**Software Requirements Specification**

for

**Smart Security Camera**

Group 4:

Julian Jones

Jacob Hopkins

Britain Mackenzie

Deontee Hendricks

Version: 1.0 June 18, 2019

Table of Contents

1. Preface

1.1 Introduction

1.2 Purpose

1.3 Document Organization

1.4 Intended Audience

1.5 Proposed Document Scope

1.6 Definitions

1. Description

2.1 Product Overview

2.2 Product Functions

2.2.1 Set – Up

2.2.2 Daily Use

2.3 User Characteristics

2.4 User Constraints

2.5 Assumptions and Dependencies

1. Functional Requirements

3.1 Model of Smart Security Camera System

3.2 Application Use Case Scenarios

3.2.1 Use Case 1: Pop-up alert

3.2.2 Use Case 2: Edit Personal Preferences

3.2.3 Use Case 3: View Video Feed

3.2.4 Use Case 4: Contact System Administrator

3.2.5 Use Case 5: Respond to User in Contact

3.2.6 Use Case 6: Manage Database System

1. Non-Functional Requirements

4.1 Reliability:

4.1.1. Video Functionality.

4.1.2. Event Detection.

4.2 Robustness:

4.2.1. Power outage.

4.2.2. Connection Failure.

4.2.3. System Failure.

4.3 Performance:

4.3.1. System Storage.

4.3.2. Streaming Speed.

4.3.3. Event Processing.

4.4 Maintainability:

4.4.1. Event and Object Library.

4.4.2. Application Updates.

4.5 Usability:

4.5.1. Mobile Integration.

4.5.2. Application.

4.6 Security:

4.6.1. User Verification.

1. Design and Implementation Compliance

5.1. Standards compliance

5.1.1. Industry Standardization.

5.1.2. Encryption.

5.2 Determining Unique Identifier:

5.2.1. Cellular Devices.

5.2.2. Non-Cellular Devices.

5.2.3. Failure to Identify.

5.3 Development constraints:

5.3.1. Hardware.

5.3.2. Encryption Design.

1. References

**1.Preface**

**1.1 Introduction**

This document explains the purpose of a smart security camera designed for residential use. The camera would operate independently of the home’s security system and is intended to be an additional safety measure.

**1.2 Purpose**

This document describes the general functionality of a smart security camera as well as the mobile UI application the allows the users to manage the system.

**1.3 Document Organization**

This document uses a numbered format to order the information. The order of the information is irrelevant if the information is not numbered.

**1.4 Intended Audience**

This document is intended for developers of the system, as well as users of the security camera.

**1.5 Proposed Document Scope**

The security camera will consist of the following subsystems:

* + - The user interface application will allow the user to receive notifications regarding the system, manage storage, and also add, remove and manage users. Users will be able to use the app to view a live video feed, as well as any recorded footage as well.
    - The camera will have thermal and facial recognition software, as well as a microphone for event identification. The camera will be motorized and will include depth and motion sensors for tracking and detection. The camera will have a backup battery so that it may continue to operate in the event of a power outage. All footage recorded on the camera will be in high definition
    - Event Handling software will determine any events reported by the camera. The camera will be capable of identifying door approaches, fire, Break ins, gunfire, and car accidents.

**1.6 Definitions**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Administrative user | In addition to standard user features.  The admin will also be able to add, remove users, as well appoint other administrative users. And manage storage |
| Authenticated user | User with access to all standard user functions. Must be added to system by administrator |
| Camera | Device responsible for recording footage to be analyzed by event handling software |
| Event | An occurrence that could potentially jeopardize the safety of the residence |
| Event Handling Software | Determines the type of event through use of computer vision algorithm and notifies user |
| User Interface Application | Mobile app that will allow users to access the system |

**2. Description:**

**2.1 Product Overview**

In the classic *boardgame* of Connect Four, two players sit opposite a board that sits on its side, with a grid of forty-two (six by seven) cells. Alternating turns, each player drops a yellow or red disk into a column, eventually building stacks. To be a victor, one must manage to create a unbroken line (horizontal, vertical, or diagonal) of their disk color. In this *software*, the same rules to be a victor apply, but a player can play against a friend, or against the program itself, with easy and hard mode.

**2.2. Product Functions**

The game will allow any player(s) who has downloaded the software to play one-player mode on their local machine, or two-player mode by connecting to a remote server which facilitates a game between two remote human players.

**2.2.1. Set-up**

Setup is dependent on user preference. The software will start on a menu screen, where the user has three choices: single-player, two-player, and leaderboard. Should the user click single-player, they are presented with a popup to query if they want easy or hard mode. Then the gameboard is loaded. Should the user click two-player, an attempt to connect to the server is made. Upon success (and a waiting player) the gameboard loads for both players, and their moves are synchronized by the server. In either gaming mode, the end result for each player is one of three: quit, lose, win. The latter is the only option that allows for a chance at the leaderboard. Finally, chose the user click leaderboard as a menu option, they will be presented with the best local scores.

**2.2.2 . Daily Use**

Frequency of use is dependent upon the player(s).

**2.3 User Characteristics**

The target group of users will be players who like strategy games, or even coders who like to decorate or improve upon simple programs.

**2.4 Constraints**

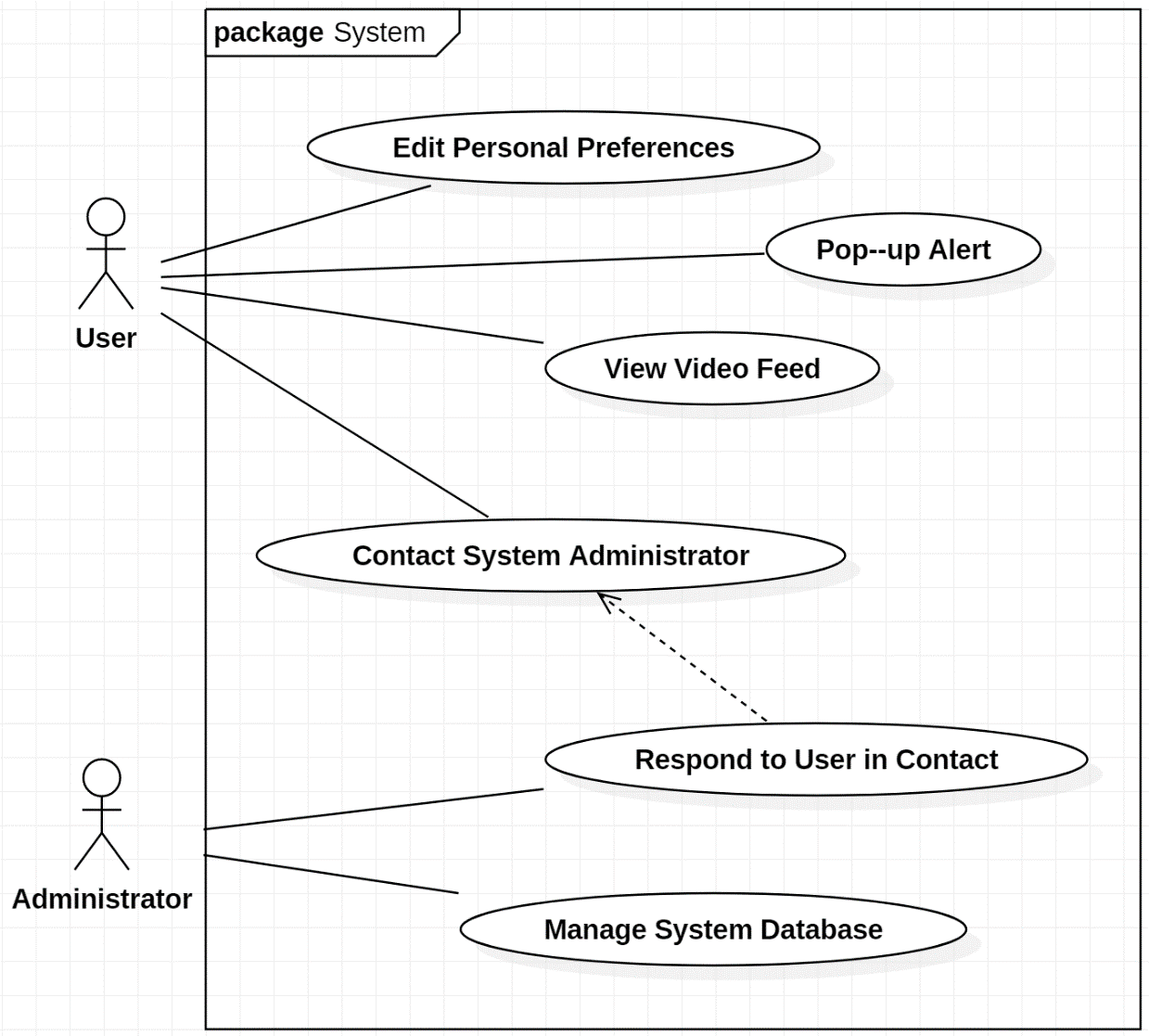
The two-player mode depends upon a remote connection to a server. A constraint is that the server must always be listening and operational. The burden of the server rests upon the users of the software, as they must implement a server on their own machine.

**2.5 Assumptions and dependencies**

The assumption of the software is that the user knows (or has the technological means to look up) the rules and strategy of Connect Four. The software assumes at least one user has setup a server to facilitate two-player mode, and logically this is dependent upon at least one user knowing how to setup port forwarding on their router.

**3. Statement of functional requirements**

**3.1. Model of Smart Security Camera System**



**3.2. Application Use Cases**

**3.2.1. - Use Case 1**

**Name:** Pop-up Alert

**Actor:** User

**Path Outline:**

1. Security camera detects a potential threat and notifies the phone application
2. Application displays a notification on the users’ phone, prompting “View” or “Ignore”
3. If user clicks “View”

3.1. Application displays live video feed on individual user’s phone

3.2. Application prompts user the “Call 911”, “Call Emergency Contact”, or “Ignore”

3.2.1. If user clicks on “Call 911” option

3.2.1.1. Application calls and alerts the police

3.2.2. If user clicks on “Call Emergency Contact” Option

3.2.2.1. If individual user has not set up an emergency contact

3.2.2.1.1. “Call Emergency Contact Button” appears gray and has no function

3.2.2.1.2. “Warning” symbol is displayed on button

3.2.3. If user clicks on “Ignore”

3.2.3.1. Notification pop-up disappears

3.2.3.2. Application turns off live feed

3.2.4. Else if user does not choose any option within 5 minutes

3.2.4.1. Application automatically notifies the police

1. If user clicks “Ignore”

4.1. The alert notification disappears from the user’s phone screen

**Entry Condition:**

1. The security camera has successfully detected all conditions to determine a situation as a threat

**Exit Condition:**

1. User has manually chosen to “Ignore” the threat on the application interface
2. User has manually chosen to contact “911” or on the application interface
3. User has manually chosen to contact “Emergency Contact” on the application interface

**System Requirements:**

1. Security Camera must be connected to a steady ethernet or WIFI connection
2. Phone application must always be in connection with the security camera system
3. Maximum number of users must be capped at 5 people per security camera for maximum streaming quality
4. Interface must always be able to show live video feed when displaying an alert
5. Security camera system must always be in contact with system administrators

**3.2.2. - Use Case 2**

**Name:** Edit Personal Preferences

**Actor:** User

**Path Outline:**

1. User clicks on the “Settings” option (Figure 1.1)
2. Application prompts user to click “Emergency Contact Information”, “Notifications”, or “Return” (Figure 1.2)
3. If user clicks “Emergency Contact Information”

3.1. Application prompts user to click “Update Contact Information” or “Return”

3.1.1. If user clicks “Update Contact Information”

3.1.1.1. User can input Name and Phone Number for their emergency contact

3.1.2. Else id user clicks “Return”

3.1.2.1. Application returns to the “Emergency Contact Information” page

1. Else if user clicks “Notifications”

4.1. If notifications are already turned off

4.1.1. User can swipe notification switch to “ON”

4.2. Else if notifications are already turned on

4.2.1. User can swipe notification switch to “OFF”

1. Else if user clicks “Return”

5.1. Application returns to the home page

**Entry Condition:**

1. User has the Security Camera system installed in the home
2. Security Camera PIN identifier has been activated by the administrator

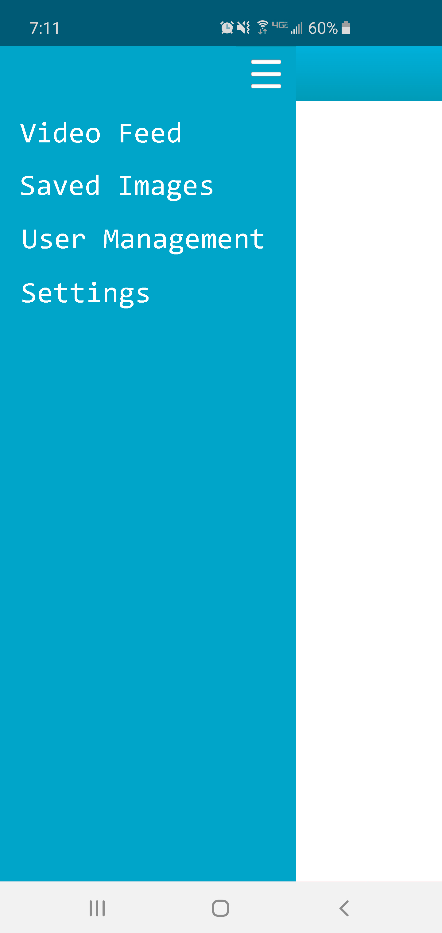
**Exit Condition:**

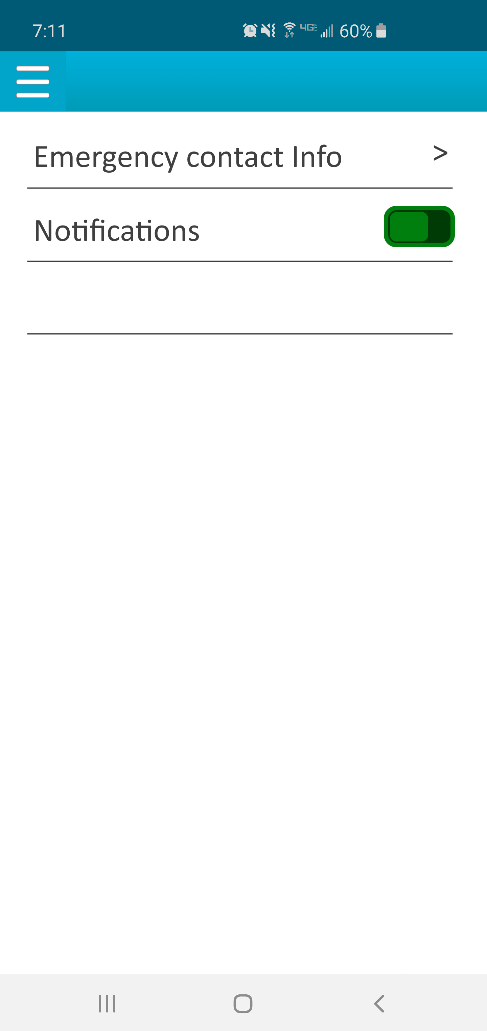
1. Application has saved all changes to any of the user’s personal information

**System Requirements:**

1. Immediate emergency contact should be 9-1-1, being unchangeable by the user
2. Contact information for a system administrator should be listed and unchangeable to the user
3. Notifications should automatically be “ON” after installation of the Smart Security Camera

**GUI Screenshots:**

**Figure 1.1: Pressing the menu button that appears in the top right of any of the different pages will open the navigation panel. This Panel allows you to quickly jump between any of the Apps Pages.**



**Figure 1.2: The Settings page allows the user to change the default emergency contact number, as well as toggle Notifications.**

**3.2.3. - Use Case 3**

**Name:** View Video Feed

**Actor:** User

**Path Outline:**

1. Main page interface prompts user to “View Live Video Feed” or “View Past Video Feed”
2. If user clicks on “View Live Video Feed” option

2.1. Application loads the live camera footage for user to view (Figure 1.3)

1. Else if user clicks on “View Past Video Feed”

3.1. Application displays list of past video feed, each timed for 24 hours and listed with options to delete or save (Figure 1.4)

3.2. User scrolls though the list manually and clicks on the desired date

3.3. Application offers the option to fast forward (2x, 4x, or 8x speed), rewind (2x, 4x, 8x, speed), or “Pause”

3.4. If user wishes to view video feed prior to the 7-day limit

3.4.1. The interface prompts user a “Request Footage from Administrator” option

3.4.2. If user clicks “Request Footage from Administrator”

3.4.2.1. Interface redirects user to “Contact System Administrator” page

**Entry Condition:**

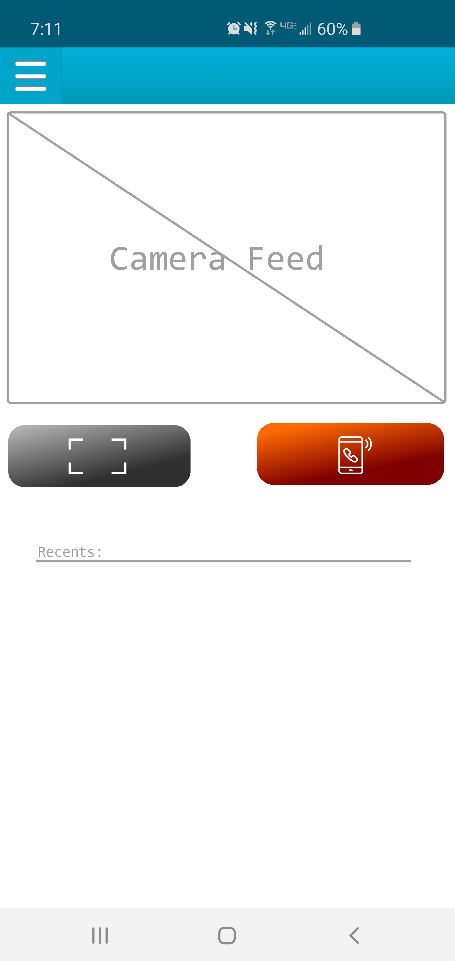
1. User has connected to the Security Camera to the phone application via PIN identifier

**Exit Condition:**

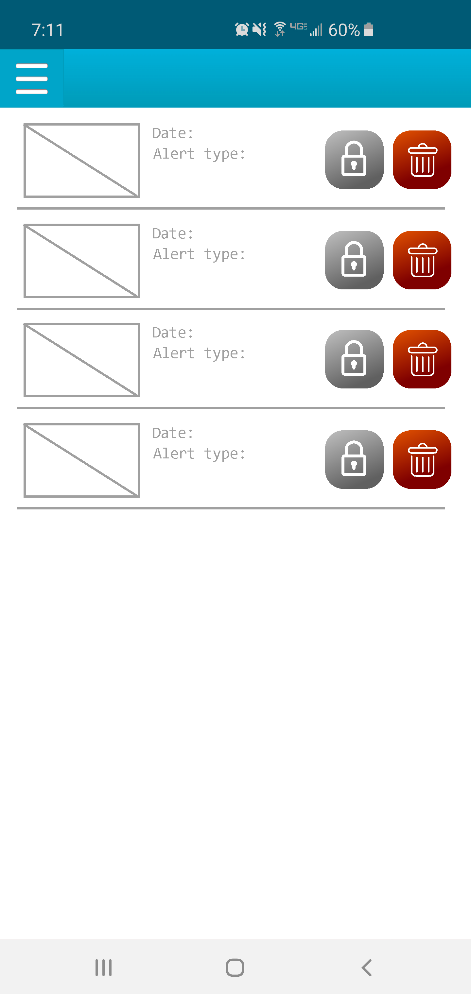
1. User has manually chosen to exit the video feed application interface via the exit option

**System Requirements:**

1. Security camera must always be able to display live video footage
2. Video stream must always be stored to the administrator database after the 24-hour mark
3. In order to maintain a reasonably sized storage space, video footage is automatically deleted from the database unless footage is manually saved by the user

**GUI Screenshots:**

**Figure 1.3: The Camera Feed Page is shown; This serves as the main Page whenever the app is restarted. This page includes a button to save a screenshot of what is currently displaying on the feed, as well as an emergency call button. The emergency call button initiates a call through the devices default Calling app to 911 or whatever the user has set as their emergency call number.**



**Figure 1.4: The “Recent” page displays a collection of video clips saved to the camera itself. The camera records a video clip from the live feed every time the system identifies a potential threat. Users can then use the “trash” icon to delete video clips, and the “lock” icon to prevent the system from deleting selected clips in the event the system is low on storage space.**

**3.2.4. - Use Case 4**

**Name:** Contact System Administrator

**Actor:** User

**Path Outline:**

1. User clicks on “Contact” option on the home page
2. Application lists “Contact System Administrator” option with phone number attached
3. Application lists “Contact System Administrator” option with email information attached
4. Application list a text box option for the user to report immediate issues

**Entry Condition:**

1. User must have registered their personal information into the application:
   * Phone number
   * Email address

**Exit Condition:**

**Requirements:**

1. Phone number must be listed as a hyperlink which automatically calls when clicked on
2. The listed email must be listed as a hyperlink which automatically allows user to type an email
3. Text box option must be connected to the system administrator for punctual response
4. Any contact information listed must not be changeable by the user

**3.2.5. Use Case 5**

**Name:** Respond to User in Contact

**Actor:** Administrator

**Path Outline:**

1. Administrator terminal menu displays a notification of a user in contact
2. If user is contacting through telephone

2.1. If there is another user on the line

2.1.1. Place user on hold

2.2. Else administrator picks up the call to address user’s needs

1. Else If user is contacting though email

3.1. Administrator addressed user needs through email

1. Else if user is contacting through chat system

4.1. Administrator responds to user’s need on the chat system

**Entry Conditions:**

1. User has contacted an administrator via any available contact methods
2. There is an administrator present for communication at any hour of the day

**Exit Condition:**

1. Administrator has successfully addressed the full needs of the user
2. If administrator is contacted via telephone, the user has hung up on the administrator

**System Requirements:**

1. Administrator must respond to an email within a 24-hour time period
2. Administrator must always be active in the chat system

**3.2.6. Use Case 6**

**Name:** Manage System Database

**Actor:** Administrator

**Path Outline:**

1. Administrator clicks on the “Manage User Database” option on the terminal menu
2. Interface displays a list of users already registered in the database (Figure 1.5)
3. Interface prompts administrator to “Add User”, “Remove User”, or “Search User”

3.1. If administrator clicks on “Add User”

3.1.1. Administrator inputs new user’s name, address, telephone number, and Camera ID

3.1.2. Administrator saves new user information to the database

3.2. Else if administrator clicks on “Remove User”

3.2.1. Administrator searches for user information

3.2.2. Administrator clicks on the user information in the list

3.2.3. Administrator removes user from the database

3.3. Else if administrator clicks on “Search User”

3.3.1. Interface prompts administrator to search by “Name” or “Camera ID”

3.3.2. Administrator clicks on user information

3.3.2. Interface prompts user to “Update User Information”

3.3.4. If administrator clicks on “Update User Information”

3.3.4.1. Administrator has the choice to update a user’s name, address, or telephone number

3.3.4.2. Administrator saves new updated information to the database

**Entry Conditions:**

1. Administrator has logged in to the terminal menu with a personal PIN identifier

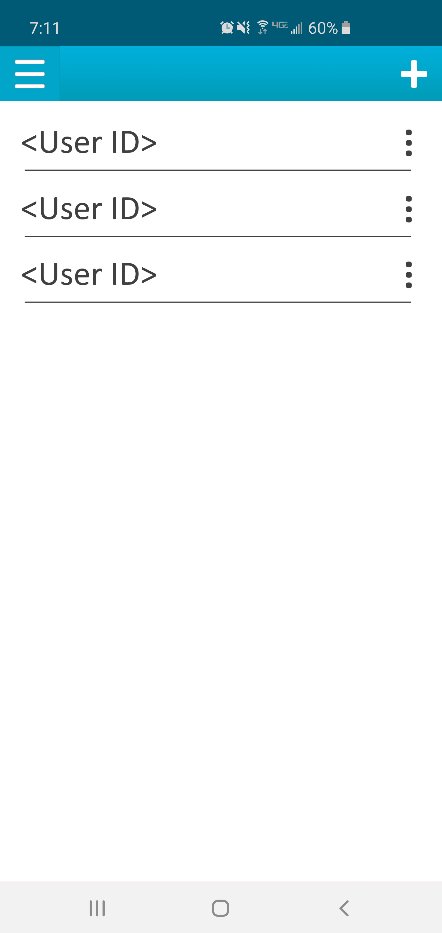
**Exit Conditions:**

1. Administrator has successfully addressed every user in contact prior to logout
2. Administrator has logged out of personal terminal menu access

**Requirements:**

1. When adding a user, the PIN of the security camera must be activated in order to register
2. When removing a user, an administrator must have user permission to do so

**GUI Screenshots:**



**Figure 1.5: The “User Management” page available to admins Lists all the smart devices that are linked to the camera and allow the admin to add/remove users as well as control what users have access too.**

**4. Non-functional requirements**

**4.1 Reliability:**

4.1.1. Video Functionality:

One area that could cause issues is the system will need to stream video simultaneously. In order to guarantee performance during normal use the number of available connections to the system is held to 5 different devices. The system will also be able to adjust quality of streaming video in order to guarantee functionality. During these times the system will still record at full resolution.

4.1.2. Event Detection:

Under normal circumstances the system will be able to differentiate movement and directionality. It will determine the heat signature of the object, and determine whether it is living, or non-living. It will then determine whether it is human or not, and if the event it is within the set of reportable events. If so, the system will report the event to the related users. To increase the processing time and reliability of reports the system will focus on its ability to differentiate humans and the objects they possess.

**4.2 Robustness:**

When the system is working under unexpected conditions (for example: power outage, no internet connection, the inability to report events, or simultaneous events) the system will remain functional.

4.2.1. Power outage:

In the case of a power outage, power use will transfer to the unit’s backup battery. Functionality will decrease during this time to maintain prolonged event detection. Admin users will be notified when a power outage is detected, as well as when the unit is in its final 20% of backup battery power. Priority events will still be recorded during power outages.

4.2.2. Connection Failure:

In event of an internet connection failure and/or inability to report events the system will continue to record events and enqueue the event notifications that were not received. During this downtime the system will attempt to reconnect and/or resend notifications at a 30 second interval and reset after a limit of 10 attempts is reached, a total of 5 minutes.

4.2.3. System Failure:

In cases of system failure the device will attempt to restart in order to regain functionality based on the error code. If unable to regain functionality the system will attempt to notify administrators, the device will then hold in standby mode. If only partial system functionality is present the system will attempt to maintain maximum functionality given partial failure.

**4.3 Performance:**

In developing the system, the major constraints noted were with system storage, streaming speed and event processing.

4.3.1. System Storage:

We decided a priority be given to most recent and priority events. The video quality for storage will be determine based on ability to store up to 100 incidents of 5-minute length at any given time. Video will be stored for one week, unless storage is full, at which point the oldest events with least priority will be removed. Video recordings will be removed from storage after 7 days from recording date, unless marked to be saved by an admin.

4.3.2. Streaming Speed:

The quality of service is heavily dependent on the internet the device is streaming over. As this is not a variable we will be able to control, we will have multiple different streaming qualities depending on the quality of internet available. In order to increase performance, streaming quality will be initially determined by the connection strength, and further refined depending on number of users accessing the feed [1].

4.3.3. Event Processing:

The main bottleneck that will affect processing time is during event analysis and threat detection. The way in which we will combat this issue is by processing events incrementally determining specific qualifying factors to determine if further analysis is required. The cases with the highest priority and possibly most computational power and speed decrease is object determination and type of human event in progress. Utilizing presets of the most likely models will help to speed up this analysis by utilizing a pipeline methodology to analyze events and the objects within that interaction simultaneously. The final threat determination will be based on each object individually and finally the full scenario. If at any point, there is a determined pre-specified event or threat the analysis sequence can be exited based on priority.

4.3.4. Compression:

As stated in 4.3.1. storage quality will be determined based on ability to store a certain number of recordings at any given time, compression will be determined based on size of hard drive of the unit allowing for multiple variations and product ranges. For direct streaming there is no need for compression as the stream is accessed directly, although encryption may affect quality of stream [2].

**4.4 Maintainability:**

The system will have multiple areas that may necessitate upgrades or maintenance.

4.4.1. Event and Object Library:

Utilizing a set of predetermined events and the scenarios and specifications of each, we could add to this library as new event types are determined. Using libraries of objects, we can easily add any new objects that may become necessary to identify and expand on the initial identifiable object set. This allowing for the system to be functional regardless of time or location. We will also be able to further refine the specification of events based on improvements in hardware or analyzing algorithm improvement.

4.4.2. Application Updates:

Utilizing the MVC model we will be able to adjust the user interface for any new versions of device software, or improved event list. The controller will not need to be changed with these improvements. This will also be beneficial if additional features and functionality need to be added to the application.

4.4.3. Hardware Integration:

Supporting a modular hardware system with the ability to support different sensor types and standards allows for replacement of deprecated hardware without replacement of the entire system. Treating each sensor as its own object is the best approach, allowing for wrappers to be utilized in order to integrate different manufacturers.

**4.5 Usability:**

4.5.1. Mobile Integration:

The application with be multi-platform for use on different mobile devices.

4.5.2. Application:

The application being mostly visually based will allow for ease of use and proof of functionality without extensive system knowledge. For example, if a user would like to view an event, they can either be directed from the notification prompt or through the related tab on the main application screen. If they would like to view recent events, they would use the recent section in the application.

**4.6 Security:**

4.6.1. User Verification:

One of the main issues regarding security that we encountered when developing the system is that of unique user verification and management of trusted users. The approach we have decided to take is the utilization of unique temporary pins that the admin will be able to input in their settings during new user creation. The pin will link to the individual device of that user and that unique device will then be added to the whitelist for that device. After being added to the whitelist the device will be able to access the system remotely through the application. Utilizing a whitelist mapped around unique identifiers as well as limiting the number of users helps to combat unwanted traffic to the system.

**5. Design and Implementation Constraints**

**5.1. Standards compliance:**

5.1.1. Industry Standardization:

Depending on client’s preference, the system will either work within ONVIF or PSIA standards in order to allow integration with other products utilizing the same standardization [3].

5.1.2. Encryption:

Secure data transmission and authentication will utilize WPA3 standards, while still allowing WPA2 connections, allowing the device to be future-proof by for the foreseeable future.

**5.2 Determining Unique Identifier:**

In order to add a new user, the user will need to download the application, at which time the application will need to determine the unique identifier for that device.

5.2.1. Cellular Devices:

For cellular devices we will utilize the IMEI number which remains constant with or without wi-fi connection and after a factory reset of the device. Utilizing a MAC address does not allow for verification over cellular network, and other identification methods are not cross-platform.

5.2.2. Non-Cellular Devices:

For non-cellular devices, after installation of the application, the MAC will be determined and used as the unique identifier for that device. As wi-fi connection is necessary for utilization of the application and the device does not have cellular capability, the MAC address will be suitable for this purpose.

5.2.3. Failure to Identify:

If the user decides to decline the application’s request to determine a unique user identification by these methods, or the application is unable to determine the unique identifier, the application will not be able to verify the user and the user will be unable to access the system. This identification process is necessary

**5.3 Development constraints:**

5.3.1. Hardware:

For full system functionality care must be taken in determining hardware compatibility between multiple sensors and the effect different component specifications will have on the performance of the system. Event analysis being the largest perceived bottle neck may require hardware modification and integration into the event processing pipeline in order to maintain necessary detection speed of events.

5.3.2. Encryption Design:

In order to stay within the standards of the WAP3 guidelines certain parameters must be considered during the development process of the system as well as the hardware requirements needed to achieve that functionality. The ability to work within a WPA2 network during the transition to the new standard will allow for immediate use as well as use into the future without degradation of the system as a whole.

**6. References**

[1] S. Namal, K. Georgantas, A. Gurvot. “Lightweight authentication and key management on 802.11 with elliptic curve cryptography.” *2013 IEEE Wireless Communications and Networking Conference (WCNC),* p. 1830-1835. Apr, 2013. [Online] doi: 10.1109/WCNC.2013.6554842.

[2] Y. Jeon, Y. Kim, J. Kim, “Implementation of a video streaming security system for smart device.” *2014 IEEE International Conference on Consumer Electronics (ICCE),* p. 97-100, Jan, 2014. [Online] doi: 10.1109/ICCE.2014.6775925

[3] W. Li, Y. Gao. “Design of network camera based on **ONVIF** in the dark environment.” *2018 International Conference on Sensor Networks and Signal Processing (SNSP),* p. 84-87. Oct, 2018. *[Online] doi:* 10.1109/SNSP.2018.00025.