

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | [PR1](#_SafeHome_must_be) | [PR2](#_A_SafeHome_camera) | [PR3](#_A_SafeHome_camera_1) | [SaR1](#_If_any_of) | [SaR2](#_SafeHome_must_contain) | [SeR1](#_When_a_user) | [SeR2](#_Webpage_data_must) | [SeR3](#_Camera’s_wireless_connection) | [SeR4](#_Webserver_program_uses) |
| [ID1](#ID1) |  |  |  |  |  | O |  |  | O |
| [ID2](#ID2) |  |  |  |  |  | O |  |  | O |
| [ID3](#ID3) |  |  |  |  |  |  |  |  | O |
| [ID4](#ID4) |  |  |  | O |  |  |  |  | O |
| [ID5](#ID5) |  |  |  |  |  |  |  |  | O |
| [ID6](#ID6) | O |  | O |  |  |  |  |  | O |
| [ID7](#ID7) | O |  |  |  |  |  |  |  | O |
| [ID8](#ID8) |  |  |  |  |  |  |  |  | O |
| [ID9](#ID9) |  |  |  |  |  | O |  |  |  |

# **Project Management**

## **Project Life Cycle**

Project will be developed in Unified Process model based on use cases. Unified Process is showing following steps.



Figure . UP overview[[1]](#footnote-1)

For each step out team will use following activities to be done.

Table . UP description

|  |  |
| --- | --- |
| Steps | Activity |
| Inception | Document, Initial use case model, Project glossary, Project plan |
| Elaboration | Use-case model, Analysis model, Architecture description, Design Model |
| Construction | Design model, Coding, Test cases |
| Transition | Deliver product, user feedback |

User in this process is Professor Kim and he will provide the feedback.

## **Development Method**

Table . Method for development activity

|  |  |
| --- | --- |
| Activity | Method |
| Communication | Physical meeting, Meeting log, Google drive |
| Requirement Model | Use case text, Use case diagram |
| Construction | Pair programming |
| Process | Unified Process |

## **Roles and Responsibility**

Table . Roles and Responsibility

|  |  |  |
| --- | --- | --- |
| Role | Responsibility | Staff Member |
| Project Manger | Mange the whole project | Yiru Jeon |
| Engineering Manager | Manage the engineering principles | Junwoo Park |
| Design Manager | Mange the design of product | Eojin Rho |

## **Risk management**

Table . Risk management

|  |  |  |
| --- | --- | --- |
| Risk | Probability | Solution |
| Lack of development time | Medium | Distribute the work for each team member |
| Low quality of product | Low | Focus on quality of product in every stage of development |
| Miss communication in team member | Medium | Frequent meeting and possible and firmed glossaries |

## **Staff member**

|  |  |  |  |
| --- | --- | --- | --- |
|  | | Profiles | |
| Name | Yiru Jeon | |  |
| Department | Computer Science | |
| Course | Master | |
| E-mail | podray777@gmail.com | |
|  | | | |
| Name | Junwoo Park | |  |
| Department | Computer Science | |
| Course | Undergraduate | |
| E-mail | junwoopark0130@gmail.com | |
|  | | | |
| Name | Eojin Rho | |  |
| Department | Computer Science | |
| Course | Undergraduate | |
| E-mail | [djwls9453@gmail.com](mailto:djwls9453@gmail.com) | |

## **Schedule**

|  |  |  |
| --- | --- | --- |
|  | Tasks | Due |
| 1st | Complete SRS | April 26, 2015 |
| 2nd | Complete analysis model | <TBD> |
| 3rd | Complete design model | <TBD> |
| 4th | Construction | <TBD> |
| 5th | Deployment | <TBD> |

# **Project Tools**

## **Development Environment**

|  |  |
| --- | --- |
| Operating System | Windows 8, 64bit |
| Language | Java |
|  | Eclipse |
| Java Version | Latest 1.7 |

## **Development Tools**

|  |  |
| --- | --- |
| Purpose | Tools |
| Writing documents | Microsoft Word 2010 |
| Writing meeting log | Google Document |
| Sharing data between teammates | Google Drive |
| Communication between teammates | KAIST Mail Service |
| Writing code | Eclipse |
| Draw use-case diagram | StarUML 5.0 |
| Server program | Apache HTTP Server Project |
| Code management | Git ([bitbucket.org/dustashes/cs350-safehome](http://www.bitbucket.org/dustashes/cs350-safehome)) |
| Repository location | TBD |

# **Appendix**.

## **Appendix A. List of Glossary**

* Arm/disarm a device: Arming (disarming) *SafeHome* activates (deactivates) a specific *SafeHome* device.
* Arm/disarm *SafeHome*: Arming (disarming) *SafeHome* activates (deactivates) entire sensors and cameras of *SafeHome*.
* Authentication: A process of identifying the homeowner; authentication uses password based system. Authentication is required in two different interfaces; control panel and webpage. Authentication in control panel requires 4-digit password. Authentication in webpage requires two passwords; each contains at least 8 characters.
* Camera: A device that records a video and transfers the video to *SafeHome* system; A camera does not act as a security sensor. It cannot report *SafeHome* that an intruder is inside contrary to motion detector, one of *SafeHome* sensors.
* Control panel: A hardware interface of *SafeHome* main device; control panel contains display, keypad, LEDs and speaker. LEDs represents status of *SafeHome* system. Speaker is used to generate emergency alarm sound.
* CPI corporation: A corporation that develops and manages *SafeHome* products and *SafeHome* system. The term represents Team #9.
* File system: A system storing video feeds data.
* Floor plan: A floor design stored in *SafeHome*. Floor plan is configured with *SafeHome* configuration functionalities. Floor plan contains a structure diagram for a home and information about *SafeHome* devices.
* Panic: An emergency situation when the homeowner faces direct threats; Silent alarming is required. Security company must notify the threats.
* *SafeHome* product/device: A device that is provided by CPI corporation; *SafeHome* devices have the same communication protocol with *SafeHome* system, so that they can communicate with each other.
* *SafeHome* system: A centralized, main device of *SafeHome* service; the device contains wireless communication module, display output interface, keypad input interface, and speaker. The device communicates *SafeHome* sensors and cameras with wireless communication module. The device interacts with a homeowner through display and keypad. When alarm is activated, the device generates alarm sound using speaker. The system runs a server application to provide Webpage interface to a homeowner.
* Security company: The term is used interchangeably with CPI corporation.
* Security zone: A group of *SafeHome* devices; devices are grouped into a security zone. Security zone provides convenience to the homeowner when *SafeHome* devices are configured.
* Sensor: A device that detects environment and generates output signal representing recognized environment.
* Web browser: An application for http webpages, for example, Internet explorer, Firefox, Chrome, Safari, and so on.
* Web interface: A homepage that is provided by a server application; the server application is executed in main device, e.g. Apache HTTP Server. A homeowner can connect to the webpage through Internet and manage his or her home. To prevent outsider attackers to corrupt *SafeHome* system, webpage contains ID/Password based authentication. The Webpage has a structure for mobile devices for the homeowner could use smartphone to access the home.
* Webpage: A webpage generated by a server application in *SafeHome* system. When the homeowner access the server, the server provides the webpage and the homeowner can interact with *SafeHome* system using the webpage.

## **Appendix B. List of Acronyms**

* SRS: Software Requirement Specification document
* UPS: Uninterruptible Power Supply
* UI: User Interface
* GUI: Graphical User Interface
* UCD: Use-case Diagrams
* UC: Use-case Scenarios
* ID: Interface Diagrams

## **Appendix C. Term Index**

Authentication 82

control panel 67

Control panel 14, 81

CPI corporation 14, 15, 81

File system 81

Floor plan 11, 81

Panic 51, 81

Security company 14, 15, 81, 82

*Security zone* *11*, *12*, 25, 39, 71, 75, 82

SRS 10, 82

thumbnail view 9, *12*

UPS 74, 82

Web browser 14, 67, 82

Webpage 15, 74, 82

## **Appendix D. Who-did-what List**

1. **Organizing documentation**

Organizing SRS Yiru Jeon

**Organizing Analysis model doc**. Junwoo Park

1. **Contents**

**List of Table** Junwoo Park

**List of Figures** Junwoo Park

**List of Swimlane diagrams** Junwoo Park

**List of Use-case diagrams** Junwoo Park

**List of Interface diagrams** Junwoo Park

**1.** **Introduction** Yiru Jeon

**1.1.** **Background**

**1.2.** ***SafeHome* Overview**

**1.3.** **Purpose and Structure**

**2.** **Overall Description** Yiru Jeon

**2.1.** **Functionalities and Future Plans**

**2.2.** **Product Perspective**

**2.3.** **User Class and Description**

**2.4.** **Operating Environment**

**2.5.** **Assumptions**

**3.** **System Features** See [Authorship of functional requirements](#authorship_f_req)

**3.1.** **SafeHome boot-up/shutdown service**

**3.2.** **Configuration Services**

**3.3.** **Real-time security service**

**3.4.** **User-requested information retrieval service**

**3.5.** **Authentication**

**3.6.** **External User Interface**

**3.6.1.** **Description**

**3.6.2.** **Web User Interface**

**3.6.3.** **Hardware User Interface**

**4.** **Non-functional Requirements**

**4.1.** **Performance Requirements** Yiru Jeon

**4.2.** **Safety Requirements** Yiru Jeon

**4.3.** **Security Requirements** Eojin Rho

**5.** **Traceability** Junwoo Park

**6.** **Project Management** Eojin Rho

**6.1.** **Project Life Cycle**

**6.2.** **Development Method**

**6.3.** **Roles and Responsibility**

**6.4.** **Risk management**

**6.5.** **Staff member**

**6.6.** **Schedule**

**7.** **Project Tools** Eojin Rho

**7.1.** **Development Environment**

**7.2.** **Development Tools**

**Appendix**.

**Appendix A. List of Glossary** Yiru Jeon

**Appendix B. List of Acronyms** Yiru Jeon

**Appendix C. Term Index** Yiru Jeon

**Appendix D. Who-did-what List** everyone

**Appendix E. References** Yiru Jeon

**Appendix F. Revision History** Junwoo Park

1. **Authorship of functional requirements**

# **List of Swimlane diagrams**

SL 1. Self-diagnosis : check whether connected sensors and cameras are okay Eojin Rho

SL 2. Initialize cameras Eojin Rho

SL 3. Finish cameras Eojin Rho

SL 4. Initialize sensors Eojin Rho

SL 5. Finish sensors Eojin Rho

SL 6. ControlPanelPassword Change Yiru Jeon

SL 7. WebpagePassword change Yiru Jeon

SL 8. Design floor plan Yiru Jeon

SL 9. Assign security zone Eojin Rho

SL 10. Backup plan for power off Yiru Jeon

SL 11. Factory reset Eojin Rho

SL 12. Manage logged-in devices Eojin Rho

SL 13. Firmware update Eojin Rho

SL 14. Arm system Eojin Rho

SL 15. Disarm system Eojin Rho

SL 16. Arm device Eojin Rho

SL 17. Disarm device Eojin Rho

SL 18. Display alarm Yiru Jeon

SL 19. Set travel mode Yiru Jeon

SL 20. View camera through floor plan window Eojin Rho

SL 21. View camera through thumbnail Eojin Rho

SL 22. Pan the camera Eojin Rho

SL 23. Zoom in/out a camera Yiru Jeon

SL 24. Panic Yiru Jeon

SL 25. Cancel task and return Eojin Rho

SL 26. Display status Yiru Jeon

SL 27. Pet angst sensor Yiru Jeon

SL 28. Finding ID Eojin Rho

SL 29. Finding password Eojin Rho

SL 30. Reporting system usage pattern Yiru Jeon

SL 31. Reporting web page access history Yiru Jeon

SL 32. Replay the record Yiru Jeon

SL 33. Authentication-control panel Yiru Jeon

SL 34. Authentication-web page Yiru Jeon

# **List of Use-cases**

UC 1. ControlPanelPassword change Yiru Jeon

UC 2. WebpagePassword change Yiru Jeon

UC 3. Design floor plan Yiru Jeon

UC 4. Assign security zone Yiru Jeon

UC 5. Backup plan for power off Yiru Jeon

UC 6. Factory reset Yiru Jeon

UC 7. Manage logged-in devices Yiru Jeon

UC 8. Firmware update Yiru Jeon

UC 9. Arm/disarm system Yiru Jeon

UC 10. Arm/disarm devices Yiru Jeon

UC 11. Display alarm Eojin Rho

UC 12. Set travel mode Yiru Jeon

UC 13. View camera through floor plan window Eojin Rho

UC 14. View camera through thumbnail Eojin Rho

UC 15. Pan the camera Eojin Rho

UC 16. Zoom in/out a camera Eojin Rho

UC 17. Panic Eojin Rho

UC 18. Cancel task and return Eojin Rho

UC 19. Display status Yiru Jeon

UC 20. Pet angst sensor Yiru Jeon

UC 21. Finding ID Eojin Rho

UC 22. Finding password Eojin Rho

UC 23. Reporting system usage pattern Yiru Jeon

UC 24. Reporting web page access history Yiru Jeon

UC 25. Replay the record Eojin Rho

UC 26 . Deny concurrent user accesses Eojin Rho

UC 27. Authentication-ControlPanel Yiru Jeon

UC 28. Authentication-Webpage Eojin Rho

# **List of Interface diagrams**

ID 1. Web interface - login page Junwoo Park

ID 2. Web interface - Accessing Security Function Junwoo Park

ID 3. Web interface - Main page with list of functions Junwoo Park

ID 4. Web interface - Security Control Panel Junwoo Park

ID 5. Web interface - viewing camera Junwoo Park

ID 6. Web interface - Single-camera view Junwoo Park

ID 7. Web interface - Thumbnail view Junwoo Park

ID 8. Web interface - Configuration menu Junwoo Park

ID 9. Control panel interface Junwoo Park

## **Appendix E. References**

* "Software Engineering: A Practitioner’s Approach (SEPA)" by R. S. Pressman, McGraw-Hill, 8th Edition
* StarUML5: <http://sourceforge.net/projects/staruml/>
* Apache HTTP Server Project: <http://httpd.apache.org/>
* Lecture Note chapter 4, UP diagram.

## **Appendix F. Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Authors | Date | Remarks |
| 1.0 | Junwoo Park  Eujin Rho  Yiru Jeon | 2015-04-26 | Initial software requirement specification |
| 2.0 | Junwoo Park  Eujin Rho  Yiru Jeon | 2015-05-06 | Initial Software Analysis Models |

1. From lecture note, chapter 4 [↑](#footnote-ref-1)