Software Requirements Specification

for

Fire and Security Alarm Monitoring Simulation System

Group No. 7

Prepared by Allen Lozano
Anand Sai Mishra
Diana Ramirez
Jaspreet Singh
Karen Salinas
Lauren Stimson

California State University, Dominguez Hills

Fall 2019

Table of Contents

Revision History

Name	Date	Reason For Changes	Version
Team 7	9/17/19	First Draft	1.0

1.　Introduction

The project is being built for the partial completion of requirements for the Advanced Software Engineering (CSC 581). The developed product may be used by a building management or a safety ensuring corporation in keeping the civilians in residing in the buildings safe in case of any intrusion or fire hazards.

1.1　Purpose

The developed system will be capable of controlling and managing a building in case of a Fire or Unauthorized access of confidential areas of the building. The system divides the buildings into zones and uses assorted sensors to detect access and fire hazard situations.
It also unites all the various safety systems into one centrally controlled area where the administrator can control the situation from a single screen.

1.2　Scope

We are creating this application for monitoring and securing a building from a central location and to be efficient enough to be managed by a single administrator.

The System consists of a centrally controllable software FSAMS along with the host of various sensors and data gathering and processing hardware.

1.3　Definitions, Acronyms, and Abbreviations

FSAMS – Fire and Security Alarms Monitoring System

2.　General Description

2.1　Product Perspective

The product that is being developed is capable of delivering a building wide fire management from one secured centralized location. It uses a collection of sensor arrays as well as communication system deliver the sensor's recorded data to the centralized system. A controller in the Controller location will be trained to be adequately capable of using the same.

2.1.1 System Interfaces
The system uses a web page running over the building's intranet system. The system requires an internet browser and required system libraries to run adequately.

2.1.2 Hardware Interfaces
The system requires a few hardware devices to be able to run properly.

2.1.2.1 Intranet Connections
The system needs a system connected to the building's intranet for the emergency information to be available to all of the system in case of an event.

2.1.2.2 Sensor Network
The network of interconnected sensor arrays that work together to pinpoint the location and severity of the event.

2.1.2.3 Sensors
Individual sensor's that contribute to each sensor array.
2.1.2.3.1 Pyroelectric Infrared Sensors Motion Detection
2.1.2.3.2 Infrared Light change detection sensor
2.1.2.3.3 Close Circuit Camera System

2.1.2.4 System
System can run on any operating system running over X86, X64 or ARM system that has a working Internet browser and available TCP/IP functionality.

2.1.3 Software Interfaces
To build the project using JavaScript, WordPress, HTML and CSS for the front-end structure. The use of Webpage as the front-end control level leaves the project to be independent of the system architecture and operating system (so long as the system is able to run an Internet Browser.

2.1.4 Communications Interfaces
This will be a desktop application and will automatically broadcast the emergency message to the first responders. It will also inform the building administrators about the emergency situation.
It works on network interfaces such as RJ45 and optical fiber cables that carries data from the sensors to the control centers.

2.1.5 User Constraints
2.1.5.1 General User
- *Ability to raise or silence alarms in the system.*
- *Ability to call for Emergency Services*
- *Ability to request for maintenance*

2.1.5.2 System Administrator
- *All Abilities of a General User*
- *Ability to add / remove users.*
- *Ability to create new zones to the system.*
- *Ability to create or assist in maintenance orders*

2.1.5.3 Maintenance Crew
- *All abilities of the Administrator.*
- *Ability to upgrade system*
- *Ability to change malfunctioning sensors*

● *Ability to upgrade/maintain sensor networks*

2.1.6 Operations
1. *Most of the building is covered and zoned into different sections for granular control of the sections of the building.*
2. *Most zones are covered with various fire suppression systems and will be triggered in case of an emergency.*
3. *The building will be using emergency exit markers like floor lighting and fluorescence paints that would be visible in low light.*
4. *It is also equipped with emergency sound systems that create a lot of noise in case of a fire.*
5. *A security alarm maybe able to lock internal doors in order to isolate zones the event of an intrusion.*
6. *It should be possible to isolate complete zones by automatic door locking.*
7. *False alarms are common, and it might be normal practice to have an alarm confirmed before alerting emergency services. There are different ways of confirming an alarm. Multiple sensors that are detecting a problem may confirm the fire in the case of a fire alarm.*
8. *Fire Alarms should be able to disable the elevators in an adequate way in case of an emergency.*

2.1.7 Site Adaptation Requirements
The building will need to be retro fitted with additional sensors for the system to pull the data from. The system also needs a secured control area for the administrator to be monitoring from. It will also need electronically controlled door locks for the automatic locking system. The system will require a backup power system in case of power failure and improve redundancy. It needs to be fitted with the sensor network and additional cabling to be able to run the system.

2.2   Product Functions

The product shall in the constraints of expectation perform as an Emergency alert and building administration system performing the following activities.
1) *Detect and alert the Building controller of a Fire or related Issue.*
2) *Send out emergency warning through the building in case of any incident.*
3) *Alert the system administrator and the supervisors of the incident.*
4) *Check for false alarms.*
5) *Call Emergency systems.*
6) *Detect Intrusion in the protected areas.*

2.3   User Classes and Characteristics

2.3.1 General User
● *Ability to raise or silence alarms in the system.*
● *Ability to call for Emergency Services*
● *Ability to request for maintenance*

2.3.2 System Administrator
- *All Abilities of a General User*
- *Ability to add / remove users.*
- *Ability to create new zones to the system.*
- *Ability to create or assist in maintenance orders*

2.3.3 Maintenance Crew
- *All abilities of the Administrator.*
- *Ability to upgrade system*
- *Ability to change malfunctioning sensors*
- *Ability to upgrade/maintain sensor network*

2.4 Constraints

2.4.1 Regulatory policies
The project needs to be compliant to all the state and federal safety requirements.

2.4.2 Hardware limitations
The Sensors and the network need to be fire and temperature resistance so that the system won't fail in case of the emergency.

2.4.3 Interface to other applications
Needs to be compliant to the requirement of modern web browsers.

2.4.4 Parallel operation
The system will need to be able to be operated in more than one system at the same time so as to avoid being locked out in case of an emergency and any employee having missed to log out.

2.4.5 Signal handshake protocols
Uses connectors such as Optical Fiber connector and RJ-45 ports to build and operate the sensor networks.

2.4.6 Reliability requirements
The system should be operational in case of any situation such as a power failure and high temperatures (up to 1800 C).
Should be able to detect and correct false alarms.
May be able to detect intrusions even in total darkness.

2.4.7 Emergency Requirements
The system shall automatically the emergency number in case of an event.

2.4.8 Performance Requirements

The system needs to be able to perform the emergency operations in minimum amount of latency and timing between the event and the action.
The system also needs to be able to be overridden by a controller on the center at any time.

2.4.9 Maintenance Requirements
The system needs to be constantly updated with the latest firmwares and standards to maintain compliance and compatibility with the Govt. regulations.

2.5 Assumptions

- *The network is never down and can be trusted to be running even in case of an emergency.*
- *The system is placed in a position with backup power supply at all time and is up and running at all times even in the case of a main power supply failure without any latency.*
- *The controllers, users and administrators are adequately trained in the operations and are in complete control of their faculties while operating the system.*

3. Specific Requirements

3.1 Functional Requirements

3.1.1 Sensor Calibration and synchronizing
Cameras and motion sensors are placed and paired for the system to work effortlessly and with minimum latency and difference in Boolean output.

3.1.2 Auto Locking
The system needs to be able to detect the intrusion and automatically lock itself in case of an intrusion to protect sensitive information and areas.

3.1.3 Emergency lights and Routes
The system involves an assortment of emergency of light and sound systems that will function regardless of the condition of the power failure. It involves multi-stage lighting such as floor lights, Emergency Exit highlights and Fluorescent paint on the walls of the offices to help safely guide the occupants out of the building in a reasonable time frame.

3.1.4 Control Center
The system should be able to take Inputs and provide Outputs at a central location with capability to be able to access the entire building from one convenient location.

3.1.5 Override Control

The system should be able to be overridden by the administrators in case of any out of expected conditions.

3.2 Non-Functional Requirements

3.2.1 Reliability

Due to the system being involved with emergency systems it needs to be reliable and can't fail on account of power failure, network failure or Internal sabotage.

3.2.2 Availability

Specify the factors required to guarantee a defined availability level for the entire system such as checkpoint, recovery, and restart. This is somewhat related to reliability. Some systems run only infrequently on-demand (like MS Word). Some systems have to run 24/7 (like an e-commerce web site). The required availability will greatly impact the design. What are the requirements for system recovery from a failure? "The system shall allow users to restart the application after failure with the loss of at most 12 characters of input".

3.2.3 Security

The system needs to be protected from physical and software sabotage form internal and external agents. It needs to be protected from tears and cuts in the network wiring and backbone laid throughout the building. It will also include the addition of a second power supply inside the control center ready with uninterrupted backup. The operators should be trained enough with the functionality of the system

3.2.4 Accessibility

The System needs to be in compliance with all of the ADA regulations and must be friendly and intuitive for people to be able to use in a friendly way.

3.2.4 Maintainability

The systems need to be monitored vigilantly and continuously to find bugs and damaged due to the continuous wear and tear of day to day use.
It will also need to be updated to maintain compatibility with the latest architectures and standards all the while maintaining compatibility with the existing systems.

3.2.5 Legal Liabilities

The system and its developers denounce all legal and Liabilities from the system and the user and corporate needs to be in acceptance of all legal fees and act of god events.

3.3 System Compliance

The system needs to be in full compliance with all the State and Federal Government mandated rules and regulations prescribed to be completed in full for the system to be approved to be run in residential and official areas of the city.

It also needs to be in compliance with the American Disability Act (ADA).

4. Specific Requirements Specifications

4.1 System Functions

4.1.1 Fire Alarm monitoring system
Includes all the systems sensor and sensor networks that are involved in detecting fire and smoke in the building and alerting the operator and administrators about the location, zone and intensity of the incident.

4.1.2 Intrusion detection system
The system includes the systems and sensor networks that are involved in controlling the access and locking of the facilities of the building. It also involves the systems that are involved in the detection and isolation of intruders in the building.

4.2 System Interfacing

4.2.1 Front End System
The front end of the system involves the website which includes the control system that is visible to the users and administrators of the system. This is the panel where the system shows and lets the user know about the location and intensity of the event.

4.2.2 Installation Environment
Involves the operating system and the browser that is required to run the system.

4.3 User Interfaces
As a user the only part of the system that the person can interfere is the front end as the system is being developed in a closed end system. Hence the user is not permitted to make changes to any of the system in the background like the Sensor and Sensor Networks.

4.4 Hardware Interfacing

4.4.1 Sensor Network

The sensors need to be interconnected to each other to triangulate the location of the incident as well as intensity of the event. It involves the combination of the interface between the sensor and the system.

4.4.2 Sensors

This is the array of sensor that is responsible in detecting and analyzing the event for the system.

4.4.3 Keyboard, Video, Mouse System

The control system which allows the admin to control and update the system state.

4.4.4 Server System

The control system needs x86, x64 or ARM platform to be running at its most efficient state and at least 1GB of system memory.

4.5 Software Requirements

The system requires a generic environment such as MacOS, Windows, or Linux. It will also need an internet browser with basic TCP/IP functionality.

4.6 Communication Interfacing

4.6.1 Emergency Communication

The system needs to be able to communicate directly with the first responders about the location and the type of emergency event occurring at the site.

4.6.2 Building Communication

The system needs to send an alert and a SMS/RCS Text message to the administrators of the building complex stating the type and zone of emergency.

4.6.3 System Administrator

The system needs to send an emergency alert to the system administrator about the location, zone, and intensity of the event. It shall also notify the system administrator about the identity of the operator in the control room.