University of Puerto Rico
Mayaguez Campus
Electrical and Computer Engineering Department

Project Proposal for the

Security Guard Monitoring System

by

Prepared by:
Diana Carbia, Project Manager
Oscar Negrón
Miguel Resto
César Rodríguez
Roberto Santos

For: Dr. Miguel Figueroa and Dr. Nayda G. Santiago
Course: ICOM 5047
Date: Wednesday, February 13, 2008

Abstract

Security guards, closed circuit television, alarms, and other means of security are used to mitigate threats to people and property. Monitoring employees of security guard companies in such an environment becomes a very difficult task, since knowing their exact position at all times is not easy, let alone efficiently managing their attendance records. These factors lead to gaps in security at the client's sites, as unmonitored guards might disregard their duties.

To solve these problems and further ease security guard companies' work we propose the Security Guard Monitoring System (SGMS). The proposed system will track security guards during their patrols or at their assigned station, record their attendance without the need of conventional static systems such as punch cards, and provide guards with a secure messaging method, all in a GPS and Wi-Fi enabled portable device. Supervisors and administrators will be able to manage and track their employees through a web application.

Table of Contents

Figures Index

Tables Index

1. Executive Summary

1.1. Introduction

During years, security companies have had a lot of problems in the process of monitoring their employee's status, positions, and time logs of their assigned guard tour station. These companies have made innumerable attempts to maintain an accurate control of their employees by providing them with special equipment, such as radio communication and magnetic punching cards. Some companies have even evolved from the punching cards to new sophisticated devices that use specialized software to record each secured checkpoint, during guards' patrols. One drawback of these systems is that they do not provide a real time guard tracking solution [1],[2].

In order to mitigate threats to people and property, physical security must be in place. This generally consists of security guards, closed circuit television, and alarms, among other things. In physical security companies communication among security guards is vital. Generally, this communication is done by radio. These radio frequencies can be intercepted by burglars or can be heard by anyone close to a security guard. Another problem is that currently supervisors of security guards do not have a consistent way to know whether or not their security guard has visited different areas in preventive runs and don't have a reliable way of handling time attendance of their employees.

To solve these problems the Security Guard Monitoring System (SGMS) is proposed, which consists of a pager-like device that security guards will carry with them during their inspection patrols and a software counterpart that supervisors will use to monitor the activities of security guards during these inspections. The system is a high-tech replacement to the traditional punch-card clocks used by security personnel to handle time attendance and activity logging. It does not pretend to replace the traditional radio device, but add an extra layer of protection and communication to the current security guard systems.

The SGMS device will provide a messaging system that will let the employees send and receive messages to and from a computer administrator by means of a small pager-like device. This will be used to notify the security guards of important news, emergencies, reports, among other important information during patrol. The guard will also have the ability to send coded messages using a numeric keypad akin to the traditional 10-code system (e.g. 7 represents "out of service", 20 represents "specify your location"). Our closest competitor does not provide a keypad in their device; only four input buttons [3]. The device will have a GPS that will send its position to a receiving server constantly, letting any user of the web application to monitor employees without any problems. Every device will have a unique number that will be used to identify them in a device map tracking system.

The SGMS administration program will be a web based software that will have a database containing information of all the employees, devices, and tracking information on the system. This web page will have a device map tracking system that will enable an end user to know the exact position of an on-shift security guard. It will be used to manage the employees on the system. The supervisors, as well as the security guards on a static area (such as an entrance gate), will be able to add and delete employees from shifts, assign guard patrol stations and devices, monitor position, and send and receive instant messages and emergency alerts. It will also enable supervisors to add, edit, or delete employees from their roster. In addition, the system will provide a time attendance application that will log access to secured areas and employee attendance.

This project will help make management of physical security assets easier and more secure. The uniqueness of this project lies in that currently most companies handle the problems mentioned above by radio communication and paperwork. There should be a robust and automated log of everything that a security company is doing and this is not available in most of the current systems.

1.2. Market Description

1.2.1. SilverGuard Security Guard Monitoring Systems

Brokling Computer Systems have their own Security Guard Monitoring System, which consists of specialized electronics and software components that are used to monitor security guards during their patrols. This hardware only replaces the punching card and time clock methods used to secure checkpoints during the security guards inspection patrols. When a security guard ends his or her shift the patrol information is sent via Data Transfer Station to a computer for storing, directly to a printer or to a Central Monitoring Station.

1.2.2. GuardWatch: Guard Patrol Monitoring Systems

GuardWatch is a security management tool used to monitor the patrolling activities of security guards. GuardWatch consists of electronic devices that are carried by the security guards to swipe in specific checkpoint stations to record time, date and location in which they passed through a checkpoint. The information recorded in the device can be transfer to a computer with GuardWatch specialized software.

1.2.3. GuardTrax

GuardTrax is a system to monitor security personnel. The device uses Global Positioning System (GPS) to acquire the location and position of a security officer on duty. The unit gathers other important data points (motion, time, heading, speed etc…). Then, using the GSM wireless network, GuardTrax transmits that data to a remote server. The server processes and sends the data, by posting it to a map-based (GIS) application that includes satellite imagery, or sends an email or text message to pre-determined supervisors.

1.3. Document Description

This document presents the proposal of the Security Guard Monitoring System. It will discuss the existing problems that are present in the actual security guard systems, and solutions to resolve them. There is a detailed explanation about the functionality of the system, the deliverables and milestones, its complete hardware and software design, and its relevance.

A work breakdown structure has being created, in which all members of the team have equally distributed all work, in two variables: time, and personnel. There is also the presentation of a risk mitigation, monitoring, and management plan for every relevant risk of the project, so the team is able to prevent them, and in case of materialization, control the damage.

On the other hand, a background of the personnel that will work in the project is included, with their responsibilities on the project, their past experiences, and their professional level. There is also the provision of a realistic budget for the project, including salaries, and benefits for our personnel.

2. Proposed Solution

2.1. Objectives

In order to improve the productivity of the guards in the security guard companies, C Group Engineering Solutions Company proposes the Security Guard Monitoring System (SGMS). C-Group Engineering Services aims to complete these concrete tasks as a measure of a successful execution:

- Provide an initial prototype of both hardware and software components and all technical documentation related by March 26, 2008.
- Provide a complete prototype with all stipulated components and user manual of the system by May 2, 2008.
- Not exceed $600 on the cost of hardware components for the prototype.

2.2. Relevance

Preventing security guards from committing fraud has become a very strong concern for security guard companies [7]. This system will give people better confidence to security companies, as they will know security guards are checking on the assigned areas as they are been directly monitored by supervisors. It will also provide a more secure environment for the on field security guards because they will be able to automatically provide their positions, in case of any emergency. In addition, the system will reduce great amount of paperwork by storing every log on the system and with this help the environment by saving trees. It will also help the environment by replacing the use of magnetic cards for checkpoint punches by deposition of non biodegradable materials.

2.3. Scope

The Security Guard Monitoring System project is based on the design and development of a unifying tool for the traditional security company system. The majority of these companies utilize a radio communication to maintain informed of status and positions of the on field security guards and the signing of papers or the passing of a magnetic card in a checkpoint or assigned vigilance area to report their attendance. The goal of the proposed system is to enable security guard supervisors to keep track of the on field security guard by means of a real time device tracking system application that will receive the exact coordinates of a pager-like device that will contain a GPS. In addition, they will be able to send and receive messages to and from security guards, and maintain personal and work information about each of them by means of an administrative program that will store data in a database.

The Security Guard Monitoring System will be divided into two major development areas: Hardware Implementation and Software Implementation.

2.3.1. Hardware Implementation

The Hardware implementation of the system will be a pager-like device that will consist of a LCD, a numeric keypad, a Wi-Fi module, a GPS module, a real time clock, a buzzer, and a vibrating module. This device will be capable of receiving text messages and displaying them on an LCD. The end user, in this case a security guard, will be able to send coded messages from the device through a keypad. The GPS module will be used to find the device's exact position. All information will be sent and received to and from a server through a Wi-Fi module.

2.3.2. Software Implementation

The Software implementation will be based on an administrative web page. This page will consist on the management of all the security company information regarding the employees (security guards, and supervisors). There will be two different kinds of modules for this page depending on the employee rank: the supervisor module, and the security guard module:

2.3.2.1. Security Guard Module - The security guard module will have limited access to the web page. Security guards will not be able to manage employee profiles, but only their own system passwords for the log in page of the application. Even though it will be limited, it will permit the security guards to check in and out other security guards from shifts, send and receive messages to and from devices, see the device map tracking system, and search for other employees, and access their emergency information.

2.3.2.2. Supervisor Module - The Supervisor Module will have full control of the web application. A supervisor will be able to add, edit, and delete employee profiles, checkpoints, devices, codes, send and receive messages, and access the device map tracking system. They will also be able to view the time attendance logs of their employees, and every other log made, that will be mapped to the pertaining employee. The only limitations for supervisors will be to delete themselves from the list of employees, delete the default administrator, and change their own rank in the system.

2.3.3. Other System Features

2.3.3.1. Restricted Access - The administrative web application will have a protection against public view. This is, no unauthorized person will be able to enter the page, since a username and password will be required to log in. Only supervisors will be able to create new accounts that will

generate a random password that can be changed by the new user of the system.

2.3.3.2. Access by User Rank - The system will have to different sections; each of them will be accessed depending on the rank of the end user. This will be a security measure to protect the identity and private information of every employee of the system (security guards, and supervisors).

2.3.3.3. Documentation - As the system is being developed, documentation of every step in the process will be available online on the following web page: http://www.ece.uprm.edu/~s031066. In addition, software and hardware user guides will be created containing explanation of the system functionalities in a step by step format.

2.4. System Limitations

The Security Guard Monitoring System does not intend to replace radio communication; therefore such solution is not included. Instead, it will be left to security companies to decide whether or not it is necessary for them to include one. The radio communication will be an upgrade for the system, and will be considered in future implementations.

It will store information of logs and activities for each security guard in its profile. This will include working shifts and hours. The supervisor will be able to view these logs, but will not be able to export them to a payroll system. This system is not intended for payroll purposes. A payroll management system could be considered for future upgrades and implementations of the system.

As there has been a great evolution of wireless technologies, C Group Engineering Solutions has decided to develop the system to work on an area in which wireless network is available. For this reason, the Security Guard Monitoring System is limited to be used only inside these exclusive areas.

2.5. Required Activities

To accomplish the full development of the Security Guard Monitoring System, the team has decided to carry out the following activities:

- Install all necessary software for development:
  - ✓ IAR Embedded Workbench
  - ✓ MySQL Server
  - ✓ MySQL GUI Tools
  - ✓ Red Hat Development Studio
  - ✓ Apache Tomcat
- Prepare an area for the mounting of a prototype for the pager-like device, that will include the following development tools:

- ✓ Oscilloscope
- ✓ Power Supply
- ✓ Multimeter
- ✓ Soldering Kit
- ✓ Electronics Tool Kit
- ✓ Magnifier Lamp
- ✓ Alligator testing Cables
- ✓ Oscilloscope testing cables

- Create an ER diagram that will be used to design a relational database.
- Create a MySQL database that will be used for storing the personal information of every user of the system. It will also be used to store the logs of every security guard, messages, checkpoint reports, and any kind of emergency situation.
- Create a Web application using the Model-View-Controller (MVC) design pattern. This page will be implemented using the Java programming language. Specifically, Java Servlets, JSP, and Java Beans as the major building blocks to build the application.
- Build up a model for the SGMS prototype development that will include block diagrams, and schematic diagrams. These diagrams will be used in the selection of hardware components, and to make a part list for ordering them on time, with respect of the proposed schedule.

2.6. Schedule

The schedule for the project has been divided based on the deliverables. The team has been divided into two major development areas; hardware and software. Diana Carbia, Miguel Resto, and Oscar Negrón will be working on the SGMS web-based application. Cesar Rodríguez and Roberto Santos will be working on the hardware device of the SGMS. The milestones of the project have been set as the due dates of each of the deliverables. The following table summarized the high level phases that encompass each of the tasks for the deliverables and culminates with the due date milestones.

Table 1: Deliverables schedule

Deliverable	Duration	Start	Finish
Project Proposal and Oral Presentation I	21 Days	Tue 1/15/08	Wed 2/13/08
Software Prototype	44 Days	Thu 2/14/08	Fri 4/25/08
Device Prototype	44 Days	Thu 2/14/08	Fri 4/25/08
Progress Report and Oral Presentation II	4 Days	Mon 3/24/08	Thu 3/27/08
User Manual	1 Days	Mon 4/28/08	Mon 4/28/08
Final Report	4 Days	Tue 4/29/08	Fri 5/2/08
Final Project Presentation	4 Days	Mon 5/5/08	Thu 5/8/08

The deadline dates for the milestones are part of the contractual agreement between C Group Engineering Solutions and the customers.

2.7. Work Breakdown and Distribution

2.7.1. Work Breakdown Structure

The following work breakdown structure displays the tasks assigned to the completion of each of the deliverables. The description of the main tasks to achieve the project has been detailed in the Proposed Solution section of this document.

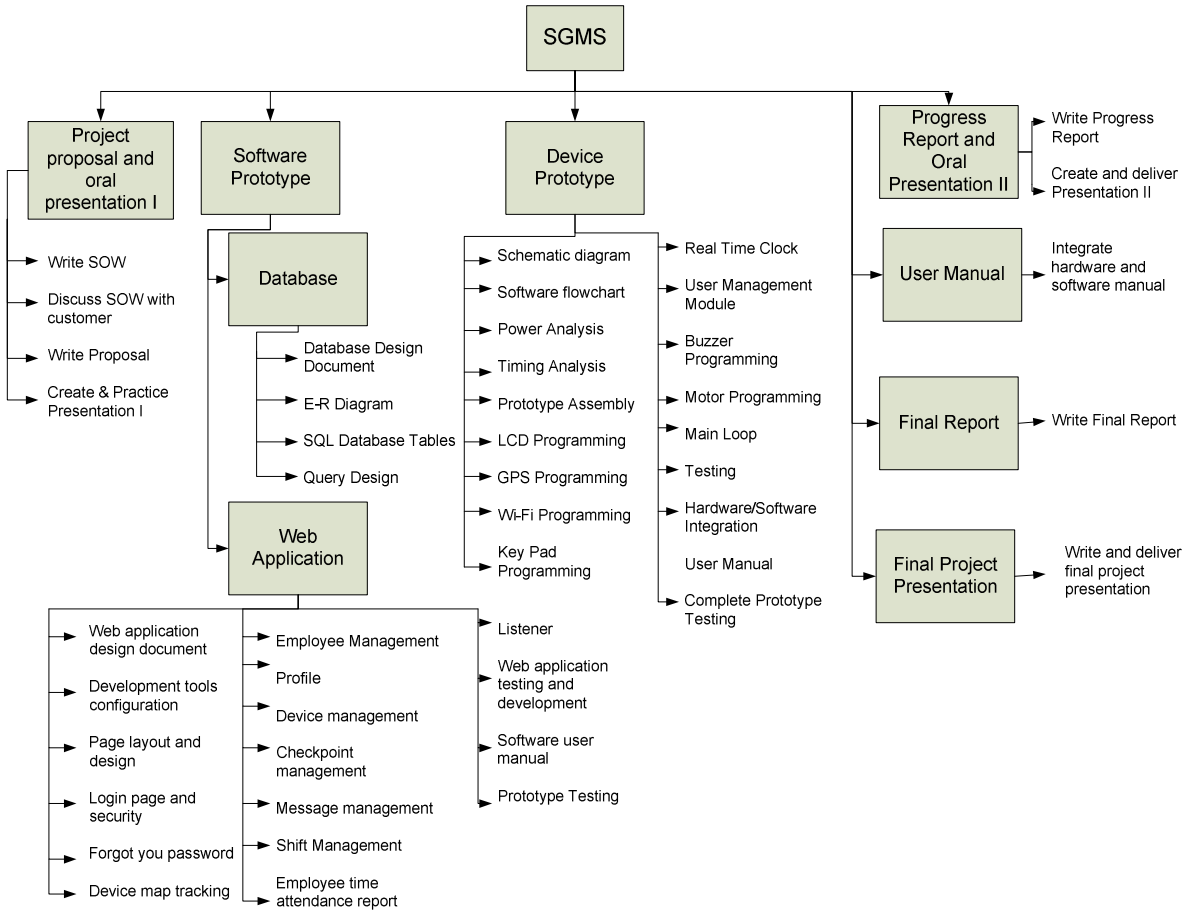

Figure 1: Work Breakdown Structure

2.7.2. Work Distribution

The following charts show the work division among the different deliverables of the group members. Detailed task-based distribution will be included as Gantt charts.

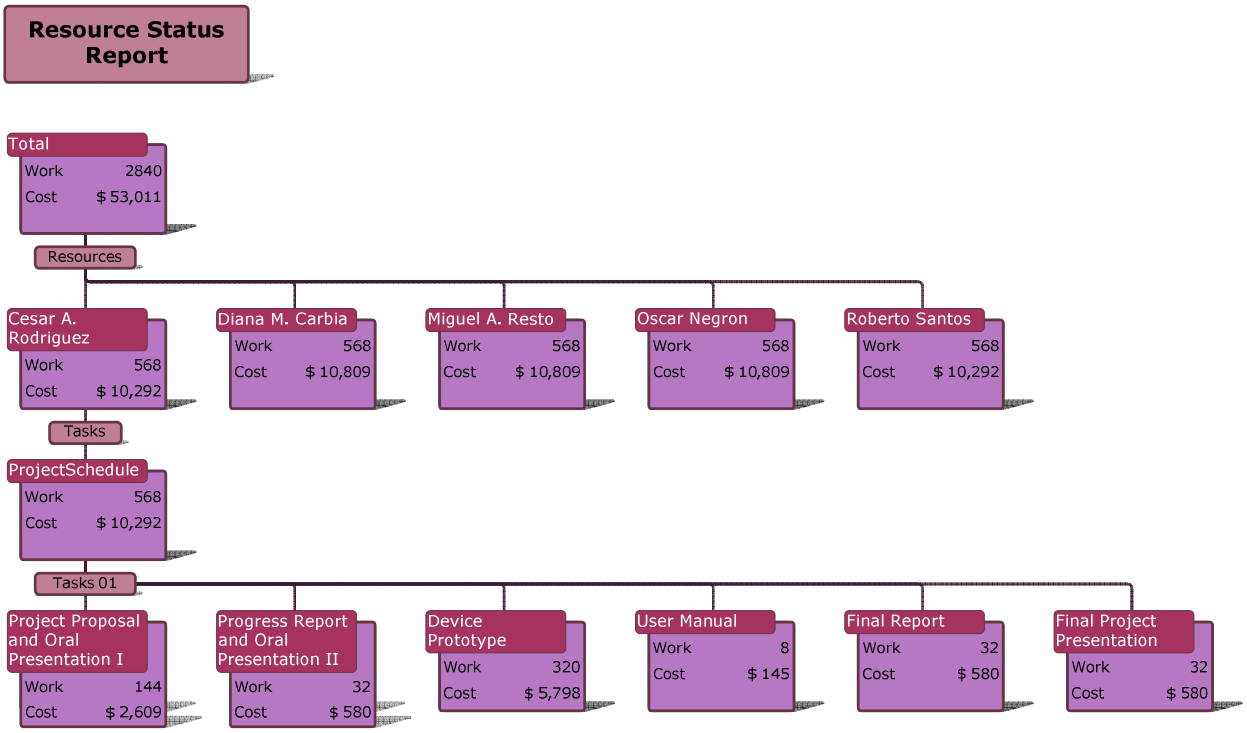

Figure 2: Deliverable resource breakdown for César A. Rodriguez

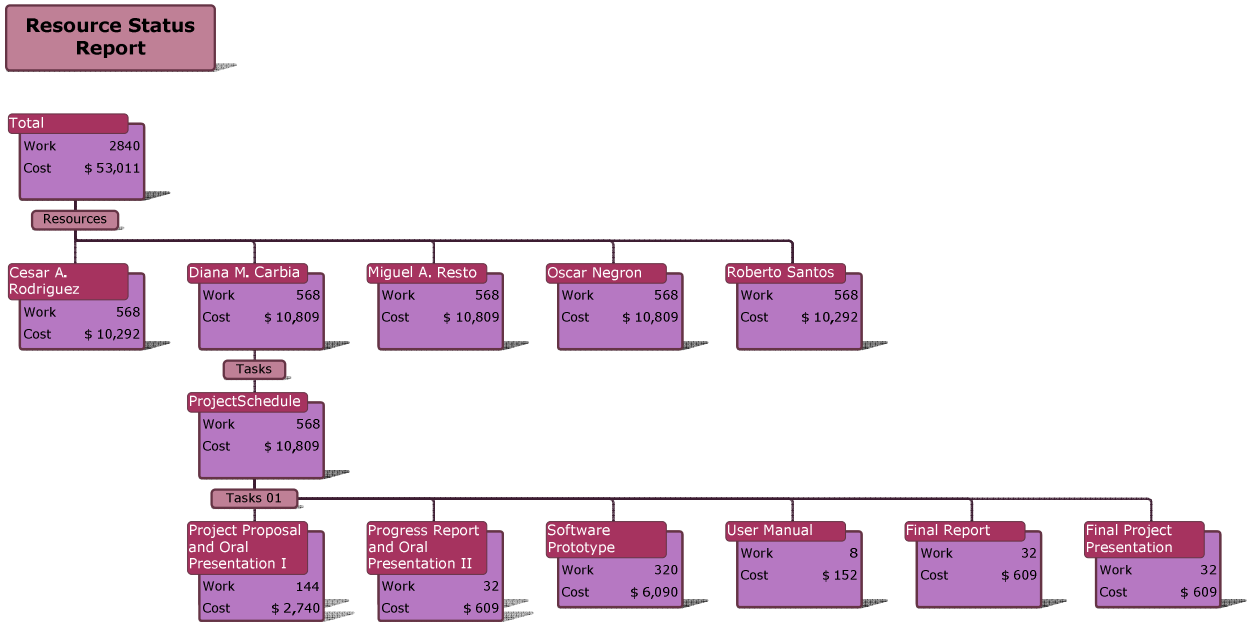

Figure 3: Deliverable resource breakdown for Diana M. Carbia

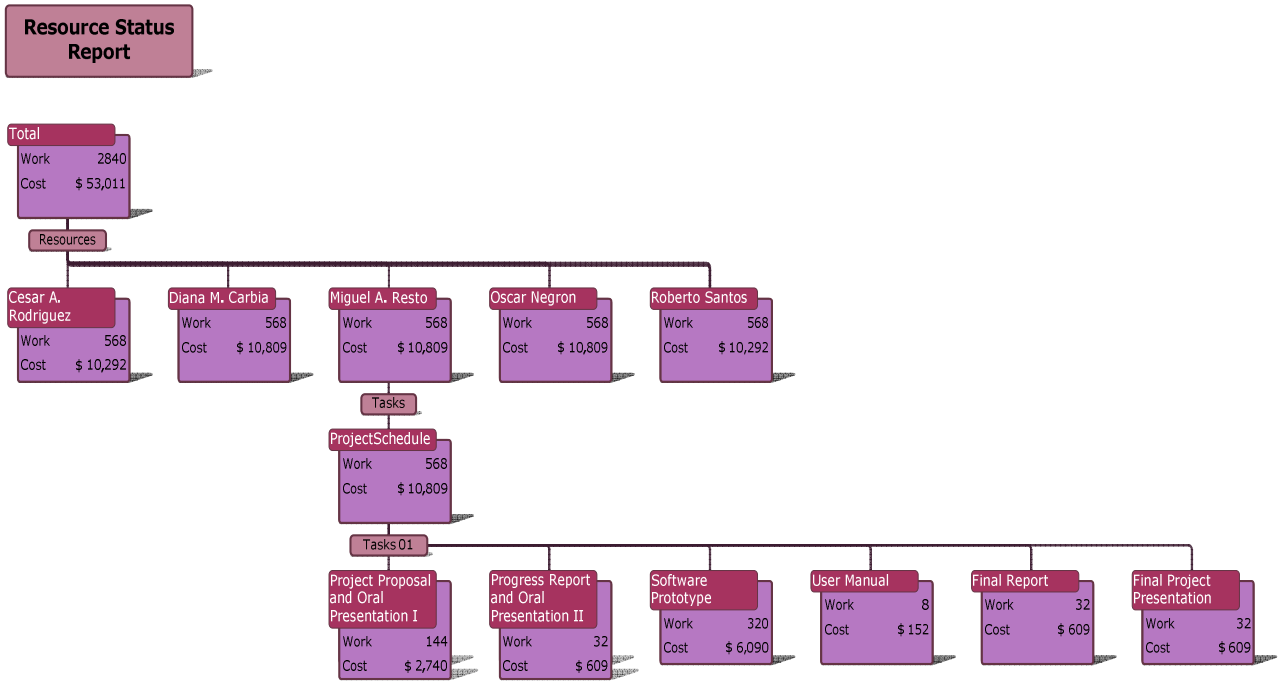

Figure 4: Deliverable resource breakdown for Miguel A. Resto

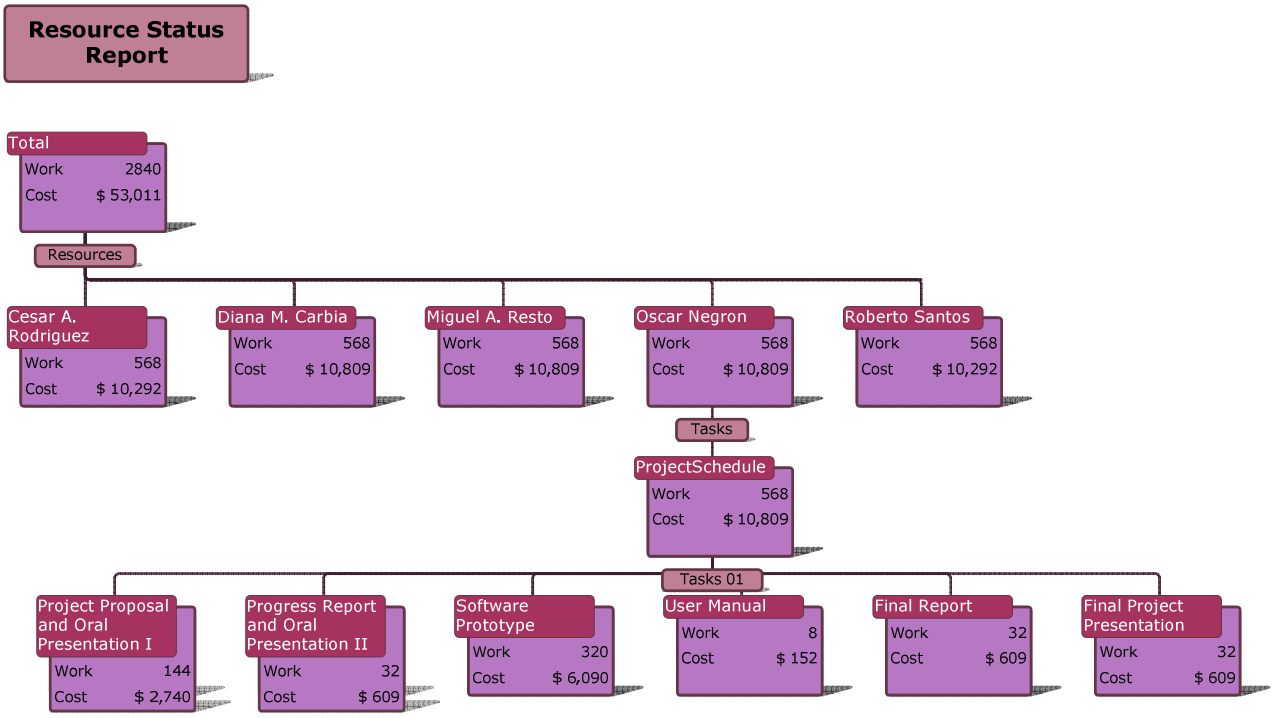

Figure 5: Deliverable resource breakdown for Oscar Negrón

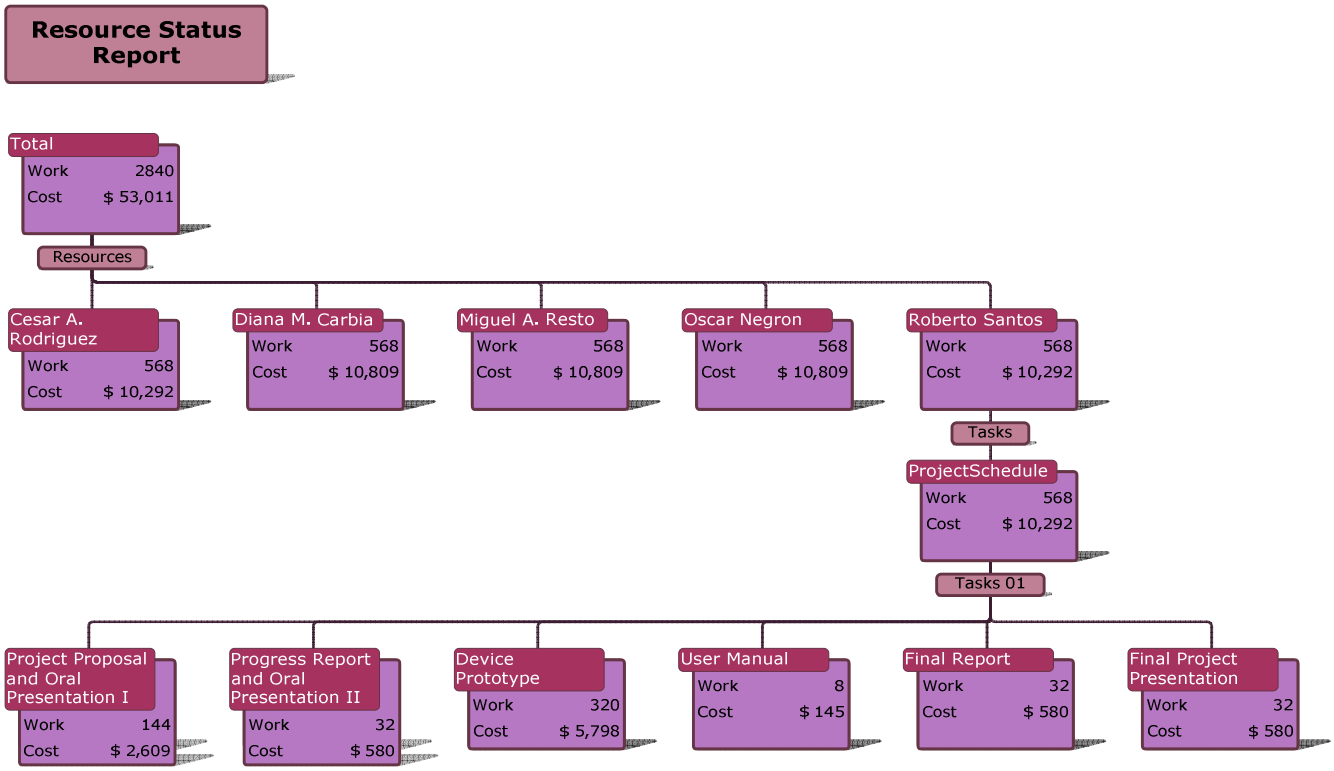

Figure 6: Deliverable resource breakdown for Roberto Santos

2.7.3. Gantt chart

The Gantt chart of the project has been created using MS Project 2008. This software was used to create the tasks and set their respective durations. The tasks were assigned to specific team members.

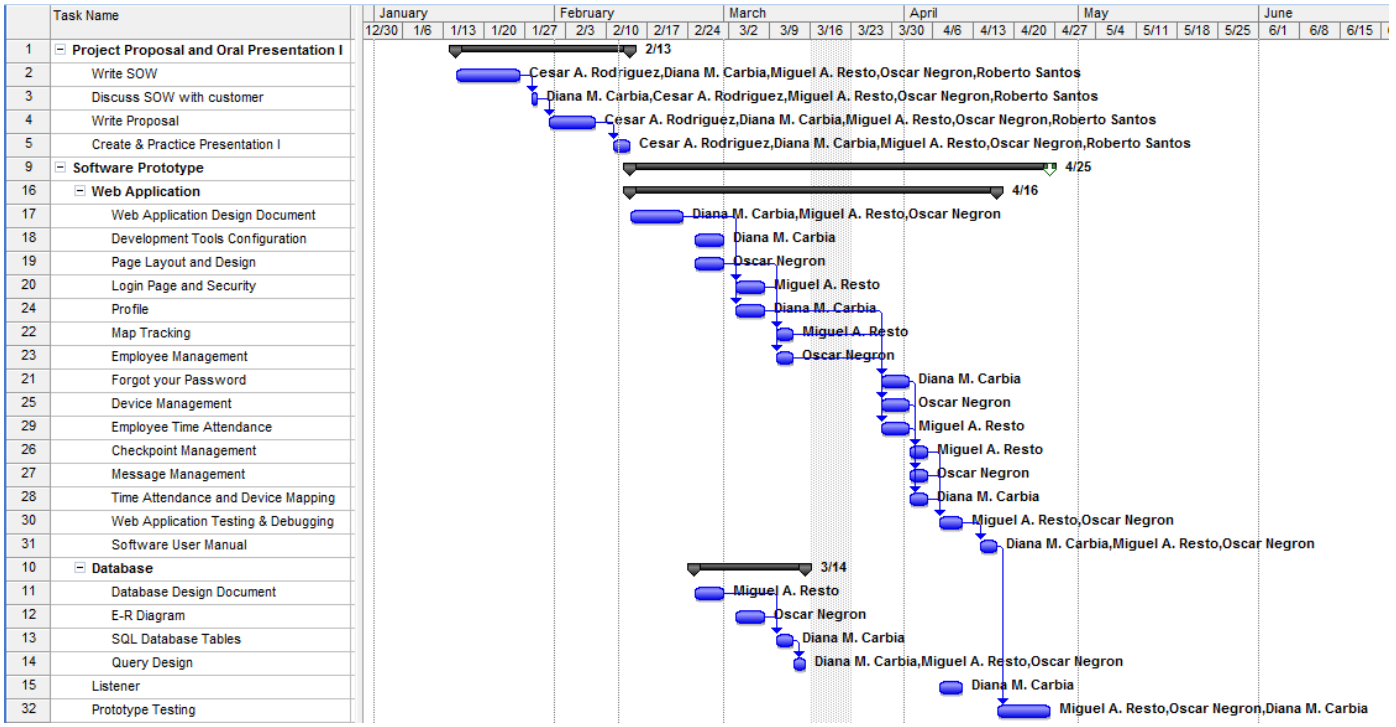

Figure 7: Gantt chart (part 1)

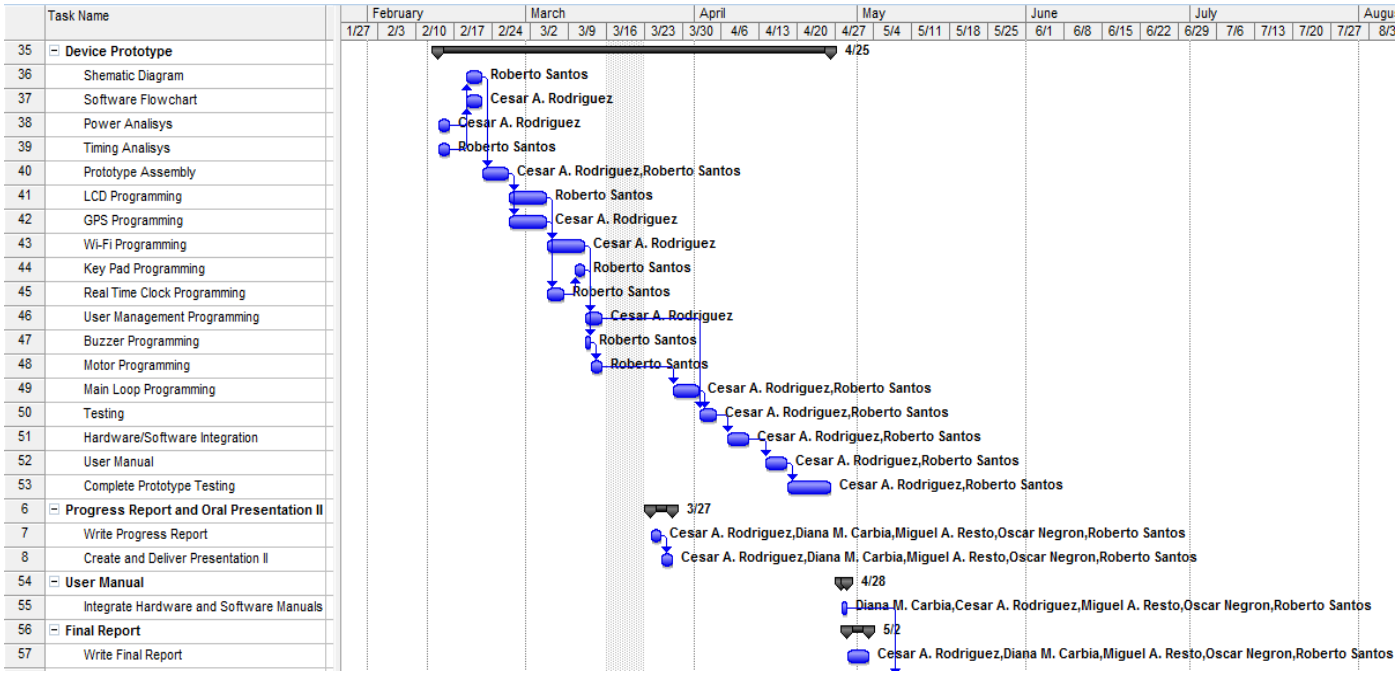

Figure 8: Gantt chart (part 2)

3. Design Specifications

This chapter describes in more detail the specifics of the three main aspects that compose the proposed design: hardware, firmware and software. The hardware and firmware specifications correspond to the hardware components proposed in the design and their driving software. The software specifications correspond to the web application backing the portable device.

3.1. Hardware Specifications

3.1.1. Hardware Components

3.1.1.1. Microcontroller – Texas Instrument's MSP430F149 microcontroller was selected as the brains of the design. The main reasons for this are that it is a very low power microcontroller, it provides several general purpose I/O ports, two USART modules, the team already has a knowledge base on it, and there exists ample support and examples of use. The microcontroller will be in charge of all interaction among the different components of the project as well as saving configuration information in its memory.

3.1.1.2. GPS Module - A GPS module will be used to locate the device's position on earth. The coordinates will be captured from the GPS module and sent to the command center's server using the Wi-Fi module. The GPS module connects to the microcontroller using the RS-232 protocol.

3.1.1.3. Wi-Fi Module - The Wi-Fi module displayed in the block diagram will be used to communicate between the device and the server by means of TCP/IP. Upon initial setup of the device the Wi-Fi connection will be configured to be encrypted (WEP, WPA, etc.), to use DHCP or static IP, and other settings. It interfaces with the microcontroller with the RS-232 protocol.

3.1.1.4. LCD - The graphic LCD is used to display information to the security guards during regular use of the device. The Home Screen will display the current time, date, and a notification of text messages sent from the command center. Security guards will have the option to send 10-code messages.

3.1.1.5. Numeric Keypad - The numeric keypad will be used by security guards to select messages to be sent and enter the necessary security codes (i.e., personal identification number)

3.1.1.6. RTC - A Real Time Clock will be used in order to keep the device's time even if it has been turned off. Initial time setup will use the time received by the GPS unit (offset to the local time from the UTC time).

3.1.1.7. Buzzer - This small audible alarm will alert the user of an incoming message. This feature can be set or unset by the user.

3.1.1.8. Vibrating motor - This tactile alarm will silently alert the user of an incoming message. This feature can be set or unset by the user.

3.1.1.9. Power supply - Though not depicted in the system block diagram, the system will be battery powered. The power source will be regulated so as to make it steady and reliable. This will result in less noise and more efficient power usage.

3.1.1.10. Reset - Within the system a small hard reset button will be included in case the device needs to be restarted.

3.1.1.11. Key lock Switch - A small switch will serve as a key-lock safety feature in order to avoid accidentally sending messages.

3.1.2. Firmware Specifications

The firmware programmed into the device will show the end user four main information screens, three of them accessible by the user and the other only appears upon an error situation such as messaging timeouts. Any of the screens will not accept input while the key-lock switch is engaged. The following is a descriptive list of the screens presented to the user:

3.1.2.1. Status Screen - This screen will show the current time, GPS and Wi-Fi signal status icons, and a new received message notification. This screen will automatically appear if the device has been idle for 5 minutes. Also, the display's backlight will turn off after 30 seconds of inactivity in order to save energy. From this screen users will be able to enter any valid 10-code value and send it to the base station, which in turn would forward the message to other guards in the area if necessary. The validity of these codes is checked by the remote server application.

3.1.2.2. Received Messages - This screen will list the last 10 received messages in descending chronological order (newest messages on top). The user will not have the ability to manually delete messages; the oldest message will be automatically deleted upon the receipt of a new one.

3.1.2.3. Settings Menu - Within this menu the user can set the audible (buzzer) and tactile (vibrator) alert preferences. These can be activated or deactivated individually.

3.1.2.4. Error Screen - This screen will not be directly accessible by the user and will only appear when a non-fatal system error occurs, such as failed communication with the server or timeouts.

3.1.3. Hardware Considerations

3.1.3.1. Power Supply - The device's power supply will be regulated using low dropout (LDO) step-down regulators in order to maintain a low-noise, reliable, and constant supply to all devices.

3.1.3.2. Noise Reduction - Signal noise will be managed through the use of decoupling capacitors placed between the power and ground pins for each

integrated circuit chip used (namely the microcontroller, GPS, Wi-Fi, RTC, and LCD chips).

3.1.3.3. Enclosure - The prototype will be large enough to hold the LCD and keypad, which are the largest items, exposed to the user, yet able to be operated using one hand. This leaves most of the space within the enclosure free for the microcontroller, batteries and other components. The enclosure will be made of plastic to avoid interfering with the GPS and Wi-Fi signals.

3.1.3.4. Reset button - A small hard reset button will be placed within the device in case the software hangs at some point during execution. This will also help during debugging.

3.1.3.5. User interface - The interaction with the user will be kept simple in order to distract the user as little as possible, calling for his or her attention only when needed (i.e., when a message is received). Maintaining a simple interface will also keep any training done by the company to its employees at a minimum.

3.1.4. Block Diagram

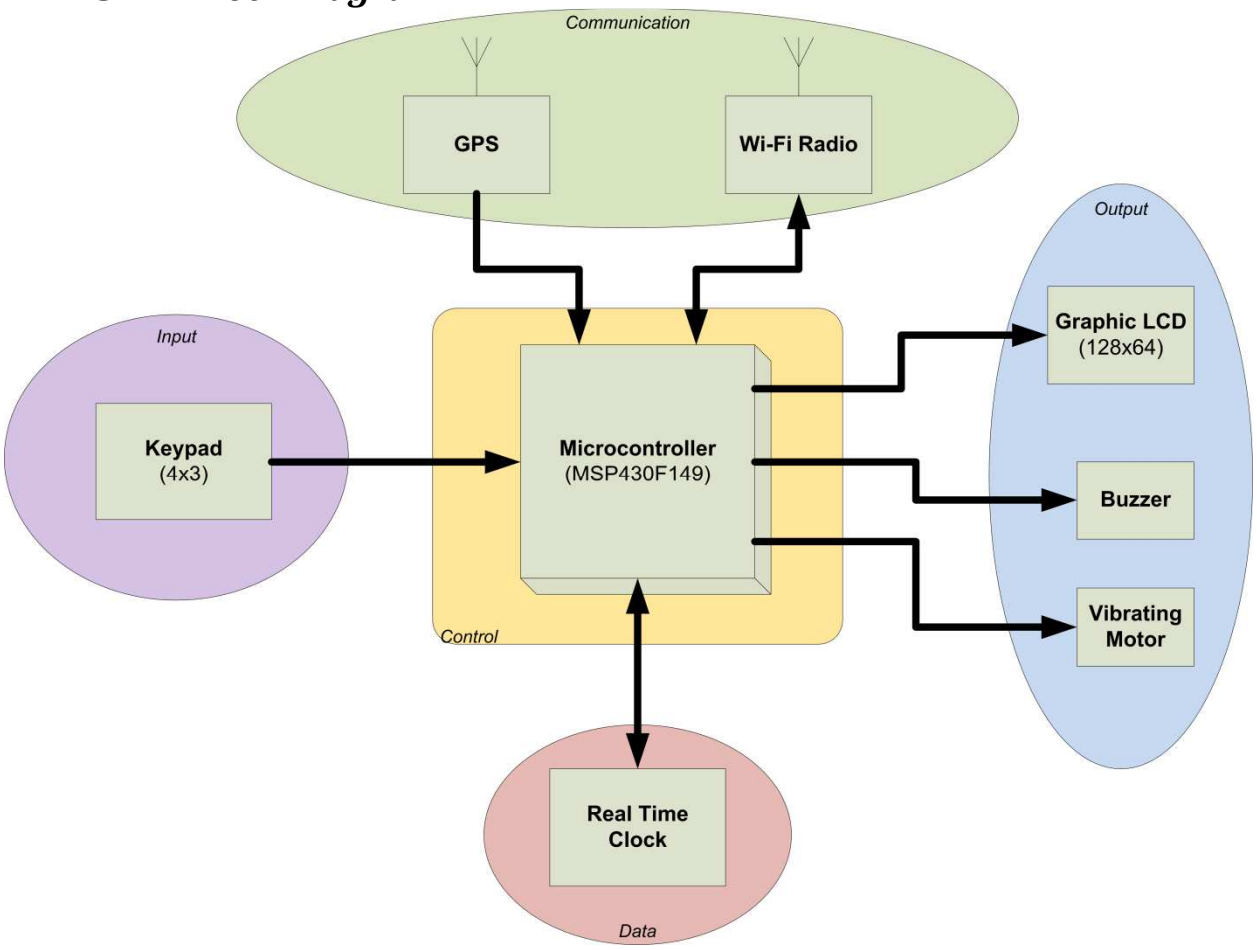

Figure 9: System level block diagram

3.1.5. Hardware Flowcharts

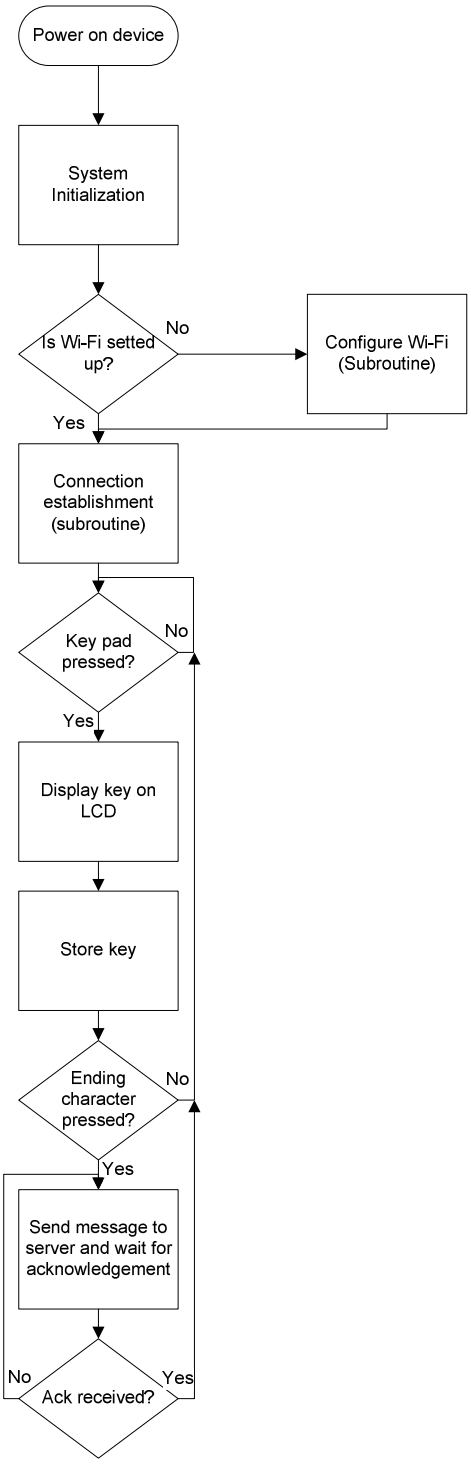

Figure 10: Portable device software flow

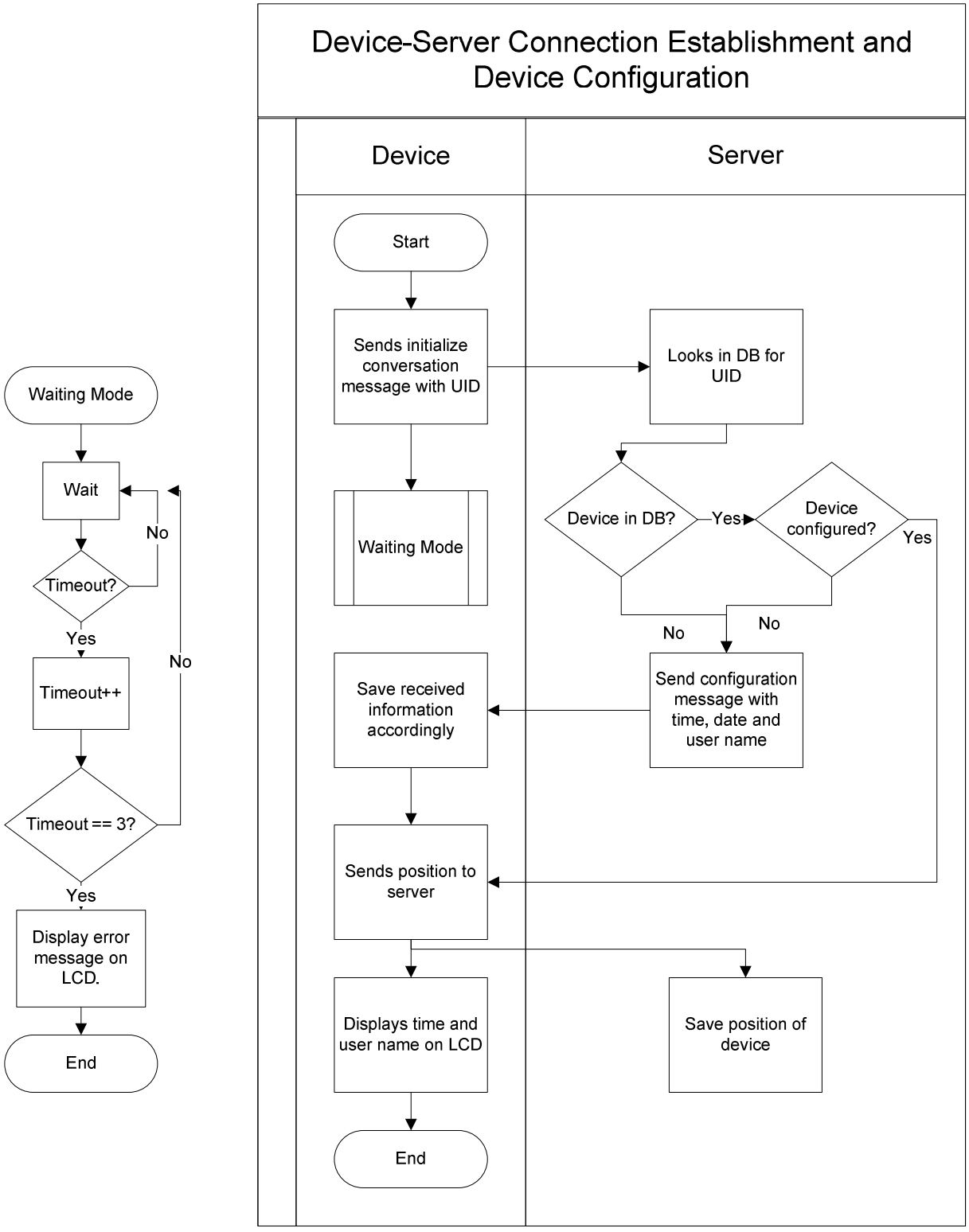

Figure 11: Portable device and server communication flow

3.2. Software Specifications

The Security Guard Monitoring System will have a web based application. This application will be used to manage all the administrative information (employees, time attendance, among others), and the monitoring of all the devices registered on the system. This program will have two different kinds of users: supervisors, and security guards. Certain modules and/or functionalities may be enabled or disabled, depending on the type of user.

In order to restrict the web application's entrance only to users that are authorized to access the SGMS web application, and to be able to detect which users make changes to specific things (e.g., deleting or adding employees), the web application will have a login page. Only authorized users of the system with the correct employee id and password combination will be able to access the page.

In case a user loses his or her password there will be a "forgot my password" page. Within that page, the user must provide the e-mail address he or she provided in his or her account profile to recover the account password.

After logging in, the user will be redirected to a home page. This home page will contain valuable information that will include which security guards are on shift, emergency alerts, among others. It is important to note that certain functionalities will be available throughout the entire page, indistinctively of the SGMS page he or she is navigating in or the user type (supervisor or security guard).

3.2.1. Functionalities available throughout the web page

3.2.1.1. Text Messaging

- This utility will let users send text messages to a specific device or to all devices.
- This will help users to send quick messages in disregard of the web page they are.

3.2.1.2. Left Hand Menu

- Used to avoid dead ends. [4]
- Displayed at the left-hand side of the screen.

3.2.1.3. New Message Notification

- Every time a code message is sent from a device, the web page user will be notified with a sound and a new message link.

3.2.1.4. Breadcrumb

- Its purpose is to give users a way to keep track of their location within the web application. [5]

3.2.2. SGMS Modules

The following modules will be available in the left hand menu described above. Each one of them is described in terms of user type: supervisor, security guard or both.

3.2.2.1. Device Map Tracking

Within this module both supervisors and security guards will be able to track in real time all on field devices using Google Maps. The user will be able to select if he or she wants to view a map of the area, or a satellite image of the area. Nevertheless, the size of the map and the area to be displayed will be configured when deploying the product at the customer site and it will depend on customer's specifications.

For easy identification of on field devices, each device will be represented by a marker in the map. The marker will be moving along the map each time the server receives new coordinates from the device itself. A green marker will stand for an on shift device with no problems, a blue marker will stand for a stolen or lost device, and a red marker will stand for a device from which an emergency message was received within the last 10 minutes.

By clicking any of the markers in the map the user will obtain more information of the device, such as the name and id of the employee that is assigned to the device.

3.2.2.2. Employee Management

The following information will be stored in the system for each employee: employee first name, middle name (if any), last name, employee id, rank (supervisor or security guard), e-mail, primary telephone, emergency telephone, address, additional information, username, password and photograph.

The employee management page will have a table containing general information about employees. The page will include the following options:

Supervisors:

1. **Add Employee -** To create an account the employee's supervisor will have to provide the employee's personal information. When an account is created an e-mail is sent automatically to the new employee. This email will contain his or her temporary password. The employee id will be used as a username to log in to the page.
2. **Delete Employee -** When an employee is deleted from the system, it is deleted from the web page view but not from the database. This is to maintain referential integrity at the database level and for history and review purposes at the company level. Supervisors are not able to delete themselves or delete the root administrator from the system.
3. **Edit Employee -** In the edit employee page, supervisors will be able to edit the employee's personal information. However, the employee id of an employee is not editable, if a supervisor submits a wrong employee id when creating an employee account, the supervisor will have to delete

the employee with the erroneous employee id and create a new one. In addition, supervisors will not be able to edit other employee's passwords.

4. **View Employee -** The view employee page will show the entire employee's personal information. This page can be used to print the employee personal information in a clean way.

Security Guards:

5. **View Employee -** Security guards will be able to view limited information about other employees such as the employee name, the employee id and the employee emergency telephone. This is to maintain confidentiality.

Supervisors and Security Guards:

6. **Employee Filter -** As employees will be added to the system, the amount of employees in the system will increase and it will be difficult to find specific employee's record within the system. To facilitate this task an employee filter by employee id or by employee name was included.

3.2.2.3. Profile

Supervisors and Security Guards:

7. Supervisors and security guards will have a personal profile page in which they will be able to change their password.

3.2.2.4. Checkpoint Management

The following information will be stored in the system for each checkpoint: checkpoint name, description, latitude and longitude.

Supervisors:

8. **Add Checkpoint -** To create a checkpoint supervisors will have to provide the checkpoint name, a brief description with which the checkpoint can be identified later and the location of the checkpoint. The location of the checkpoint can be selected by specifying a point on a Google map or by setting the position latitude and longitude by hand.
9. **Delete Checkpoint -** When a checkpoint is deleted from the system, it is deleted from the web page view but not from the database. This is to maintain referential integrity at the database level and for history and review purposes at the company level.
10. **Edit Checkpoint -** The checkpoint name, description, and location can be edited in the same way the checkpoint is added.
11. **View Checkpoint -** Like devices in the device map tracking page, the view checkpoint page will display in a Goggle map the exact position of the checkpoint. This page will also display the checkpoint name and description.

3.2.2.5. Device Management

The following information will be stored in the system for each checkpoint: device unique id, device name.

Supervisors:

12. **Add Device -** To add a new device, supervisors will have to provide the device name and the device unique id located inside the device battery compartment of the device.
13. **Delete Device -** Supervisors will not be able to delete on shift devices.
14. **Edit Device -** In addition to provide a way of editing the device name and device id, this function provides a way of changing the status of the device. If a device is stolen or lost the supervisor can use this page to change the device status to Stolen, Lost, among others.
15. **View Device -** The view device page will show the device information. This page can be used to print the device information in a clean way.

3.2.2.6. Employee Time Attendance Report

Supervisors:

This page will display information about the amount of time a security guard spends on the job and his or her checkpoint rating (number of checkpoint made per number of assigned checkpoints.).

When opening this page it will be automatically filtered and only information about the employee's last thirty (30) days of work will be displayed on a time attendance table. The table will contain the following information: start date and time of the employee shift, end date and time of the employee shift, checkpoint rating (number of checkpoints made per number of assigned checkpoints) and the amount of worked hours.

In addition supervisors will also be able to specify the start and end date on which the time attendance report is done. Moreover, to help supervisor measure the employee's performance based on a range of time the following information will be displayed below the table: total amount of worked hours and the total checkpoint rating.

3.2.2.7. Message Management

The message management page will provide to the users an advanced way to manage the sent and received messages in the SGMS.

Supervisor and Security Guards:

16. **Sent Messages -** All messages sent by the logged-in employee will be displayed in this module. If the end user selects any message, detailed information of it the sender id and name, the receiver or receivers' identification and name, the time, the date, and the text message of the received message will be displayed.
17. **Received Messages -** All messages sent by the devices will be displayed in this module. If the end user selects any message, detailed information of it including a map with the location from where the message was sent, the sender id and name, the receiver or receivers id and name, the time, the date, and the text message of the received message will be displayed.

18. **Compose Message -** This is an advance version of the simple text message functionality that the user has throughout the SGMS web application. The user will be able to send text message to the pager-like devices. Unlike the simple text message, in this version the user can send messages to any selected devices.

3.2.2.8. Shift Management

Supervisors and Security Guards will use this module to view, create, and delete employee shifts. This page will have a table with all the on shift employees with the following information: security guard id and name, device name, shift start time and shift end time.

Supervisors and Security Guards:

19. **Delete Shift -** Delete employee from the shift.
20. **Create Shift -** Add an employee to the shift. This option will open a wizard in which the employee will have to follow the following steps:
    1. **First Step -** Choose a security guard from list
    2. **Second step -** Choose a device from the list
    3. **Third Step -** Checkpoints will be added, one by one, in order, and the range of time to reach each checkpoint
    4. **Final Step -** Confirm your request
21. **View Shift -** Within this option the employee will be able to view the shift information.

4. Risk Management and Considerations

4.1. Risk Management Plan

Risks are always present in the development of a project, even if it is very small. The designers and developers of the system must be prepared in case any of them materializes, preventing irreversible damage to the project. The following is the risk mitigation, monitoring, and management plan for the SGMS project:

4.1.1. Conflict between Team Members

Mitigation

- Declare that conflict deserves respect; it will not be treated as a sign of unprofessional behavior.
- Declare up front that everybody's win conditions will be respected.
- Arrange up front that when win conditions are mutually exclusive or partly so, the parties will be expected to move into mediation to resolve conflict.

Monitoring

- Check if two or more members of the group never agree on arguments.
- Having all the tools to resolve an issue, check if it takes too long to resolve it.

Management

- Establish a mediator.
- The mediator will be a person that has no power over any of the members of the conflict, and has no interest on any particular resolution.
- The mediator will ask for all the member consent before helping them.

4.1.2. Customer Cannot Attend Meetings

Mitigation

- Manager must coordinate meetings with the customer, so customer is capable of determining if the prototype meets the expectations.
- Manager must send a notification (emails, phone calls), to remind customer of the next scheduled meeting.

Monitoring

- Manager must confirm that customer knows the meeting dates.

Management

- Manager must talk to customer, pointing out the importance of these scheduled meetings
- If risk materializes a lot, manager must warn customer that the project could be extended by the lack of revision and approval, at customer's expense.

4.1.3. One or more of the team members leaves the group

Mitigation

- Assign tasks to all team members depending on their knowledge, abilities and academic load.
- Establish realistic goals distributing them equally inside the range of time in which the project was to be delivered, so that team members feel comfortable with deliverables and do not feel stressed with the project.
- Work must be divided in independent modules.

Monitoring

- Manager must periodically have one to one meetings with each team member to talk about how the project is going, how they feel about the project and how they are managing their time.
- Manager must check the quality of delivered work of each team member.

Management

- Reassign modules to the remaining team members of the group depending on their activities and completed work.

4.1.4. Computer Crash

Mitigation

- Make various copies of the software in development in different places, and copies of the documentation related to it, in several locations

Monitoring

- The project manager should always check the equipment, and the developing environments in which the team is developing the software.
- Any change on the performance of the developing environment should be tracked, and taken into account, and reported.

Management

- Stop all development in defective equipment or environments, and report them.
- Move to a stable system and carry on working.

4.2. Contractual Aspects

This section explains the legal agreements between C Group Engineering Solutions and our costumer Miguel Figueroa and Nayda Santiago.

4.2.1. Agreements with client

C Group Engineering Solutions have agreed with Miguel Figueroa and Nayda Santiago to limit the SGMS to the specifications stated in this document and in the SOW (see appendix). Changes to any of the specifications of the project will need to be agreed upon by both parties in writing.

4.2.2. Progress Report Requirements

Progress reports will be conducted on the dates agreed upon and set upon in the milestone section of this document. The project reports will include a summary of completed tasks, a summary of tasks that need to be completed, overview of problems encountered, and what actions have been taken to mitigate them, and a risk monitoring sheet.

4.3. Legal considerations

In order for this product to be usable in the United States all the radio and telecommunications components have to be FCC compliant. The component list of the project has been revised to have FCC compliant Wi-Fi radio and GPS module.

To protect the privacy of security guards the system will have a turn off button that will disable tacking of the security guard. This is done as a preventive measure in order to ensure that tracking of the security guard will only take place during the 8 hour shift and that tracking could be prevented if the guard has the device outside working hours.

4.4. Environmental Issues

Lead is a poisonous element hence it cannot be degraded or transformed into some other material, and it is extremely difficult to clean up after dispersal in our environment; it already widely contaminates our environment and is harmful in very small amounts [6]. Components compliant with the Restriction of Hazardous Substances (RoHS) Directive have been chosen when available, as not all manufacturers follow this directive yet.

5. Budget

5.1. Human Resources

To develop the Security Guard Monitoring System (SGMS), C Group Engineering Solutions requires three Software Engineers I and two Hardware Engineers I. Each Software Engineer I has a yearly salary of $39,593.00 with an hourly payment equivalence of $19.03. Each Hardware Engineer I has a yearly salary of $37,690.50 with an hourly payment equivalence of $18.12. The SGMS will be developed in a 16 weeks period, from January 9 of 2008 to May 5 of 2008. The total days of labor are 71 days excluding 10 holidays. This gives us a total 568 hours of labor for 71 days working 8 hours a day. The following table explains the total cost of human resources.

Table 2: Personnel costs calculation

Employees	Position	Dollars/Hour	Hours/Contract	Payment/Contact
D. Carbia	Software Engineer I	$19.03	568	$10,809.04
M. Resto	Software Engineer I	$19.03	568	$10,809.04
O. Negrón	Software Engineer I	$19.03	568	$10,809.04
R. Santos	Hardware Engineer I	$18.12	568	$10,292.16
C. Rodríguez	Hardware Engineer I	$18.12	568	$10,292.16
		Employment Cost		$53,011.44
		Unemployment Insurance (1.40%)		$742.16
		Retirement (15.0%)		$7,951.71
		State Insurance Fund (1.55%)		$821.67
		Social Security (6.20%)		$3,286.70
		Medicare (1.45%)		$768.66
		Total Employment Cost		***$66,582.34***

5.2. Hardware Components

In order to construct the pager-like device, there are some parts that need to be acquired for the hardware development:

- **Microcontroller** -- It is an essential part for this device because has the function to control the whole system.
- **Radio** – It is used to communicate the device with an internet server.
- **GPS** – It connects to a satellite to give the current location of the device.

- **LCD Display** – Needed for the initial device configuration, to display the received text messages and other visual functionalities.
- **Keypad** – Serves as human-device interface. It is needed to input the numeric code messages to be send from the device and other functionalities.
- **RTC** - The real time clock module will be used to extract the actual time and date to be displayed in the device.
- **Buzzer** – It is used to alert the device user with a sound for incoming instant messages and other system alerts.
- **Vibrating Motor** – It is used to alert the device user with a vibration for incoming instant messages and other system alerts.
- **Low drop-out (LDO) Voltage Regulators** – These devices maintain a constant voltage supply across a range of varying current loads, which helps in avoiding errors.

Table 3: Hardware components costs calculation

Component	Model	Price	Qty.	Cost
Microcontroller	MSP430F149	$150.00	1	$150.00
Radio	WLNB-AN-DP101	$109.06	1	$109.06
GPS	EM-406A	$59.95	1	$59.95
LCD Display	GDM12864H	$19.95	1	$19.95
Keypad	190562 (Jameco #)	$8.75	1	$8.75
RTC	BQ3285	$2.10	1	$2.10
LDO Regulator (5V)	LP2950-50LPR	$0.27	1	$0.27
LDO Regulator (3.3V)	LP2950-33LPR	$0.27	1	$0.27
LDO Regulator (adj.)	TLV1117	$0.29	1	$0.29
Buzzer	COM-07950	$1.95	1	$1.95
Vibrating motor	256382PS (Jameco #)	$4.65	1	$4.65
		Total Hardware Cost		***$356.97***

5.3. Software Components

To develop the security guard monitoring system web page, the following programs will be use:

- Red Hat Development Studio – Integrated development environment used for the development of the web based applications.

- MySQL GUI Tools – Used to create and modified the data base.
- MySQL Server – Server used to support the data base.
- Apache Tomcat – Used as the web server.

Table 4: Software costs calculation

Program	Price	Quantity	Cost
Red Hat Development Studio	$99.00	3	$297.00
MySQL GUI Tools	$0.00	3	$0.00
MySQL Server	$0.00	3	$0.00
Apache Tomcat	$0.00	3	$0.00
	Total Software Cost		***$297.00***

5.4. Overall Cost

Table 5: Overall costs calculation

Category	Cost
Total Employment Cost	$66,582.34
Total Hardware Cost	$356.97
Total Software Cost	$297.00
Project Cost	$67,236.31
80% Overhead	$53,789.04
Total Project Cost	***$121,025.35***

6. Personnel Biographies

6.1. Diana Carbia – Software Engineer I (Project Manager)

Diana Carbia is a Computer Engineer from the University of Puerto Rico at Mayaguez Campus. She has worked with Java, C, and Assembly languages on her past project experiences. She has been involved in the development of projects such as: Biometric Control and Time Attendance System, My Log Viewer: RSS Log File Reader Application, Command Shell, among others.

Her role in the development of the Security Guard Monitoring System will be as the project manager. She is responsible for the distribution of work, completing work on time, efficiently planning meetings, making a project plan, and software development of the project.

6.2. Oscar Negrón – Software Engineer I

Oscar G. Negrón López is a Computer Engineer with specialization in Software from the University of Puerto Rico at Mayagüez Campus. Oscar has knowledge of the following programming language and software skills: Java, C, Assembly, JSP, Servlets, HTML, UML, and SQL. He has taken software/hardware specialization courses like: Programming Language, Databases Systems, Software Engineering and Digital Systems Design.

6.3. Miguel Resto – Software Engineer I

Miguel Resto is a Computer Engineer from the University of Puerto Rico at Mayagüez. He has programming experience in JAVA, C, C++, C# and Database systems. Miguel worked for the Microsoft ACE Engineering Team during spring 2007 in which he executed product test for the 2.5 release of the TAMe application, wrote the Secure Application Test Class lab manuals for the MS ACE Security Team, and met with customers and the product owner to discuss the design of an engagement framework site. His areas of expertise are web application development, databases and web application security.

Miguel will be the lead of the design, development and testing of the SGMS web application. He will also work with the relational database design and creation, and he will help in the documentation process.

6.4. César Rodriguez – Hardware Engineer I

Cesar Rodriguez is a Computer Engineer from the University of Puerto Rico at Mayaguez. His work experience covers working with software, hardware, and information security. Particularly to this project it is of importance his experience

working with the Biometric Access Control and Time Attendance system for the Microprocessor Interfacing course. Working on that assignment he acquired the necessary experience in Assembly and C language necessary for working on this project. Cesar will leverage on his experience to work with Roberto on the hardware aspects of SGMS.

6.5. Roberto Santos – Hardware Engineer I

Roberto Santos is a Computer Engineer from the University of Puerto Rico at Mayaguez with an emphasis on embedded systems and integrated circuits. He has worked on several engineering assignments with the National Security Agency, spanning over nearly two years. He has software design experience in C/C++, PERL, x86/assembly, and VHDL. His hardware experience is in embedded systems and integrated circuits design.

Roberto Santos will be responsible in part with the hardware definition, documentation, design, development, testing, and support of this project.

7. References

1. Using The SilverGuard Security Guard Monitoring Systems are easy as 1,2,3... (2003). Retrieved 02 13, 2008, from Brookly Computer System Inc.: http://www.bcsint.com/sggsm.htm

2. GuardWatch - Guard Tour System. (2007). Retrieved 02 13, 2008, from GuardWatch: http://www.scionelectronics.co.uk/index.htm

3. Do more, with less. (2007). Retrieved 02 13, 2008, from GuardTrax: http://www.novatracker.com/guardtrax.php

4. Effective Web Navigation. (2007). Retrieved 02 13, 2008, from HWG News: http://www.hwg.org/opcenter/newsletters/tips/jul00a.html

5. Breadcrumb. (2007, 08). Retrieved 2008, from Wikipedia: http://en.wikipedia.org/wiki/Breadcrumb

6. Lead in the Environment. (2000, 09 25). Retrieved 02 13, 2008, from Lead in the Environment: http://www.uwsp.edu/geo/courses/geog100/Lead-InEnv.htm

7. Security Guards Aid in Robbery. (n.d.). Retrieved 02 13, 2008, from New Times Online: www.newtimesonline.com/index.php?option=com_ content&task=view&id=6353&Itemid=181