Contents

List of Figures

Chapter 1

Introduction

Introduction

Chapter 2

Functional Requirements

2.1 High-level functionality

The high level functionality of this system can be broken down into several major sections. Sensors play a major role in interfacing the real world with the several other sections of the controller. Physical security, both inside and outside of the home is important. This goes hand in hand with family security once family members have left the premises of the household. Finally, green energy management can be easily integrated with the other systems to ensure prudent usage of resources.

2.1.1 Sensors

The most crucial part of the system that ties all of the other parts together is the sensor network. They are the interface between the real world and the controllers. They detect if the house has been intruded upon by outsiders through sensors on the windows and doors. They can alert the family if somebody left the stove top on. Living patterns can be established and monitored to warn of health problems or to control the HVAC so that energy is not wasted when nobody is home or they are all asleep. Cameras, motion detectors, hall effect sensors, and other miscellaneous sensors comprise the majority of this network.

Cameras play multiple roles in the sensor network. Facial recognition can be used to detect family members entering and leaving the house to track their activities. They can be used to alert when strangers are approaching the door or are on the premises in either a friendly manner or in a more cautious one depending on the family members currently at home.

Motion detectors provide the security system with the means to trigger alerts when motion is detected in certain areas of the home while the system is armed. A network of motion detector sensors will be positioned in the hallways of the home, with particular attention to entries to the home. Motion detectors outside the house will be able to control the lighting system such that people approaching the home can be illuminated and easily identified.

Temperature sensors and hall effect sensors are two other major components. Temperature sensors can be used by both physical security, to ensure that the oven has not been on for an extended period of time without user interaction as well as for green energy management to control the overall temperature of the house or each room. Hall effect sensors can be used with temperature sensors to detect if windows or doors have been left open when they should be closed in order to prevent wasting energy. These sensors can also be used to detect intruders attempting to break in through windows or doors.

2.1.2 Family Safety

In addition to necessary home security functionality, the system will incorporate methods to provide safety to members of the users' family. Child safety is a particular concern that will be addressed by this portion of the home security system. Sensors will be implemented on cabinets as well as certain areas of the home that may contain hazardous materials that could be harmful to children. Contact sensors will be present on medicine cabinets, closets with cleaning materials, and knife drawers to alert the user that these areas of the home have been accessed.

2.1.3 Security System

2.1.4 Green Energy Management

2.2 Scenarios

Arming the System - NFC Device

The resident is leaving the home and wishes to arm the security system. The resident can do so by approaching the security console and holding their NFC device within 0.2 meters of the interface. The resident must hold their NFC device near the console until the device is read and identified by the system as belonging to the resident of the home. Once this is confirmed, the user may leave the home while the system initiates the arm countdown. Once the system completes the countdown, the system has been successfully armed.

Disarming the System - NFC Device

The procedure for disarming the system using an NFC device is very similar to the arming procedure. The resident enters the home at which point the disarm countdown begins. The resident holds his NFC device up to the console to disarm the system. The NFC device is identified and the security system is disarmed and the countdown is interrupted.

Arming the System - Keypad

The resident wishes to arm the security system, but is not in possession of an NFC device. The resident can arm the system by entering a valid security code. Once the code has been entered, it is validated by the system. The system initiates the arm countdown, and the resident may now leave the home. The arm countdown completes and the system is now armed.

Disarming the System - Keypad

The procedure for disarming the system using the keypad is very similar to the arming procedure. The resident enters the home at which point the disarm countdown begins. The resident enters a valid security code into the console using the keypad to disarm the system. The NFC device is identified and the security system is disarmed and the countdown is interrupted.

Window Intrusion

The security system is in the armed state. An intruder attempts to open a window from outside the home. The system receives a signal from the window's sensor that notifies the system that a window has been opened. The system enters its alarm state.

Door Intrusion

The security system is in the armed state. An intruder picks the lock on the front door and opens it. The system begins the alarm countdown alongside audible beeping once the intruder opens the door. The intruder leaves the premises while the countdown continues. The countdown reaches zero and the system enters the alarm state.

Fridge Left Open

The resident opens the fridge door for a drink, and does not close it fully. Unaware, the resident leaves the kitchen and sits down in the living room. Meanwhile, a countdown has begun while the fridge door remains open. The countdown finishes and a notification is sent to the resident via SMS. The kitchen speaker broadcasts an audible message stating that the fridge door has been left open. The user enters the kitchen and closes the fridge door, resetting the system.

Childproof Cabinets

A child in the home has accessed a cabinet that contains hazardous or dangerous materials. The contact sensor installed on the cabinet door triggers a countdown. When the countdown reaches zero, and audible alarm is produced and an SMS is sent to the resident of the home to notify them of the event.

Separately, an adult resident of the home accesses the same cabinet. The contact sensor on the cabinet door triggers the countdown. The resident pushes a hidden actuator located on the inside of the cabinet to halt the countdown. The resident closes the cabinet door when he / she is finished and the sensor notifies the process to go back to its normal wait state.

Child Bedroom Safety

The resident of the home has placed his child in the crib for the night. When the resident leaves the bedroom, he arms the child bedroom safety system and closes the door. During the middle of the night, the child climbs out the crib and falls to the floor. Motion sensors installed in the room detect this unexpected activity and sound an alarm in the parents' bedroom to notify them of the event.

2.3 Use case model

Use case name	`NFCDisarmSystem`
Participating Actors	Initiated by `Resident`
Flow of Events	1. The `Resident` enters the home while in possession of an NFC device. 2. The system begins the disarm countdown. 3. The `Resident` approaches the console and holds the NFC within 0.2 meters of the console. 4. The data on the NFC device is read and validated by the system. 5. The system enters the disarmed state and the disarm countdown is halted.
Entry Condition	The system is in the armed state and the Resident enters the home in possession an NFC device.
Exit Condition	The system is disarmed.
Quality requirements	TODO

Use case name	`KeyPadDisarmSystem`
Participating Actors	Initiated by `Resident`
Flow of Events	1. The `Resident` enters the home. 2. The system begins the disarm countdown. 3. The `Resident` approaches the console and enters their code using the keypad on the console. 4. The entered code is validated by the system. 5. The system enters the disarmed state and the disarm countdown is halted.
Entry Condition	The system is in the armed state and the Resident enters the home.
Exit Condition	The system is disarmed.
Quality requirements	TODO

Use case name	`NFCArmSystem`
Participating Actors	Initiated by `Resident`
Flow of Events	1. The `Resident` approaches the console and holds the NFC within 0.2 meters of the console. 2. The data on the NFC device is read and validated by the system. 3. The system begins the arm countdown. 4. The `Resident` leaves the home. 5. The system arm countdown completes and the system enters the armed state.
Entry Condition	The system is in the disarmed state and the `Resident` wishes to arm it using an NFC device.
Exit Condition	The system is armed.
Quality requirements	TODO

Use case name	`KeyPadArmSystem`
Participating Actors	Initiated by `Resident`
Flow of Events	1. The `Resident` approaches the console and enters their code. 2. The entered code is validated by the system. 3. The system begins the arm countdown. 4. The `Resident` leaves the home. 5. The system arm countdown completes and the system enters the armed state.
Entry Condition	The system is in the disarmed state and the `Resident` wishes to arm it using the keypad.
Exit Condition	The system is armed.
Quality requirements	TODO

Use case name	`WindowIntrusionAlarm`
Participating Actors	Initiated by any actor.
Flow of Events	1. A window is opened. 2. The system receives the signal that the window has been opened. 3. The system enters the alarm state.
Entry Condition	The system is in the armed state and a window is opened.
Exit Condition	The system alarm is triggered.
Quality requirements	TODO

Use case name	`DoorIntrusionAlarm`
Participating Actors	Initiated by any actor.
Flow of Events	1. A door is opened. 2. The system begins the alarm countdown. 3. The initiating actor does not disarm the system. 4. The alarm countdown reaches zero. 5. The system enters the alarm state.
Entry Condition	The system is in the armed state and a door is opened.
Exit Condition	The system alarm is triggered.
Quality requirements	TODO

Use case name	`FridgeOpenNotification`
Participating Actors	Initiated by any actor.
Flow of Events	1. The initiating actor opens the fridge door. 2. The system begins a countdown. 3. The countdown completes without the fridge door being closed. 4. A notification is broadcast via SMS and loudspeaker throughout the house, depending on configuration.
Entry Condition	Fridge door is opened.
Exit Condition	A “fridge has been left open” notification is broadcast.
Quality requirements	TODO

Use case name	`CabinetAlarm`
Participating Actors	Initiated by any actor. `Resident` is a participant.
Flow of Events	1. A secure cabinet is opened by the initiating actor. 2. The contact sensor within the cabinet is tripped and a countdown begins. 3. The countdown timer reaches zero. 4. An audible alarm is produced by the system and an SMS is sent to the `Resident` notifying them of the intrusion.
Entry Condition	A secure cabinet is opened.
Exit Condition	An audible alarm is produced and an SMS alert is sent to the `Resident`
Quality requirements	TODO

Use case name	`CabinetAccess`
Participating Actors	Initiated by `Resident`.
Flow of Events	1. A secure cabinet is opened by the `Resident`. 2. The contact sensor within the cabinet is tripped and a countdown begins. 3. The `Resident` pushes a hidden actuator within the cabinet. 4. The countdown timer is stopped. 5. The `Resident` closes the cabinet after they are finished.
Entry Condition	A secure cabinet is opened.
Exit Condition	The secure cabinet is closed.
Quality requirements	TODO

2.4 Object model

2.5 Dynamic model

2.6 Interfaces

There are two interfaces between the components. The sensors need a way to communicate to the controller their current data and the controller needs to communicate to the actuators. Data from the controller needs to be sent to a central server, which is then accessible through other user interfaces.

2.6.1 Physical Hardware and Controller

The hardware such as sensors and actuators communicate wirelessly through bluetooth to the controller. Two way communication is required as the hardware needs to be able to register with the controller. The controller should also be able to poll each sensor on a regular schedule to ensure that they are operational and functioning properly. Examples of these sensors include temperature, Some sensors need to report their status when an event occurs so the controller interface needs to be able to handle tight polling with interrupts to correctly collect all data.

2.6.2 Server

The server acts as the man in the middle interface between the controller and the graphical user interfaces. The controller sends data, as appropriate, to the server on a regular basis. The server stores the data in a database. The user accesses the data and can send state updates through an API exposed by the web server.

Chapter 3

Non-Functional Requirements

Chapter 4

User Interfaces

The main user interface for this system is the user's smart phone device. Most individuals have a smartphone, be it an iPhone or an Android device, and integration into these platforms would make it easy for users to adopt to the system.

4.1 Smartphone Application

A smartphone application will allow the user to monitor their residence as well as turn on or off various components of the system. If the device has near-field communication built into it, then it will be able to be used to arm and disarm the system upon entry or when leaving the premises.

The application will have three main purposes. The first is to display data and statistics over time in a easily understood manner. The second is to allow fine control over various sub-systems such as the state of the security system, thermostat, and lights – both interior and exterior. The final duty is to track the status of each family member through GPS integrated into the mobile device.

It is relatively simple application. Figure 4.1 shows a wireframe of the first screen seen when the application is started. This is the main navigation between the different features. A simple settings wireframe is shown in Figure 4.2. Not all capabilities are shown in the wireframes to reduce complexity. Navigation flow is also omitted to avoid any platform specific paradigms. Access control is required to prevent younger family members from accidently unlocking doors or disarming the security system.

Features of this application are determined by the sensors and actuators in the system. The application will need to use a secure API accessible through a website hosted by the server. This setup is described in Section 4.3.

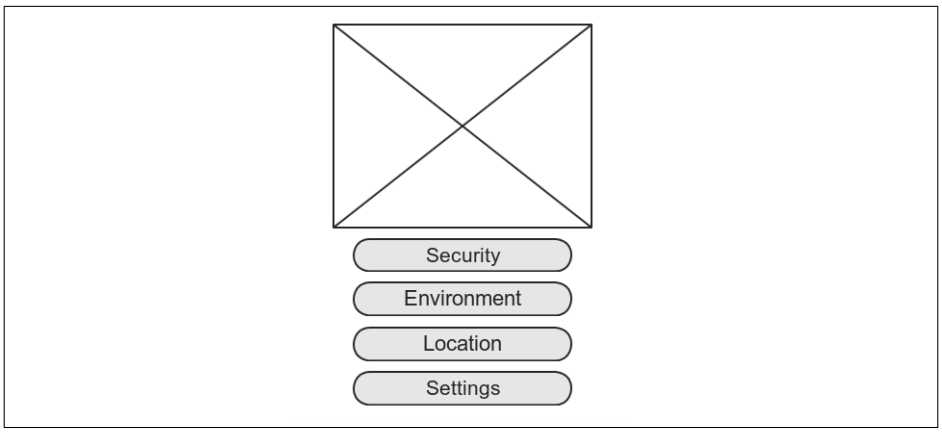

Figure 4.1: Wireframe of the home screen

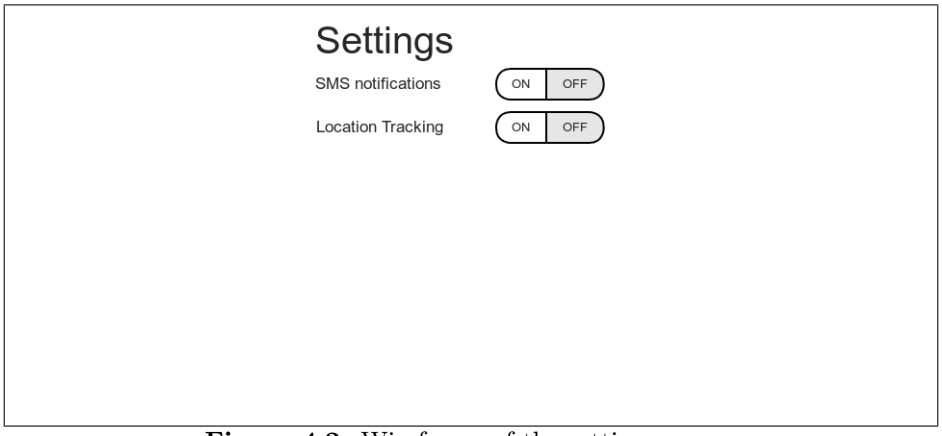

Figure 4.2: Wireframe of the settings screen

Various portions of the security system can be controlled through the wireframe in Figure 4.3. The entire system can be armed and disarmed, locks on doors activated and deactivated, and the status of the windows can be reported. Pressing on the button for window status will bring up another more detailed screen that lists individual windows and reports their status, closed or open. Door locks, if it is supported can be locked or unlocked from this screen if the lock supports it.

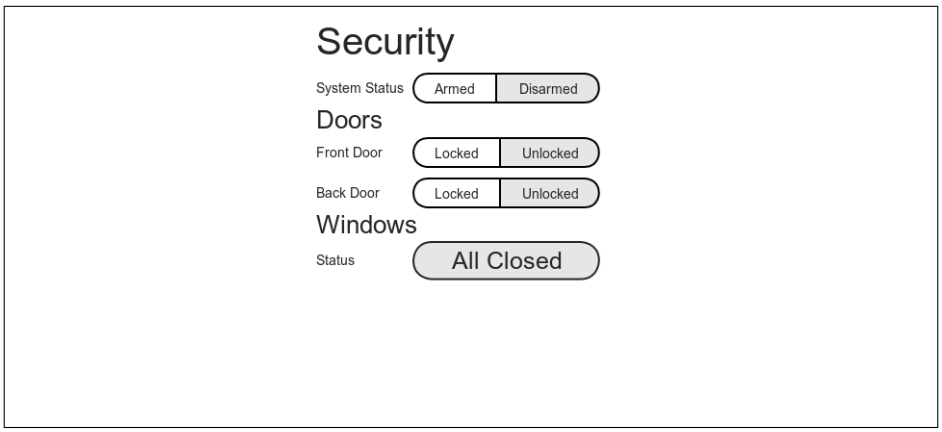

Figure 4.3: Wireframe of the security screen

Environmental details are controlled in Figure 4.4. The temperature of the house can be monitored and set. Pressing on the button labeled "HISTORY" will bring up a graph of the household temperature over a period of time. This screen can also display images from cameras at the doors to allow for the user to check who is at the door before unlocking it. Details from more specific portions of the enviroment can be displayed here as well. For example, the status of the stove and oven in the kitchen. It is also possible to report the internal temperature of the oven to ensure that it is not overheating.

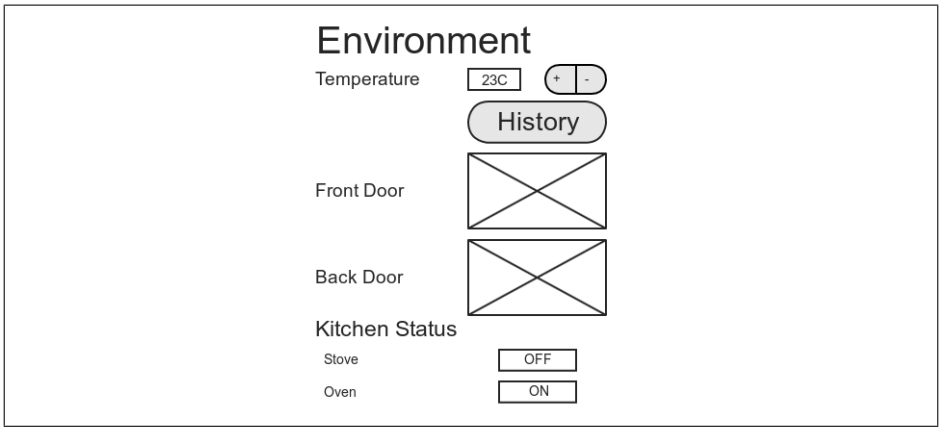

Figure 4.4: Wireframe of the environment screen

Family member locations – at least those with smartphones and this application – are displayed in Figure 4.5. Each family member will have a pin on the map to show their location using their device's GPS capabilities. Clicking on a name will move the map to the present location of that person. It will also display in text where the family member presently is located.

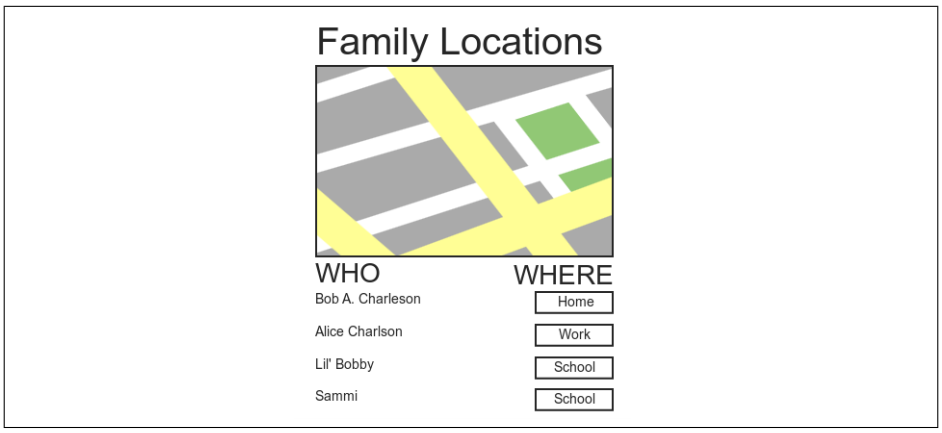

Figure 4.5: Wireframe of the locations screen

4.2 Near-field Communication Keypad

A keypad located near the main entrances to the house provides a physical interface to setting the security system and other states. Two methods are provided for arming and disarming. The first is near-field communication if the user's smartphone supports it. Authentication is done with a simple tap of the device to the keypad and then the user can set the state of the system. The other authentication method is for the user to input their unique keycode. The intention of this keypad is a fallback method in case the user does not have a smart phone or if they have mis-placed it.

4.3 Web Server

A web server serves two purposes. It provides an interface between the mobile application described in Section 4.1 and the system controller. Data can be accessed remotely through API requests and the state of the system can be modified by sending requests to it. The other purpose is to maintain a log of all the events for trend analysis and household history. The server should be located at a remote location for data security. A graphical frontend implemented on the server will also allow for remote monitoring when the user does not have their phone on their person.