

---

# Software Requirement Specification For the SafeHome Product Software

---

***Prepared By***

*Team 3*

*Eut-deum Kim*

*Myung-kyung Lee*

*Ji-seong Gu*

*Da-bi Ahn*

***Issued at***

*2008. 4. 13.*

*Version 2.0.0*

This document is inspected and approved by persons who signed below. Therefore, this document will be used as the basis for later process. This document can't be modified or supplemented without approval signature.

**Signature :**

**Name :** Moon-zoo Kim

**Title :** Client

**Date :** 2008. 4. 13.

**Signature :**

**Name :** Eut-deum Kim

**Title :** Team Member

**Date :** 2008. 4. 13.

**Signature :**

**Name :** Myung-kyung Lee

**Title :** Team Member

**Date :** 2008. 4. 13.

**Signature :**

**Name :** Ji-seong Gu

**Title :** Team Member

**Date :** 2008. 4. 13.

**Signature :**

**Name :** Da-bi Ahn

**Title :** Team Member

**Date :** 2008. 4. 13.

**Signature :**

**Name :**

**Title :**

**Date :**

**Signature :**

**Name :**

**Title :**

**Date :**

## Document History

Issue	Date	Change Reason	Author
01	2008. 3. 8.	Building a rough draft Adding a meeting record	Team 3
02	2008. 3. 10.	Adding functions Adding a meeting record	Team 3
03	2008. 3. 13.	Adding functions Adding a meeting record	Team 3
04	2008. 3. 15.	Adding general description Adding a meeting record	Team 3
05	2008. 3. 17.	Changing essential structure Standardize words Adding a meeting record	Team 3
06	2008. 3. 19.	Changing essential structure Standardize words and sentences Adding a meeting record	Team 3
07	2008. 3. 20.	Changing functions Standardize words and sentences Adding glossary Adding a meeting record	Team 3
08	2008. 3. 21.	Changing functions Adding a meeting record Adding glossary Final review and modification	Team 3
09	2008. 3. 28.	Adding a link table Adding an index page	Team 3
10	2008. 4. 4.	Reconstruction Merge & delete some items	Team 3
11	2008. 4. 10.	Reconstruction Merge & delete some items	Team 3
12	2008. 4. 11.	Reconstruction Adding pictures	Team 3
13	2008. 4. 13.	Modifying an index page Final review and modification	Team 3

# TABLE OF CONTENT

<b>General Description .....</b>	<b>5</b>
1 Scope .....	5
2 Product Perspective .....	5
<b>Functional Requirements .....</b>	<b>6</b>
1 Security Functions .....	6
1.1 Arm/Disarm System/Sensor .....	6
1.1.1 Arm/Disarm System .....	6
1.1.2 Arm/Disarm Sensors .....	8
1.2 Alarm Condition Encounter .....	10
2 Surveillance Functions .....	12
2.1 Generate Video Output .....	12
2.1.1 Show Current Video .....	12
2.1.2 Show Recorded Video .....	15
2.2 Camera Password Management .....	17
<b>Non-functional Requirements .....</b>	<b>19</b>
3 Administration Functions .....	19
3.1 Internet Login ID/Permission Management .....	19
3.2 Sensor Threshold Management .....	21
3.3 Floor Plan Management .....	23
4 Other Functions .....	26
4.1 Installation .....	26
4.2 Internet Login ID/Password Validation .....	26
4.3 Internet Login Password Management .....	28
<b>Appendix .....</b>	<b>31</b>
A Link Table .....	31
B Glossary .....	33
C Word Index .....	35
D Picture & Table Index .....	36
E Meeting Records .....	37
F Who-did-what list .....	53

# General Descriptions

## 1 Scope

This document describes the requirement specification and constraints in the SafeHome Product software.

## 2 Product Perspective

- SafeHome hardware structure is consist of the control panel, home-based PC, CPI server. The control panel is an interface, PC takes charge of external access & storing data and CPI server provides web service.
- The homeowner can secure his/her house with the SafeHome Product more conveniently. The SafeHome Product provides the security functions and surveillance functions.
- The homeowner can set the security mode via control panel and internet. The system dials phone calls to the homeowner and the SafeHome service team when the sensors detect abnormality.
- The homeowner can view surveillance images of the house via internet.
- To access to the SafeHome software installed on PC, the homeowner must use web browser program even if the homeowner is at his/her home. External direct connection to the control panel, sensors, cameras are not allowed because there can be security troubles
- All transmissions between PC and sensors, PC and CPI server are done with encrypted data.
- All transmissions between PC and sensors are done via wireless connection(802.11b).

# Functional Requirements

## 1 Security Functions

### 1.1 Arm/Disarm System/Sensor

#### 1.1.1 Arm/Disarm System

##### 1.1.1.1 Description

This requirement document describes the scenario, requirements and constraints when the homeowner wants to activate some sensors, to deactivate sensors, or to test if all sensors are working correctly. But we don't care about how the system tests each sensor. The homeowner can do these via internet or via control panel of the house.

##### 1.1.1.2 Scenario

**\* If the homeowner or the guest uses the control panel directly, the scenario starts at 10.**

1. The homeowner or the guest enters the SafeHome Product Web site.
2. The system displays input boxes to receive internet login ID and passwords of the web site.
3. The homeowner or the guest inputs his/her internet login ID and two passwords.
4. The system verifies ID and the passwords and loads the level data of inputted ID.
5. The system is changed to log on mode and displays major functions of SafeHome Product.
6. The homeowner or the guest selects "Security" from menu.
7. The system displays the sub menu.



**Figure 1-1.**  
The sub menu of  
Security Function

8. The homeowner or the guest selects "Arm/Disarm System" from sub

menu.

9. The system displays the picture of the control panel.



Figure 1-2.  
Control Panel

10. The homeowner or the guest enters his/her password.

**A. When the homeowner or the guest arms the system**

11. The homeowner or the guest pushes 'away' button.
12. The system activates all sensors after tolerance time.

**B. When the homeowner or the guest disarms the system**

11. The homeowner or the guest pushes 'stay' button.
12. The system activates perimeter sensors. Motion detecting sensors are not activated.

**C. When the homeowner or the guest turns off the system**

11. The homeowner or the guest pushes 'off' button.
12. The system deactivates all sensors.

**D. When the homeowner tests the sensors**

11. The homeowner or the guest pushes 'test' button.
12. If all sensors are working correctly, the system displays an 'OK' sign.

**E. When the homeowner modify the master password**

11. The homeowner pushes 'code' button.
12. The homeowner inputs a current master password.
13. The homeowner inputs a new master password.
14. The homeowner inputs the password again.
15. The system stores the password.

**F. When the homeowner adds a new secondary password**

11. The homeowner pushes 'bypass' button,
12. The homeowner inputs a new secondary password.
13. The homeowner inputs the password again.
14. The system stores the password.

#### ***1.1.1.3 Qualification Provision***

- The homeowner or the guest must have the appropriate permission if using this function via internet.
- The system must be fully configured.
- The system must be "ready state". It means 'all doors and windows are closed.

#### ***1.1.1.4 Priority***

Highest

#### ***1.1.1.5 Special Requirements***

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"

#### ***1.1.1.6 Constraints***

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- The tolerance time in A.12 is defined in "Sensor Threshold Management" part.
- The control panel password must be 4-digit number.

#### ***1.1.1.7 Exceptions***

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- If any errors are detected in D, the system beeps and displays the ID of erroneous sensor.
- If he/she inputs incorrect control panel password twice, the system beeps three times and does not accept user's input for 5 minutes.
- If the system encounters an alarm condition, all arm/disarm functions does not work until an alarm condition is destroyed or the homeowner calls off an alarm by setting "off" mode.

### **1.1.2 Arm/Disarm Sensors**

#### ***1.1.2.1 Description***

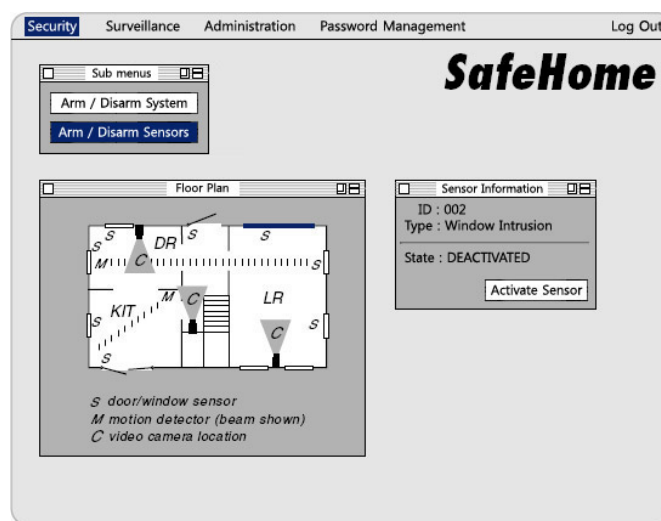
This requirement document describes the scenario, requirements and constraints when the homeowner wants to activate/deactivate sensors via internet.

#### ***1.1.2.2 Scenario***

1. The homeowner or the guest enters the SafeHome Product Web site.
2. The system displays input boxes to receive internet login ID and passwords of the web site.
3. The homeowner or the guest inputs his/her internet login ID and two passwords.



4. The system verifies ID and the passwords and loads the level data of inputted ID.
5. The system is changed to log on mode and displays major functions of SafeHome Product.
6. The homeowner or the guest selects "Security" from menu.
7. The system displays the sub menu.
8. The homeowner or the guest selects "Arm/Disarm Sensors" from sub menu.
9. The system displays a floor plan of the house.
10. The homeowner selects a sensor icon from the floor plan.
11. The system displays the status of the sensor - "Activated" or "Deactivated" or "Alarm" and menu - "Activate sensor", "Deactivate sensor".



**Figure 1-3.**  
Selecting a sensor  
from the floor plan

#### **A. When the homeowner activates sensor**

12. The homeowner selects "Activate sensor" button.
13. The system activates selected sensor of the house.
14. The system changes the status of selected sensor to "Activated".
15. The system displays "Sensor is activated." message box.

#### **B. When the homeowner deactivates sensor**

12. The homeowner selects "Deactivate sensor" button.
13. The system deactivates selected sensor of the house.
14. The system changes the status of selected sensor to "Deactivated".
15. The system displays "Sensor is deactivated." message box.

### **1.1.2.3 Qualification Provision**

- The homeowner or the guest must have the appropriate permission.
- The system must be fully configured.

### **1.1.2.4 Priority**

Medium priority, to be implemented after basic functions.

### 1.1.2.5 Special Requirements

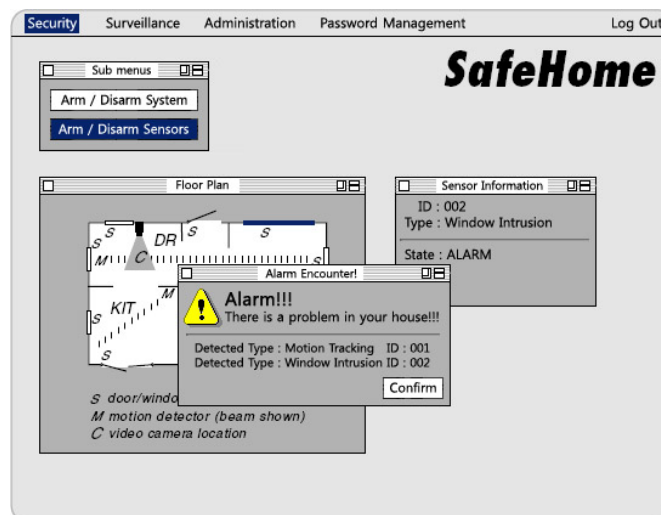
- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"

### 1.1.2.6 Constraints

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"

### 1.1.2.7 Exceptions

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- If the system encounters an alarm condition, all arm/disarm functions does not work until an alarm condition is destroyed or the homeowner calls off an alarm by setting "off" mode.



**Figure 1-4.**  
Alarm condition  
encounter on the  
security functions

## 1.2 Alarm Condition Encounter

### 1.2.1 Description

This requirement document describes the scenario, requirements and constraints when a sensor event is occurred. The system serves a notice to homeowner and service center.

### 1.2.2 Scenario

1. The system recognizes an alarm event from sensors.
2. The system calls to monitoring service and provides informations about the location of the house and what has been detected after tolerance time.
3. The system reports what happened to homeowner via control panel, PC, web browser, and telephone. It displays the message box which contains prompting messages and system status information.

### 1.2.3 Qualification Provision

- The system must be fully configured.

#### ***1.2.4 Priority***

Highest

#### ***1.2.5 Special requirements***

None

#### ***1.2.6 Constraints***

None

#### ***1.2.7 Exceptions***

- If the call is failed, the system dials again after 20 seconds.

## 2 Surveillance Functions

### 2.1 Generate Video Output

#### 2.1.1 Show Current Video

##### 2.1.1.1 Description

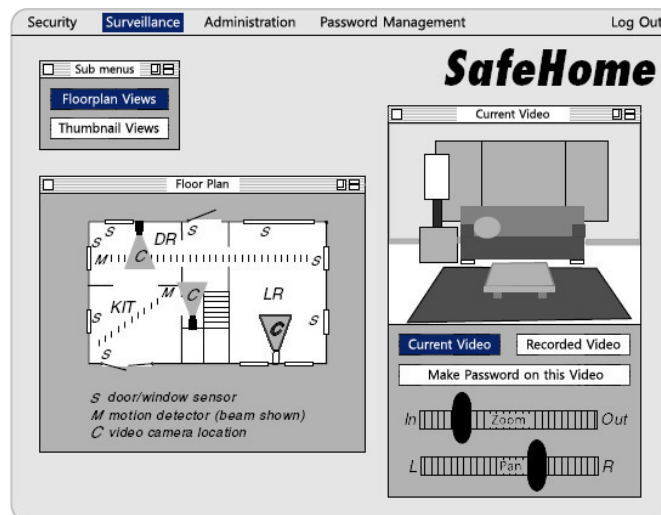
This requirement document describes the scenario, requirements and constraints when the homeowner or the guest view current output of camera placed throughout the house from any remote location via the Internet for surveillance.

##### 2.1.1.2 Scenario

1. The homeowner or the guest enters the SafeHome Product Web site.
2. The system displays input boxes to receive internet login ID and passwords of the web site.
3. The homeowner or the guest inputs his/her internet login ID and two passwords.
4. The system verifies ID and the passwords and loads the level data of inputted ID.
5. The system is changed to log on mode and displays major functions of SafeHome Product.
6. The homeowner or the guest selects "Surveillance" from menu.
7. The system displays the sub menu and the floor plan of the house.

##### A. When the homeowner uses the floor plan to select a camera

8. The homeowner or the guest selects a camera icon from the floor plan.
9. The system displays current video at one frame per second and zoom scroll bar and pan scroll bar in the bottom of window.

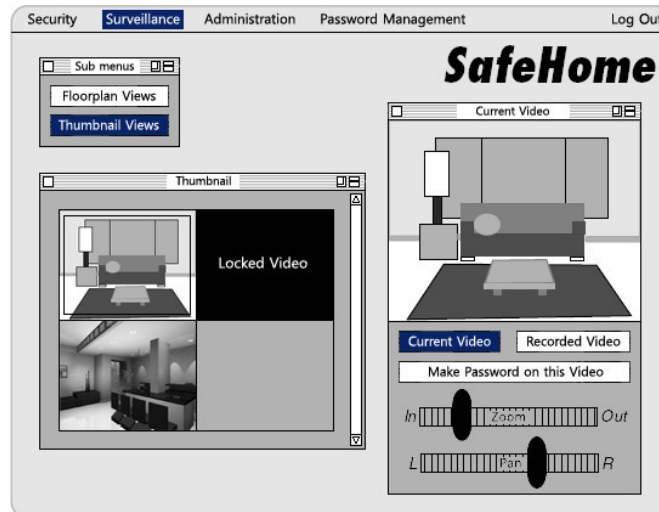


**Figure 2-1.**  
Selecting a video  
from the floor plan

##### B. When the homeowner uses the thumbnail to select a camera

8. The homeowner or the guest selects "Thumbnail views" from sub menu.
9. The system displays thumbnail of videos.
10. The homeowner or the guest selects an image to view.
11. The system displays current video at one frame per second and zoom

scroll bar and pan scroll bar in the bottom of window.



**Figure 2-2.**  
Selecting a video  
from the thumbnail

### **2.1.1.3 Qualification Provision**

- The homeowner or the guest must have the appropriate permission.
- Cameras must be fully configured.
- Cameras must be well-positioned to pan in all of range without any interruption.

### **2.1.1.4 Priority**

High

### **2.1.1.5 Special Requirements**

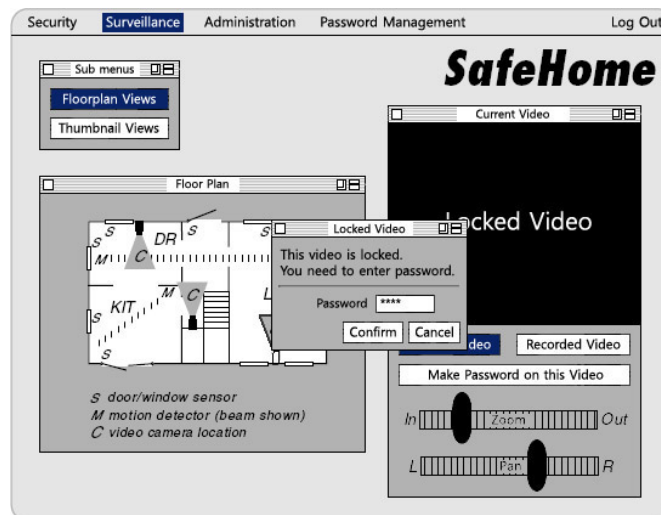
- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- The person that has administrator permission can watch videos without any camera passwords.

### **2.1.1.6 Constraints**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"

### **2.1.1.7 Exceptions**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- If the guest selects any locked video, the system displays a password input window and guest can see video only if he/she enters correct camera password. if not, the system shows only black screen.

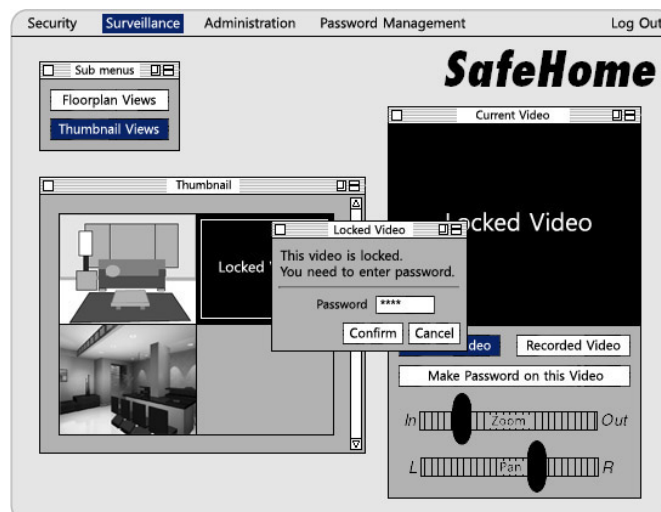


**Figure 2-3.**  
Selecting a locked video



**Figure 2-4.**  
The camera password is incorrect

- If there is any locked video, the system displays "locked video" thumbnail image.



**Figure 2-5.**  
Selecting a locked video from the thumbnail

- If the system encounters an alarm condition, the system displays a message box that contains an alarm message and why the alarm is activated.



**Figure 2-6.**  
Alarm condition  
encounter on the  
surveillance  
functions

## 2.1.2 Show Recorded Video

### 2.1.2.1 Description

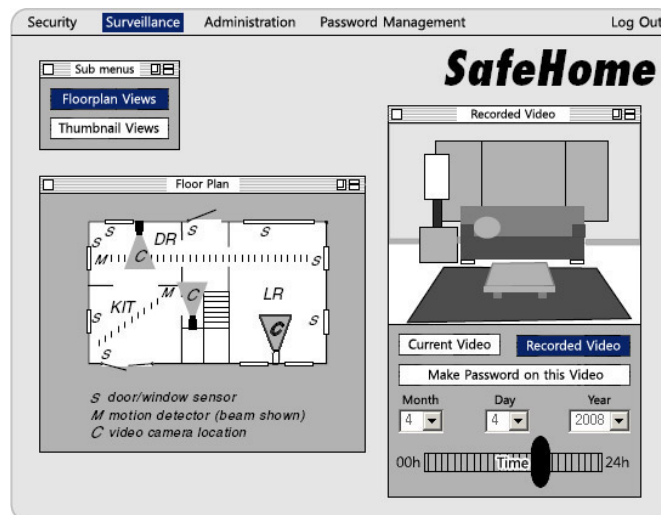
This requirement document describes the scenario, requirements and constraints when the homeowner or the guest view recorded output of camera placed throughout the house from any remote location via the Internet for surveillance.

### 2.1.2.2 Scenario

1. The homeowner or the guest enters the SafeHome Product Web site.
2. The system displays input boxes to receive internet login ID and passwords of the web site.
3. The homeowner or the guest inputs his/her internet login ID and two passwords.
4. The system verifies ID and the passwords and loads the level data of inputted ID.
5. The system is changed to log on mode and displays major functions of SafeHome Product.
6. The homeowner or the guest selects "Surveillance" from menu.
7. The system displays the sub menu and the floor plan of the house.

#### **A. When the homeowner uses the floor plan to select camera**

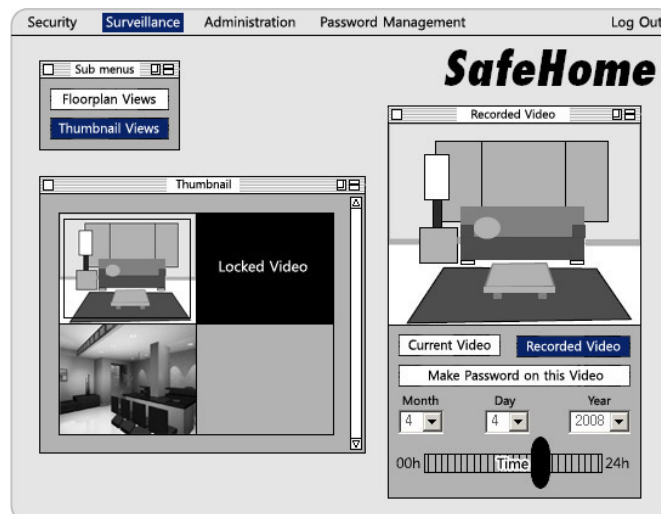
8. The homeowner or the guest selects a camera icon from the floor plan.
9. The system displays current video.
10. The homeowner or the guest selects "Recorded Video" button.
11. The system displays recorded video at one frame per second and Month-Day-Year button and time slide.



**Figure 2-7.**  
Selecting a recorded video from the floor plan

#### **B. When the homeowner uses the thumbnail to select camera**

8. The homeowner or the guest selects "Thumbnail views" from sub menu.
9. The system displays thumbnail of videos.
10. The homeowner or the guest selects an image to view.
11. The system displays current video.
12. The homeowner or the guest selects "Recorded Video" button.
13. The system displays recorded video at one frame per second and Month-Day-Year button and time slide.



**Figure 2-8.**  
Selecting a recorded video from the thumbnail

#### **2.1.2.3 Qualification Provision**

- The homeowner or the guest must have the appropriate permission.
- Cameras must be fully configured.

#### **2.1.2.4 Priority**

Moderate

#### **2.1.2.5 Special Requirements**

- Including the internet ID/passwords validation - See "4.2 Internet Login



ID/Passwords Validation"

- The person that has administrator permission can watch videos without any camera passwords.
- The recorded video data is stored for 30 days.

#### **2.1.2.6 Constraints**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"

#### **2.1.2.7 Exceptions**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- If the guest selects any locked video, the system displays a camera password input window and guest can see video only if he/she enters correct camera password. if not, the system shows only black screen.
- If there is any locked video, the system displays "locked video" thumbnail image.
- If there is no recorded video, the system displays "Data not found" image on the video screen.
- If the system encounters an alarm condition, the system displays a message box that contains an alarm message and why the alarm is activated.

## **2.2 Camera Password Management**

### **2.2.1 Description**

This requirement document describes the scenario, requirements and constraints when the homeowner sets/modifies/deletes the password to each cameras.

### **2.2.2 Scenario**

**\* After selecting a specific camera**

#### **A. When the homeowner locks video or modify a password**

1. The homeowner selects "Make Password on this Video" button.
2. The system displays a window consist of two input boxes.
3. The homeowner inputs same passwords into two input box and selects "Confirm" button.



**Figure 2-9.**  
Locking/modifying/  
deleting a camera  
password

#### **B. When the homeowner deletes a password**

1. The homeowner selects "Make Password on this Video" button.
2. The system displays a window consist of two input boxes.
3. The homeowner selects "Delete Password" button.

### **2.2.3 Qualification Provision**

- The homeowner has the administration permission.

### **2.2.4 Priority**

Low

### **2.2.5 Special Requirements**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"

### **2.2.6 Constraints**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- The camera password must be 4-digit number or characters.

### **2.2.7 Exceptions**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- If the homeowner inputs different passwords at A.3, the system displays an alert message box and blank input boxes to input passwords again.
- If the system encounters an alarm condition, the system displays a message box that contains an alarm message and why the alarm is activated.

# Non-functional Requirements

## 3 Administration Functions

### 3.1 Internet Login ID/Permission Management

#### ***3.1.1 Description***

This requirement document describes the scenario, requirements and constraints when the administrator registers new IDs or changes other ID's permission to access SafeHome Product Website's functionality.

#### ***3.1.2 Scenario***

1. The administrator enters the SafeHome Product Web site.
2. The system displays input boxes to receive internet login ID and passwords of the web site.
3. The administrator inputs his/her internet login ID and two passwords.
4. The system verifies ID and the passwords and loads the level data of inputted ID.
5. The system is changed to log on mode and displays major functions of SafeHome Product.
6. The administrator selects "Administration" from menu.
7. The system displays the sub menu.
8. The administrator selects "ID/Permission Management" from sub menu.
9. The system displays IDs which is registered to the system and check boxes.

#### **A. When the administrator registers a new secondary ID**

10. The administrator selects "New ID Registration" buttons.
11. The system displays input boxes to receive ID and passwords of the new secondary ID.
12. The administrator inputs a new ID and two passwords and selects "Confirm" button.
13. The system stores the new ID's data and refreshes the ID list of 9.



**Figure 3-1.**  
Registration of a  
new secondary ID

**B. When the administrator changes other ID's permission.**

10. The administrator changes other ID's permission using the check boxes and selects "Confirm" button.
11. The system stores the permission data.



**Figure 3-2.**  
Changing ID's  
permission

**C. When the administrator delete existing ID**

10. The administrator selects "X" buttons exists by each of IDs.
11. The system displays confirming window.
12. The administrator selects "Confirm" button.
13. The system deletes the ID's data and refreshes the ID list of 9.



**Figure 3-3.**  
ID deletion  
confirming window

### **3.1.3 Qualification Provision**

- The homeowner must have the administration permission.

### **3.1.4 Priority**

Low

### **3.1.5 Special Requirements**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"

### **3.1.6 Constraints**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- Duplicated the internet login ID is not permitted by the system.
- There is only one administrator ID - made by the homeowner at SafeHome Product software installation. The administrator ID's permission cannot be changed and administrator ID cannot be deleted.

### **3.1.7 Exceptions**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- If the system encounters an alarm condition, the system displays a message box that contains an alarm message and why the alarm is activated.

## **3.2 Sensor Threshold Management**

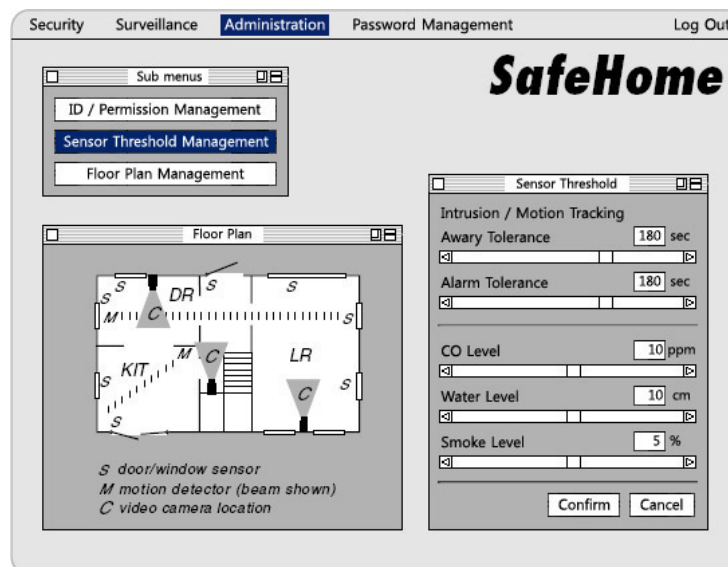
### **3.2.1 Description**

This requirement document describes the scenario, requirements and constraints when administrator sets tolerance time from perceiving intrusion state to alarm

state(alarm) or from pushing armed button to armed state(away) or sets up CO, smoke, and water level sensor's threshold.

### 3.2.2 Scenario

1. The administrator enters the SafeHome Product Web site.
2. The system displays input boxes to receive internet login ID and passwords of the web site.
3. The administrator inputs his/her internet login ID and two passwords.
4. The system verifies ID and the passwords and loads the level data of inputted ID.
5. The system is changed to log on mode and displays major functions of SafeHome Product.
6. The administrator selects "Administration" from menu.
7. The system displays the sub menu.
8. The administrator selects "Sensor Threshold" menu.
9. The system displays floor plans and threshold control slide bars.



**Figure 3-4.**  
Changing the  
sensor threshold  
values

10. The administrator controls threshold of each sensor with its own control slide bar and selects "Confirm" button.
11. The system stores the sensor threshold values.

### 3.2.3 Qualification Provision

- The homeowner must have the administration permission.
- The system must be fully configured.

### 3.2.4 Priority

Low

### 3.2.5 Special Requirements

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- Window, door and motion tracking sensors have two control bar "Away" and "Alarm". Tolerance time from perceiving intrusion state is alarm and that from pushing armed

- button to be armed state is away. The initial values of these are 180 seconds.
- The system displays encouraging level of each CO, Water level, smoke sensor.
- The initial level of each sensors is the encouraging level.

### **3.2.6 Constraints**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- Tolerance time for alarming should be more than 10 seconds, less than 5 minutes.
- There should be low upper bound to the control bar to guarantee safety.

### **3.2.7 Exceptions**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- If the system encounters an alarm condition, the function is canceled and the system displays a message box that contains an alarm message and why the alarm is activated.

## **3.3 Floor Plan Management**

### **3.3.1 Description**

This requirement document describes the scenario, requirements and constraints when the administrator or the engineer sets up an appropriate floor plan and settings for cameras and sensors via Internet to use whole sensors and cameras.

### **3.3.2 Scenario**

1. The administrator enters the SafeHome Product Web site.
2. The system displays input boxes to receive internet login ID and passwords of the web site.
3. The administrator inputs his/her internet login ID and two passwords.
4. The system verifies ID and the passwords and loads the level data of inputted ID.
5. The system is changed to log on mode and displays major functions of SafeHome Product.
6. The administrator selects "Administration" from menu.
7. The system displays the sub menu.
8. The administrator selects "Floor Plan Management" from sub menu.
9. The system displays the sub-sub menu.

#### **A. When the administrator draws a new floor plan**

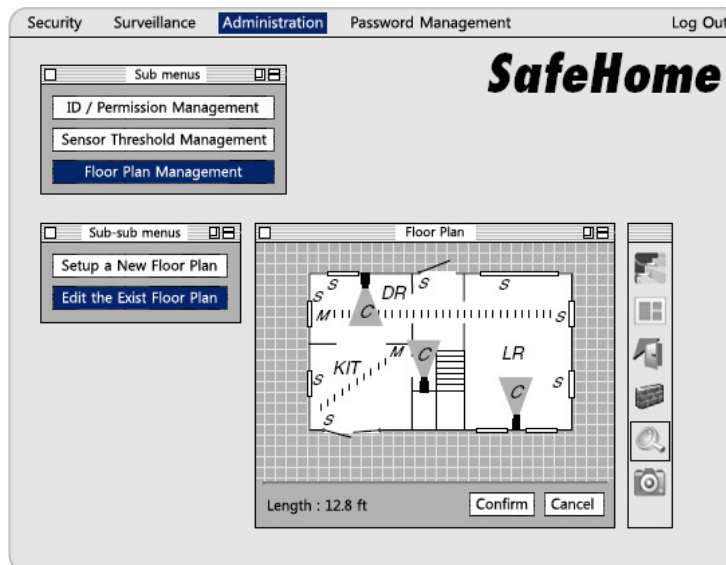
10. The administrator selects "Setup a New Floor Plan" from sub-sub menu.
11. The system displays grid, icons which stand for walls, doors, and windows, and libraries of sensors and cameras.
12. The administrator draws a floor plan on the grid using appropriate icons and libraries.
13. The system stores the floor plan data.



**Figure 3-5.**  
Drawing a new  
floor plan

**B. When the administrator edits the existing floor plan.**

10. The administrator selects "Edit the Existing Set-up" from sub-sub menu.
11. The system displays pre-defined floor plans with grid, icons, and libraries.
12. The administrator changes the floor plan, and selects "Confirm" button (moving sensors or cameras, adding new ones, deleting existing ones, editing setting for cameras and sensors, or editing the floor plan).
13. The system stores the floor plan data.



**Figure 3-6.**  
Editing the existing  
floor plan

### 3.3.3 Qualification Provision

- The homeowner must have the administration permission.
- All sensors and cameras can be represented by the library of sensors and cameras.

### 3.3.4 Priority

Moderate

### 3.3.5 Special Requirements



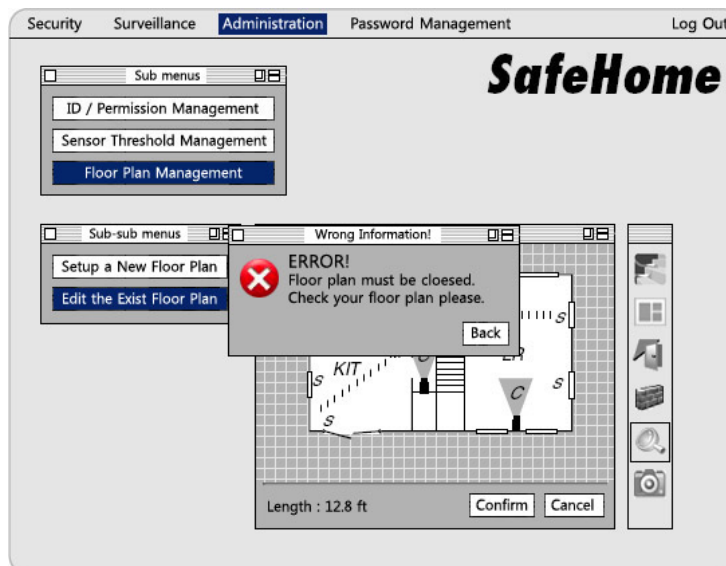
- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- If user stretches the icons, it should extend. And if user shrinks the icons, it should shrink.
- The system shows the length with selective measurement system(feet or inches).
- All cameras or sensors should be labeled by system automatically.

### 3.3.6 Constraints

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"

### 3.3.7 Exceptions

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- If the system encounters an alarm condition, the function is canceled and the system displays a message box that contains an alarm message and why the alarm is activated.
- If the floor plan isn't closed, the system displays "The floor plan must be closed" message box.



**Figure 3-7.**  
None-closed floor  
plan error

## 4 The Other Functions

### 4.1 Installation

#### 4.1.1 Description

This requirement document describes the counter scenario, requirements and constraints when the homeowner installs the SafeHome Product software on the home-based PC for the first time.

#### 4.1.2 Scenario

1. The homeowner executes the SafeHome Product software installation file on the home-based PC.
2. Installation the software searches for the SafeHome Product component - wireless box - and an internet connection.
3. Installation the software receives the homeowner's name, master password to access the control panel, ID and two passwords to log on the SafeHome Product Web site, the phone numbers of the homeowner and the SafeHome Product service team.
4. Installation the software starts to install.

#### 4.1.3 Qualification Provision

- There is the SafeHome Product wireless box and the home-based PC.
- There is an internet connection between the home-based PC and the CPI server.

#### 4.1.4 Priority

Low, but must be implemented.

#### 4.1.5 Special Requirements

- The software must be able to detect if this PC is the home-based PC and there is the wireless box and internet connection.

#### 4.1.6 Constraints

- The SafeHome Product software must be installed on the home-based PC, the component of the SafeHome Product.

#### 4.1.7 Exceptions

- If there is no SafeHome Product wireless box, the installation software displays "Can't detect wireless box component." message box and terminated.
- If PC is not the home-based PC, the installation software displays "PC is not appropriate to install the SafeHome Product software." message box and terminated.
- If there is no internet connection, the installation software displays "Internet connection is needed to install the SafeHome Product software." message box and terminated.

### 4.2 Internet Login ID/Passwords Validation

#### 4.2.1 Description

This requirement document describes the scenario, requirements and constraints when

the homeowner logs in the SafeHome Product Web site with his/her internet login ID and passwords.

#### **4.2.2 Scenario**

1. The homeowner or the guest enters the SafeHome Product Web site.
2. The system displays input boxes to receive internet login ID and passwords of the web site.

The screenshot shows a web browser window with a navigation bar at the top containing links: Security, Surveillance, Administration, Password Management, and Log Out. The main heading is 'SafeHome'. In the center, there is a 'Login Please' dialog box. This dialog box contains three input fields: 'Your ID' with the text 'SafeHomeID', 'Your Password 1' with masked characters '\*\*\*\*\*', and 'Your Password 2' with masked characters '\*\*\*\*\*'. A 'Login' button is located at the bottom right of the dialog box. Below the dialog box, there is a message: 'If you forget your administrator ID or passwords, Please contact with SafeHome Service Team abcdefg@SafeHome.com, TEL 012-345-678-9110'.

**Figure 4-1.**  
Internet login  
ID/password  
validation

3. The homeowner or the guest inputs his/her internet login ID and two passwords.
4. The system verifies ID and the passwords and loads the level data of inputted ID.
5. The system is changed to log on mode and displays major functions of SafeHome Product.

#### **4.2.3 Qualification Provision**

None

#### **4.2.4 Priority**

Moderate

#### **4.2.5 Special Requirements**

- Depending on the level of ID, the system displays the usable major functions selectively.
- If the homeowner or the guest logs in and doesn't do any action for 10 minutes, the system regards that the homeowner logs out and changes state.
- When the homeowner or the guest inputs the internet login passwords, the system displays "\*" characters matching each input.
- The system should distinguish the internet login password by uppercase or lowercase.

#### **4.2.6 Constraints**

- The internet login password should be at least eight characters to sixteen characters at maximum in length.

#### 4.2.7 Exceptions

- If the internet login ID or password is incorrect, the system displays "Wrong ID or password" message box.



**Figure 4-2.**  
Internet login  
ID/password  
validation error

### 4.3 Internet Login Password Management

#### 4.3.1 Description

This requirement document describes the scenario, requirements and constraints when the homeowner or the guest wants to change his/her own internet login passwords.

#### 4.3.2 Scenario

1. The homeowner or the guest enters the SafeHome Product Web site.
2. The system displays input boxes to receive internet login ID and passwords of the web site.
3. The homeowner or the guest inputs his/her internet login ID and two passwords.
4. The system verifies ID and the passwords and loads the level data of inputted ID.
5. The system is changed to log on mode and displays major functions of SafeHome Product.
6. The homeowner or the guest selects "Password Management" from menu.
7. The system displays input boxes to receive current internet login passwords, new internet login passwords, confirming passwords.
8. The homeowner or the guest inputs his/her current internet login passwords, new internet login passwords, confirming passwords and selects "Confirm" button.
9. The system stores the new internet login passwords.



**Figure 4-3.**  
Internet login  
password  
management

### **4.3.3 Qualification Provision**

None

### **4.3.4 Priority**

Low

### **4.3.5 Special Requirements**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"

### **4.2.6 Constraints**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"

### **4.2.7 Exceptions**

- Including the internet ID/passwords validation - See "4.2 Internet Login ID/Passwords Validation"
- If current passwords are incorrect or new passwords and confirming passwords are not same each, the system displays "Wrong passwords or incorrect confirming passwords" message box and go back to login display.



**Figure 4-4.**  
Internet login  
password  
management error

- If the system encounters an alarm condition, the system displays a message box that contains an alarm message and why the alarm is activated.

# APPENDIX

## A. Link Table

Function Name	Source Module Name	Description	Target Module Name	Internet Login Password									
				4:3:7:2: If current passwords are not	4:2:7:1: If the internet login ID or password	4:2:6:1: The internet login password	4:2:5:3: When the homeowner or the	4:2:5:1: Depending on the level of 1	4:2:2:1: The homeowner or the queue	3:3:7:3: If the floor plan isn't closed	3:2:2:1: The administrator enters the	2:2:7:2: If the homeowner inputs different	2:1:2:7:4: If there is no recorded video
Security Functions	Arm/Disarm System	1.1.1.2.*. If the homeowner or the	Arm/Disarm System										
		1.1.1.2.1. The homeowner or the g											
		1.1.1.2.10. The homeowner or the											
		1.1.1.2.D12. If all sensors are work											
		1.1.1.5.1. Including the internet ID/											
		1.1.1.6.1. Including the internet ID/											
	Arm/Disarm Sensor	1.1.1.6.2. The tolerance time in A.1											
		1.1.1.7.1. Including the internet ID/											
		1.1.1.7.4. If the system encounters											
	Alarm Condition Encounter	1.1.2.2.1. The homeowner or the g	Alarm Condition										
		1.1.2.5.1. Including the internet ID/											
		1.1.2.6.1. Including the internet ID/											
Surveillance Functions	Show Current Video	1.1.2.7.1. Including the internet ID/	Show Current Video										
		1.1.2.7.2. If the system encounters											
		1.2.2.2. The system calls to monito											
		1.2.2.3. The system reports what h											
		2.1.1.2.1. The homeowner or the g											
		2.1.1.2.A9. The system displays cu											
	Show Recorded Video	2.1.1.2.B9. The system displays th	Show Recorded Video										
		2.1.1.2.B11. The system displays c											
		2.1.1.5.1. Including the internet ID/											
		2.1.1.6.1. Including the internet ID/											
		2.1.1.7.1. Including the internet ID/											
		2.1.1.7.4. If the system encounters											

Function Name	Source Module Name	Description	Target Module Name
Surveillance Functions	Show Recorded Video	2.1.2.2.B9. The system displays th	
		2.1.2.2.B11. The system displays c	
		2.1.2.2.B13. The system displays r	
		2.1.2.5.1. Including the internet ID/	
		2.1.2.6.1. Including the internet ID/	
		2.1.2.7.1. Including the internet ID/	
	Camera Password Management	2.1.2.7.5. If the system encounters	
		2.2.2.*. After selecting a specific c	
		2.2.2.A3. The homeowner inputs s	
		2.2.5.1. Including the internet ID/p	
Administration Functions	Internet Login ID/Permission Management	2.2.6.1. Including the internet ID/p	
		2.2.7.1. Including the internet ID/p	
		2.2.7.3. If the system encounters a	
		3.1.2.1. The administrator enters th	
	Sensor Threshold Management	3.1.5.1. Including the internet ID/p	
		3.1.6.1. Including the internet ID/p	
		3.1.7.1. Including the internet ID/p	
		3.1.7.2. If the system encounters a	
	Floor Plan Management	3.2.2.1. The administrator enters th	
		3.2.5.1. Including the internet ID/p	
		3.2.6.1. Including the internet ID/p	
		3.2.7.1. Including the internet ID/p	
The Other Functions	Internet Login ID/Passwords Validation	3.2.7.2. If the system encounters a	
		3.3.2.1. The administrator enters th	
		3.3.2.A12. The administrator draws	
	Internet Login Password Management	3.3.2.B12. The administrator chang	
		3.3.5.1. Including the internet ID/p	
		3.3.6.1. Including the internet ID/p	
		3.3.7.1. Including the internet ID/p	
		3.3.7.2. If the system encounters a	



## B. Glossary

### **SafeHome Product**

The product that consists of the SafeHome Product software, home-based PC, control panel, wireless box, sensors, cameras, accessibility to CPI servers and service team.

### **SafeHome Product software**

The software that manages storing data, sensor and camera setting and external access.

### **SafeHome Product service team, service team**

The division of the SafeHome company that provides the password-missing case disposal service, the sensor-detection disposal service and so on.

### **SafeHome Product Web site**

The web site that operates SafeHome Products.

### **administration**

The permission level that allows user to use all functions of the SafeHome Product software.

### **administrator**

The user who has the administration permission.

### **camera**

A optical device that records video data.

### **control panel**

The interface located in the house of the homeowner and providing security mode changing functions.

### **CPI server**

The server computer located in the SafeHome company and providing the web service.

### **guest**

A person who doesn't have the administrator permission or isn't the homeowner.

### **home-based PC or PC**

The computer located in the house of the homeowner, storing all data except web data and providing exceptional access gate.

### **homeowner**

The user who has the house and purchases the SafeHome Product.

### **input box**

A blank form that the system displays to receive data from the homeowner or guest.

### **internet login ID/password**

A ID and passwords that needs to log in to SafeHome Web site.

### **master password**

A password that needs to operate the control panel. Master password owner can make/delete secondary passwords.

### **message box**

A box form that the system displays to inform the homeowner or the guest.

### **permission**

The authority that needs to use some functions.

**priority**

The order that how much the user want to use.

**secondary password**

A password that needs to operate the control panel. Secondary password owner can not make/delete another secondary passwords.

**sensor**

A device that detects specified objects.

**thumbnail**

Snapshots provided by the SafeHome Product software to let users know the content of the video file.

**threshold**

A bounded value that doesn't make sensors to respond.

**tolerance time**

The time that the system waits after the first sensor response. After tolerance time, if there is the sensor reponse yet, the system makes phone call to SafeHome Product service team.

**validation**

The process that the system verifies a internet login ID and passwords, changes user state to log-in state and gives appropriate permission.

**wireless box**

The device located in the house of the homeowner and providing wireless transmission among the home-based PC, control panel, cameras and sensors.

## C. Word Index

### A

Administration, 19  
alarm, 10  
Arm/Disarm, 6  
away mode, 7

### B

bypass mode, 7

### C

code mode, 7  
control panel, 5, 7  
CPI server, 5

### E

encrypt, 5

### F

floor plan, 12, 23  
frame per second, 16

### G

grid, 23

### H

home-based PC, 5, 26

### I

installation, 26  
internet login ID, 19, 26  
internet login password, 28

### L

library, 23  
log on/out, 27

### M

master password, 7

### O

off mode, 7

### P

PCI server, 26  
permission, 19

### R

ready state, 8

### S

secondary password, 7  
sensor, 8  
stay mode, 7  
surveillance, 12  
System, 6

### T

test mode, 7  
threshold, 21  
thumbnail, 12

### V

validation, 26  
video, 12

### W

wireless connection, 5

## D. Picture & Table Index

<b>Figure 1-1.</b> The sub menu of Security Function .....	6
<b>Figure 1-2.</b> Control Panel .....	7
<b>Figure 1-3.</b> Selecting a sensor from the floor plan .....	9
<b>Figure 1-4.</b> Alarm condition encounter on the security functions .....	10
<b>Figure 2-1.</b> Selecting a video from the floor plan .....	12
<b>Figure 2-2.</b> Selecting a video from the thumbnail .....	13
<b>Figure 2-3.</b> Selecting a locked video .....	14
<b>Figure 2-4.</b> The camera password is incorrect .....	14
<b>Figure 2-5.</b> Selecting a locked video from the thumbnail .....	14
<b>Figure 2-6.</b> Alarm condition encounter on the surveillance functions .....	15
<b>Figure 2-7.</b> Selecting a recorded video from the floor plan .....	16
<b>Figure 2-8.</b> Selecting a recorded video from the thumbnail .....	16
<b>Figure 2-9.</b> Locking/modifying/deleting a camera password .....	18
<b>Figure 3-1.</b> Registration of a new secondary ID .....	20
<b>Figure 3-2.</b> Changing ID's permission .....	20
<b>Figure 3-3.</b> ID deletion confirming window .....	21
<b>Figure 3-4.</b> Changing the sensor threshold values .....	22
<b>Figure 3-5.</b> Drawing a new floor plan .....	24
<b>Figure 3-6.</b> Editing the existing floor plan .....	24
<b>Figure 3-7.</b> None-closed floor plan error .....	25
<b>Figure 4-1.</b> Internet login ID/password validation .....	27
<b>Figure 4-2.</b> Internet login ID/password validation error .....	28
<b>Figure 4-3.</b> Internet login password management .....	29
<b>Figure 4-4.</b> Internet login password management error .....	30
<b>Table D.</b> Link Table .....	31

## E. Meeting Records

To be continued on the next page.

The 1st Meeting Record															
<b>Course</b>	CS350 Software Engineering	<b>Instructor</b>	prof. Moon-zoo Kim												
		<b>Recorder</b>	Eut-deum Kim												
<b>Time</b>	March. 8th, 2008. p.m. 07:00~08:00	<b>Location</b>	Resting room in CS building												
<b>Subject</b>	How will we carry out Software Engineering project?														
<b>Attendee</b>	<b>Student Num</b>	<b>Name</b>	<b>Remark</b>												
	20010090	Eut-deum Kim													
	20030364	Myung-kyung Lee													
	20060034	Ji-seong Gu													
	20060340	Da-bi Ahn													
C o n t e n t s	<p>◎ The Contents of the meeting</p> <p><b>1. The Essential Discussion</b></p> <ul style="list-style-type: none"> <li>· Applying Water-fall mode, we'll schedule a plan and follow it. Because we need to provide for unforeseen accidents, the plan will be estimated sufficiently.</li> <li>· We'll make out the meeting record after every meeting and sign on it.</li> </ul> <p><b>2. Next schedule</b></p> <ul style="list-style-type: none"> <li>· We mediate our schedule to make chances of face-to-face meeting as many as possible and divide works to do among team member. As a result, we agree to meet three times from march 10th to 15th.</li> <li>· We need to read dialog text very carefully because it contains requirement specifications in everywhere. Dialog text is 124 pages long, so we divide it in three parts, read part by part every meeting, extract requirement specifications and integrate them during meeting by discussion.</li> <li>· After meeting, we are scheduled to cover the text like below.</li> </ul> <table border="1" style="width: 100%; border-collapse: collapse; margin: 10px 0;"> <thead> <tr> <th style="width: 20%;">Date</th> <th style="width: 20%;">Time</th> <th style="width: 60%;">Text</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">March. 10.</td> <td style="text-align: center;">p.m. 08:30 ~ 10:00</td> <td style="text-align: center;">SafeHome project dialog page 1~41</td> </tr> <tr> <td style="text-align: center;">March. 13.</td> <td style="text-align: center;">p.m. 07:00 ~</td> <td></td> </tr> <tr> <td style="text-align: center;">March. 15.</td> <td style="text-align: center;">p.m. 06:00 ~</td> <td></td> </tr> </tbody> </table> <ul style="list-style-type: none"> <li>· We schedule to make the base of the requirement specifications until march 15th and use DOORS to complete documentation in next week.</li> </ul>			Date	Time	Text	March. 10.	p.m. 08:30 ~ 10:00	SafeHome project dialog page 1~41	March. 13.	p.m. 07:00 ~		March. 15.	p.m. 06:00 ~	
	Date	Time	Text												
	March. 10.	p.m. 08:30 ~ 10:00	SafeHome project dialog page 1~41												
	March. 13.	p.m. 07:00 ~													
	March. 15.	p.m. 06:00 ~													
	※ We admit and agree with the contents of this meeting record.														
	<b>Signature</b>	Eut-deum Kim _____	Myung-kyung Lee _____												
		Ji-seong Gu _____	Da-bi Ahn _____												

The 2nd Meeting Record				
<b>Course</b>	CS350 Software Engineering		<b>Instructor</b>	prof. Moon-zoo Kim
			<b>Recorder</b>	Eut-deum Kim
<b>Time</b>	March. 10th, 2008. p.m. 08:30~10:00		<b>Location</b>	Resting room in CS building
<b>Subject</b>	Summarizing of the text of "SafeHome project dialog" ~ 41p and considering the requirement facts, finding ambiguousness			
<b>Attendant</b>	<b>Student Num</b>	<b>Name</b>	<b>Remark</b>	
	20010090	Eut-deum Kim		
	20030364	Myung-kyung Lee		
	20060034	Ji-seong Gu		
	20060340	Da-bi Ahn		
<b>C o n t e n t s</b>	◎ The Contents of the meeting <b>1. The Essential Discussion</b> · At this time, we are concerned about requirement analysis and we don't know well the requirement specifications present in dialogs. So, we regard to extract the requirement specifications from dialogs and point out ambiguity as important.			
	<b>2. Requirement Specification - Basic Structure</b> · make use of one or more PCs, various wall-mounted control panels, various sensors, appliance / device controllers. · All communicate via 802.11b wireless protocols, and designed for new home and existing homes			
	<b>3. Requirement Specification - Home Security Functions</b> · Functions <ul style="list-style-type: none"> <li>① sensor monitoring for unauthorized access(breake-ins)</li> <li>② Monitoring for fire, smoke, and CO levels.</li> <li>③ Monitoring for water levels in basement</li> <li>④ Monitoring for outside movement.</li> <li>⑤ Change security setting via the Internet</li> </ul> · Discussing Security Functions use case in textbook page 190.			
	※ We admit and agree with the contents of this meeting record.			
	<div> <div>Signature</div> <div> <div>Eut-deum Kim</div> <div>Ji-seong Gu</div> </div> <div> <div>Myung-kyung Lee</div> <div>Da-bi Ahn</div> </div> </div>			

◎ The Contents of the meeting

- Pointing out ambiguity and questions - about Security Functions

① Ambiguity in defining words

- Does 'sensor' from arm / disarm contain cameras?
- What is 'PC'? home-based PC or CPI server?
- What authority does 'administrator' have? How can 'administrator' be generated?
- What is 'security zone'?
- What is 'outside' from the word 'outside movement'?

② How does the homeowner set the levels of 'fire, smoke, CO levels, water levels'?

③ What action will be done when the trouble occurs during level monitoring?

④ What is the constraint in generating ID and passwords? Does the system distinguish uppercase and lowercase? Can the number or special characters be included? How about maximum / minimum length? Aren't there other constraints?

⑤ If the homeowner loses his / her ID or passwords when the homeowner connects the system via Internet, how does the system provide ID or passwords? How does the system confirm his / her identity? By SSN? phone?

- Discussing Control Panel use case in textbook page 193

- Pointing out ambiguity and questions - about Control Panel

① Some keypads don't have any function defined - max, test, bypass, instant, code, chime, panic

② How to set initial master password? How can the homeowner change it?

③ Action cases about away / stay mode are not enough.

- Besides away / stay modes, is any other mode needed? How about 'complete release'?
- How much time will be needed after select away mode? The homeowner needs enough time to leave the house.
- How much time will be allowed the homeowner to input password? If inputted password is wrong, how many times will be allowed the homeowner to retry?

④ Action cases about sensor detection are not enough.

- How does the system respond if the homeowner opens a window or a door in stay mode?
- How does the system respond if window / door sensor detects something but motion tracking sensor doesn't? How about opposite case?
- How does the system connect to the homeowner if sensors detects something and the system reports to the police?

#### 4. Requirement Specification - Home Surveillance Functions

- Functions

① Connect to one or more video cameras placed inside/outside house.

## ◎ The Contents of the meeting

- ② Control pan/zoom for cameras.
- ③ Define camera monitoring zones.
- ④ Display camera views on PC.
- ⑤ Access camera views via the Internet.
- ⑥ Selectively record camera output digitally.
- ⑦ Replay camera output.

· Discussing use case in textbook page 220, 222.

· Pointing out ambiguity and questions

- ① When does the camera record function start? The system records video continuously? When away mode is activated? Can the homeowner activate the camera separately?
- ② How does the system receive a floor plan data? How does the system respond when a floor plan is changed? How about changing positions of sensors or cameras?
- ③ How does the system respond if sensors or cameras don't work well?
- ④ Because of the mounted position of camera, the available pan angle can be limited.
- ⑤ How to implement the zoom function? Digital zoom or optical zoom?
- ⑥ Ambiguity in video data
  - Where does the system store video data? In the PC or CPI server?
  - What type does video data stored in? Video file? Sequence of Image files?
  - Resolution of stored video data / frame per second / color or monochrome?
  - How much does the system store replay record data?
  - If transfer rate is 1 frame per sec, the system can't respond to zoom or pan command immediately.
  - If FPS is changed by bandwidth, how does the system measure bandwidth? What will be the standard in changing FPS?

**5. Next schedule**

· After meeting, we are scheduled to cover the text like below.

Date	Time	Text
March. 10.	p.m. 08:30 ~ 10:00	SafeHome project dialog page 1~41
March. 13.	p.m. 07:00 ~	SafeHome project dialog page 42~83
March. 15.	p.m. 06:00 ~	

· We plan to read textbook based on [Page in SEPA 6th regarding SafeHome product] list.



The 3rd Meeting Record					
<b>Course</b>	CS350 Software Engineering		<b>Instructor</b>	prof. Moon-zoo Kim	
			<b>Recorder</b>	Eut-deum Kim	
<b>Time</b>	March. 13th, 2008. p.m. 07:20~09:30		<b>Location</b>	Resting room in CS building	
<b>Subject</b>	Summarizing of the text of "SafeHome project dialog" 42p ~ 83p and considering the requirement facts.				
<b>Attendant</b>	<b>Student Num</b>	<b>Name</b>	<b>Remark</b>		
	20010090	Eut-deum Kim			
	20030364	Myung-kyung Lee			
	20060034	Ji-seong Gu			
	20060340	Da-bi Ahn			
<b>C o n t e n t s</b>	◎ The Contents of the meeting <b>1. The Essential Discussion</b> · Most part of the text is about design, architecture and test. · At this time, we need elements about requirements only, so we look over the page and extract several items. · From text, we find an additional function. <b>2. Extracted Requirement Specifications - Home Security Functions</b> · New requirement is raised by the marketing team - 'a doggie angst sensor' - but <u>it won't be implemented</u> until the next release. · All sensors are controlled by the control panel. If any of sensors has trouble, that sensor interface should send signal to the control panel, and the control panel would make contact with the someone. ① Question - In the textbook, they say only 'outgoing call' - who will be the 'outgoing object'? · When the alarm condition encounter, the sensors cannot be disable. · Phone numbers must be stored in the control panel, not in the sensors. <b>3. Extracted Requirement Specifications - Home Surveillance Functions</b> · Do we have to make the floor plan? - according as "Golden Rule", we might make it. But, if we don't, instead of the floor plan, the surveillance function interface will display the list of the cameras and their locations.				
	※ We admit and agree with the contents of this meeting record.				
	<b>Signature</b>	Eut-deum Kim _____		Myung-kyung Lee _____	
		Ji-seong Gu _____		Da-bi Ahn _____	

◎ The Contents of the meeting

#### 4. Additional Function - Administration Functions

· Functions

- ① Inputting new settings or editing exist settings.
- ② Providing tools for drawing the floor plan.
- ③ Labeling sensors and cameras manually or automatically.
- ④ Establishing settings for sensors and cameras.
- ⑤ Moving / adding / deleting sensors or cameras. (if in the edit mode)
- ⑥ Doing consistency checking and help the administrator to avoid mistakes.

#### 5. Next schedule

- Because we thing that we gathered the requirement items quitely, we would begin to write the requirement specification documents.
- The important components of SafeHome product are the control panel, security functions, surveillance functions and administration functions. So, we split the subjects like below.

Name	Component
Eut-deum Kim	The Security Functions
Myung-kyung Lee	The Control Panel
Ji-seong Gu	The Administration Functions
Da-bi Ahn	The Surveillance Functions

- We agree that if someone find insufficiency of the requirement details, write down and discuss it on the next meeting.
- After meeting, we are scheduled to cover the text like below.

Date	Time	Text
March. 10.	p.m. 08:30 ~ 10:00	SafeHome project dialog page 1~41
March. 13.	p.m. 07:20 ~ 09:30	SafeHome project dialog page 42~83
March. 15.	p.m. 07:00 ~	SafeHome project dialog page 84~124

The 4th Meeting Record								
<b>Course</b>	CS350 Software Engineering		<b>Instructor</b>	prof. Moon-zoo Kim				
			<b>Recorder</b>	Eut-deum Kim				
<b>Time</b>	March. 15th, 2008. p.m. 07:20~08:50		<b>Location</b>	Resting room in CS building				
<b>Subject</b>	Summarizing of the text of "SafeHome project dialog" 83p ~ 124p and considering the requirement facts.							
<b>Attendant</b>	<b>Student Num</b>	<b>Name</b>	<b>Remark</b>					
	20010090	Eut-deum Kim						
	20030364	Myung-kyung Lee						
	20060034	Ji-seong Gu						
	20060340	Da-bi Ahn						
<b>C o n t e n t s</b>	◎ The Contents of the meeting <b>1. The Essential Discussion</b> · Most part of the text is about design, implementation and testing of the web applications by outsourcing, team structure, estimation, scheduling and so on. · At this time, we need elements about requirements only, so we look over the page and extract several specifications. · We define more detailed template of the requirement specification.							
	<b>2. Extracted Requirement Specifications - General System Composition</b> · SafeHome hardware structure is consist of the control panel, home based PC, CPI server. The control panel is an interface, PC takes charge of external access & storing data and CPI server provides web service. (page 279) · During installation, SafeHome PC used to configure the system. The type and number of each sensor, master password, telephone number are stored in PC. Telephone number is used when a sensor event occurs. (page 227) · From this statement, we assume that CPI server stores web site login ID, passwords. The other informations like video data, sensor configuration are stored in PC.							
	<b>3. Extracted Requirement Specifications - Control Panel</b> · If a sensor event occurred, the software invokes an alarm. (page 228)							
	※ We admit and agree with the contents of this meeting record.							
	<table border="0"> <tr> <td rowspan="2"><b>Signature</b></td> <td>Eut-deum Kim _____</td> <td>Myung-kyung Lee _____</td> </tr> <tr> <td>Ji-seong Gu _____</td> <td>Da-bi Ahn _____</td> </tr> </table>				<b>Signature</b>	Eut-deum Kim _____	Myung-kyung Lee _____	Ji-seong Gu _____
<b>Signature</b>	Eut-deum Kim _____	Myung-kyung Lee _____						
	Ji-seong Gu _____	Da-bi Ahn _____						

## ◎ The Contents of the meeting

- After delay time configured by the homeowner, the software dials a telephone number of a monitoring service, provides information about the location and the nature of the detected event. (page 228)
- If a telephone connection isn't obtained, the software redial the telephone number every 20 seconds. (page 228)
- The homeowner receives security information via a control panel, the PC, or a browser. (page 228)
- The control panel receives a 4-digit password. If it doesn't match with the master password, it is compared to the secondary password. (page 232)
- The secondary password may be assigned to people who require entry to the home when the owner is not present. (page 232)
- ① Question - How the homeowner can set the secondary password?

**4. Template of the Requirement Specification**

- By experience in describing the component requirement, we conclude clauses of the requirement specifications.
  - ① Description : a general function and description.
  - ② Scenario : a user scenario considering all user actions.
  - ③ Qualification Provision : precondition.
  - ④ Priority : implementation priority.
  - ⑤ Special Requirement : technical requirements that doesn't be described in the scenario.
  - ⑥ Constraints : constraints of user input or etc that doesn't be described in the scenario. For example, constraints of ID / password.
  - ⑦ Exceptions : if events that have no relations with user actions or events that doesn't be described in the scenario by user actions.

**5. Next schedule**

- After meeting, we are scheduled to have a meeting next week

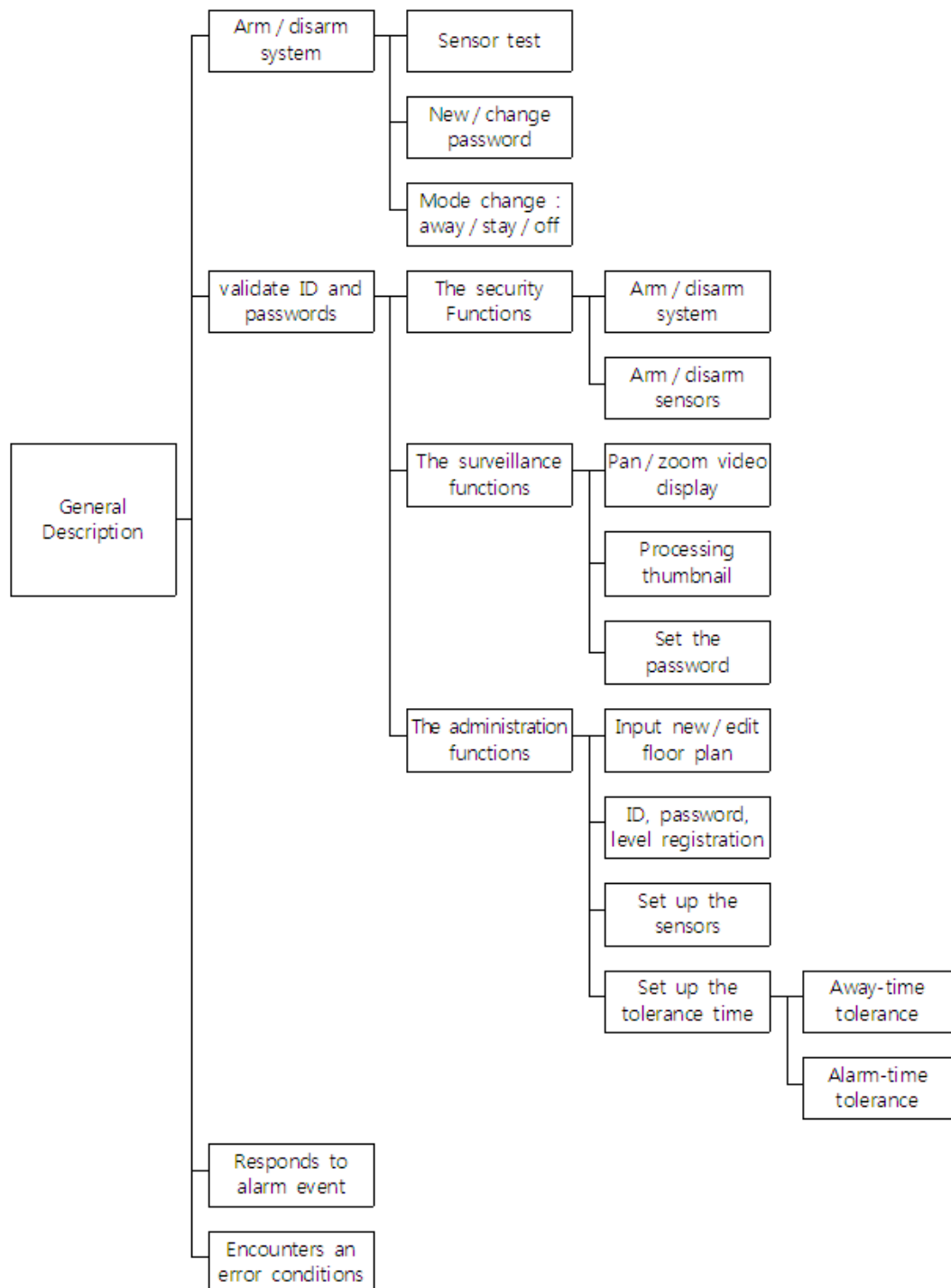
Date	Time
March. 17.	p.m. 07:00 ~
March. 19.	p.m. 04:30 ~

The 5th Meeting Record				
<b>Course</b>	CS350 Software Engineering		<b>Instructor</b>	prof. Moon-zoo Kim
			<b>Recorder</b>	Eut-deum Kim
<b>Time</b>	March. 17th, 2008. p.m. 08:00~09:20		<b>Location</b>	Resting room in CS building
<b>Subject</b>	The structure of the requirement and general assumptions			
<b>Attendant</b>	<b>Student Num</b>	<b>Name</b>	<b>Remark</b>	
	20010090	Eut-deum Kim		
	20030364	Myung-kyung Lee		
	20060034	Ji-seong Gu		
	20060340	Da-bi Ahn		
<b>C o n t e n t s</b>	◎ The Contents of the meeting			
	<b>1. The Essential Discussion</b>			
	· Since the last meeting, we have tried to describe the requirement modules, but base assumptions are insufficient. So we agree to add several assumptions to describe the requirement specifications.			
	· We conclude the essential structure of the requirement specifications.			
	· We standardize several words to describe uniformly.			
	<b>2. Assumptions</b>			
	· To access to the SafeHome software installed on PC, the homeowner must use web browser program even if the homeowner is at his/her home. External direct connection to the control panel, sensors, cameras are not allowed because there can be security troubles.			
	· Using web browser, the homeowner can connect to the SafeHome software through the CPI server. The CPI server validates the homeowner's ID and passwords, takes data from the SafeHome software installed on PC and makes up UI.			
	· The SafeHome software receives the master password and phone number to be dialed when the appropriate events are occurred during installation. The software doesn't receives any other input at the other time except access via internet.			
	※ We admit and agree with the contents of this meeting record.			
<b>Signature</b>	Eut-deum Kim _____		Myung-kyung Lee _____	
	Ji-seong Gu _____		Da-bi Ahn _____	

© The Contents of the meeting

- To register new login ID, passwords and their level, the homeowner or the administrator uses the Administration Function.

**3. the essential structure of the requirement specifications.**



◎ The Contents of the meeting

**4. standardized words**

- SafeHome, SafeHome Product Web site, web site : be careful about uppercase and lowercase.
- activate / deactivate : don't use 'on / off'.
- the homeowner : don't use 'client' or 'customer'.
- guest : person who uses secondary password.
- ~ of the house : don't use '~ of the home'.
- the system displays ~ : if the system shows something on the screen.
- view : feature that the system displays on the screen.
- The words will be added continuously.

The 6th Meeting Record					
<b>Course</b>	CS350 Software Engineering		<b>Instructor</b>	prof. Moon-zoo Kim	
			<b>Recorder</b>	Eut-deum Kim	
<b>Time</b>	March. 19th, 2008. p.m. 04:30~06:20		<b>Location</b>	Resting room in CS building	
<b>Subject</b>	Supplementary requirement, assumptions and standardized words				
<b>Attendant</b>	<b>Student Num</b>	<b>Name</b>	<b>Remark</b>		
	20010090	Eut-deum Kim			
	20030364	Myung-kyung Lee			
	20060034	Ji-seong Gu			
	20060340	Da-bi Ahn			
<b>C o n t e n t s</b>	◎ The Contents of the meeting <b>1. The Essential Discussion</b> · Most parts of the requirements are nearly finished, but to complete works, we need more assumptions and accurate definitions. · There is some inconsistency because of misunderstanding in communication - for example, functions of "Validation of ID and passwords". We talk about general assumptions more deeply. · We standardize several words and sentences to describe uniformly.				
	<b>2. Assumptions</b>				
	· Validations of ID / passwords is the function that verifies the identify of the homeowner or guest and permits him/her to access to the functions according to the level of the ID.				
	· For every one SafeHome Product package, only one ID can have administrator permission. The other IDs are just guest IDs.				
	· To register new login ID, passwords and their level, administrator uses the administration functions to generate ID, temporary passwords and its level. Guest is able to log on with ID and temporary passwords and change his / her passwords. Guest ID can access the security functions and surveillance functions according to its level, but cannot access the administrator functions.				
	· Administrator can change the level of the guest IDs or delete them.				
	※ We admit and agree with the contents of this meeting record.				
	<b>Signature</b>	Eut-deum Kim _____		Myung-kyung Lee _____	
		Ji-seong Gu _____		Da-bi Ahn _____	



## © The Contents of the meeting

- Administrator can watch the video locked without password and cancel the lock.

**3. standardized words**

- input box : a blank form that the system displays to receive data from the homeowner or guest.
- guest : a person who doesn't have the administrator permission or isn't the homeowner.
- select : the action of the homeowner or guest to use functions on the web site.
- push : the action of the homeowner or guest to use functions on the control panel.
- his / her, he / she : don't use 's / he'. be careful for order.
- duplication (of IDs or passwords) : don't use 'redundancy'.
- The words will be added continuously.

**4. standardized sentences**

- The system must be fully configured.
- The administrator must be in a log-in state and have the administrator permission.
- The system must store passwords as encrypted data in the CPI server.
- The sentences will be added continuously.

**5. Next schedule**

- After meeting, we are scheduled to have a meeting tomorrow.

Date	Time
March. 17.	p.m. 08:00 ~ 09:20
March. 19.	p.m. 04:30 ~ 06:20
March. 20.	p.m. 05:30 ~

- We plan to integrate, renumber the requirement parts and add links on them.

The 7th Meeting Record					
<b>Course</b>	CS350 Software Engineering		<b>Instructor</b>	prof. Moon-zoo Kim	
			<b>Recorder</b>	Eut-deum Kim	
<b>Time</b>	March. 20th, 2008. p.m. 05:30~12:00		<b>Location</b>	Resting room in CS building	
<b>Subject</b>	Integration of the modules, supplementary requirement, assumptions and standardized words				
<b>Attendant</b>	<b>Student Num</b>	<b>Name</b>	<b>Remark</b>		
	20010090	Eut-deum Kim			
	20030364	Myung-kyung Lee			
	20060034	Ji-seong Gu			
	20060340	Da-bi Ahn			
<b>C o n t e n t s</b>	◎ The Contents of the meeting <b>1. The Essential Activities</b> · We integrate, renumber the requirement parts and add links on them. · But, there are still some discordances among the modules - we need to standardize them more. · We establish scales to measure priority. The scales must be used in a point of the client's view and consists of 5 steps, very low - low - moderate - high - highest. · The password management module was in the Administration Functions, but we take it out of the original location and set it as the major function because the homeowner or user must be able to change his/her passwords although he/she doesn't have the administrator permission. · We add more several standardized words and sentences. · We conclude the basic structure of the documents.				
	※ We admit and agree with the contents of this meeting record.				
	<b>Signature</b>	Eut-deum Kim	Myung-kyung Lee		
		Ji-seong Gu	Da-bi Ahn		

<b>C o n t e n t s</b>	© The Contents of the meeting	
	<b>2. The Basic Structure of the Documents - Will be the Table of Content</b>	
	General Description	3.2.0 General Functions
	1 Scope	3.2.1 Permission Management
	2 Product Perspective	3.2.2 ID Registration
		3.2.3 Floor Plan Management
		3.2.4 Tolerance Time Setting
		3.2.5 Sensor Threshold Setting
	Requirement Specification	3.3 Security Functions
	1 Installation	3.4 Surveillance Functions
	1.1 Description	3.4.0 General Functions
	1.2 Scenario	3.4.1 Thumbnail Processing
	1.3 Qualification Provision	3.4.2 Pan and Zoom Video
	1.4 Priority	3.4.3 Recorded Video
	1.5 Special Requirements	3.4.4 Password Management
	1.6 Constraints	3.5 Password Change
	1.7 Exceptions	4 Alarm Condition
	2 Control Panel	Appendix
	2.1 Mode Change	1 Glossary
	2.2 Sensor test	2 Meeting Records
	2.3 Password Management	3 Who-did-what list
	3 Access via Internet	
	3.1 ID/passwords Validation	
	3.2 Administration Functions	
	<b>3. standardized words</b>	
	· the SafeHome Product service team, service team	
	· The words will be added continuously.	
	<b>4. standardized sentences</b>	
	· If the system encounters an alarm condition, all activate-deactivate functions does not work until an alarm condition is destroyed or the homeowner calls off an alarm by setting "off" mode.	
	· If the homeowner input different passwords at ~, the system displays an alert message box and blank input boxes to input passwords again.	
	· This requirement document describes the scenario, requirements and constraints when ~.	

## © The Contents of the meeting

- All sentences are begun with "The homeowner"+verb or "The system"+verb as much as possible.

**5. Next schedule**

- We plan to make hard-copy documents and reviews finally tomorrow.

## F. Who-did-what list

Here is our who-did-what list in student number order.

Eut-deum Kim	Wrote all meeting records. Drew all UI pictures. Made document forms. Made the appendix. Wrote the Installation module. Wrote the Internet Login ID / password Validation module.
Myung-kyung Lee	Wrote general description. Wrote the Arm / Disarm System module. Wrote the Arm / Disarm Sensors module. Wrote the Alarm Condition module.
Ji-seong Gu	Wrote the ID / Permission Management module. Wrote the Sensor Threshold Management module. Wrote the Floor Plan Management module. Wrote the Internet Login Password Management module. Inputted data into DOORS.
Da-bi Ahn	Wrote the Show Current Video module. Wrote the Show Recorded Video module. Wrote the Camera Password Management module.