Keypad Project

Requirements Definition Document

RDD Version 3.0

Team T02
4 February 2021

Tanner Evans (manager)
Thomas Bowidowicz (documents)
Robin Acosta
Marcos Lopez
Jared Bock
Jacob Varela

CS 460 Software Engineering

TABLE OF CONTENTS

1 Introduction

1.1 Purpose

This Requirements Definition Document (RDD) is for a keypad system used at community entrance points. The keypad system will be used to restrict access to a given community to those who possess a valid code. This document is intended to define the desired functionality of the project, the structure and implementation, as well as any constraints, technical or non-technical. This document will also direct the rest of the design and implementation of the software.

1.2 Background

Gated entries are a common method of securing both commercial and residential properties and are a feature that residents and owners pay a premium for. The keypad entry of a neighborhood is designed so that only those with the code can enter, including service vehicles, guests, and residents. The goal of this particular project is to design the software of a keypad used in a residential community that can also be scaled to broad use across a range of gate systems regionally.

The keypad system should be functional and dependable for those who have authorized access while also ensuring that the keypad doesn't allow unauthorized visitors (those without the code) to open the gate. It should also possess features that make it convenient and practical for residents as well as administrators in charge of troubleshooting and the gate code itself.

This document begins with a section covering the objectives that the project will achieve. These are largely the specific functions that the keypad will be able to perform and this section will serve as a benchmark for the future progress of the software development. The next section covers the system organization of the project defining the exact system, components, interactions, and layout of the proposed keypad. The following section covers the capabilities of the proposed system detailing what the keypad will be able to do. Finally, the constraints section goes over the challenges and limitations that were imposed on the design of the system. These stem from both the customer requests and the physical hardware and software constraints that have been realized.

2 Objectives

For this document, objectives will be divided into two sections: functional and non functional objectives. The functional objectives are the main tasks that the keypad needs to be able to perform while the non functional objectives are the tasks that are required due to external constraints and are not covered by the function objectives. The functional objectives will be concerned with the primary specific function of the keypad while the non functional will be more broad goals for the system. These objectives correspond to the criticality of function and were determined based on the degree of importance that certain

elements had to the project as a whole. Both functional and non functional objectives are listed in order of the importance that they play in the system as a whole.

2.1 Functional Objectives

- The primary objective will be to facilitate the gate keeping non community members without the password out and allowing those in the community with the password to enter.
  - To facilitate this, the keypad will unlock the gate when a correct password is input. There will be one keypad per gate.
- The system will have clear auditory signals to indicate to the user that the gate is locked or unlocked.
- The system will have a password protected administrator mode. The system will have two tiers of passwords so the administrator can change both the general and administrative password.

2.2 Non-Functional Objectives

2.2.1 Reliability

- The keypad will be functioning constantly and must not interfere with the safe flow of traffic in and out of the community.
- The system should be resilient so that the community does not become inaccessible or inescapable at any time.

2.2.2 Scalability

- The system should be easy to replicate across a wide range of gated communities.
  - This is a key objective of the client who plans to roll out this keypad and software nationally across many types of gates.

2.2.3 Security

- The system will be secure preventing people without the password from entering the community or changing the password illicitly.

2.2.4 Interfaces

- The user will interact with the keypad via the buttons on the keypad itself.
  - There will be auditory signals from a speaker mounted on the keypad to indicate to the user the state of the gate and whether or not any input password is correct or not.

3 System Organization

This section of the document will cover the layout and organization of the entire keypad system including items that are outside of the scope of the proposed work (such as the gate and its sensors).

3.1 Main System

The main system is the keypad itself. It will be the first and only point of contact between the system and the user.

3.2 Location

The keypad will be located near the entrance into a community on the driver side of the road for easy access. The keypad will be placed about five feet above the ground to allow its use with users in varying sizes of vehicles. This location will be static and should not move.

3.3 Connected Components

The gate will be the main component connected to the keypad. To ensure the simplicity and resilience of the system, the keypad will be hardwired to the gate. It will receive a signal from the keypad to tell it to unlock. The gate will be connected to its own sensors that will insure the gate will not close on any vehicles that are passing through.

3.4 User

The user will be the drivers of a vehicle looking to gain entrance into the community. This can be anyone from people who live in the community to those going into the community for services (i.e. garbage trucks, mail and delivery drivers). The simplicity of the system will enable all persons to easily access the keypad successfully.

3.5 Input

The input system for the device is provided by the thirteen buttons on the keypad face.

3.6 Output

The output system for the device is provided by the speaker on the keypad which indicates the success of password entry and the state of the gate.

3.7 Figure

The first figure below describes the general flow of the system. The user will interact with the keypad, the keypad will communicate with the gate to send the unlock command, and the gate will be connected to both the keypad and the gate's own internal sensors. The second figure is the layout of the keypad face including the 0-9 number buttons as well as the # and * buttons.

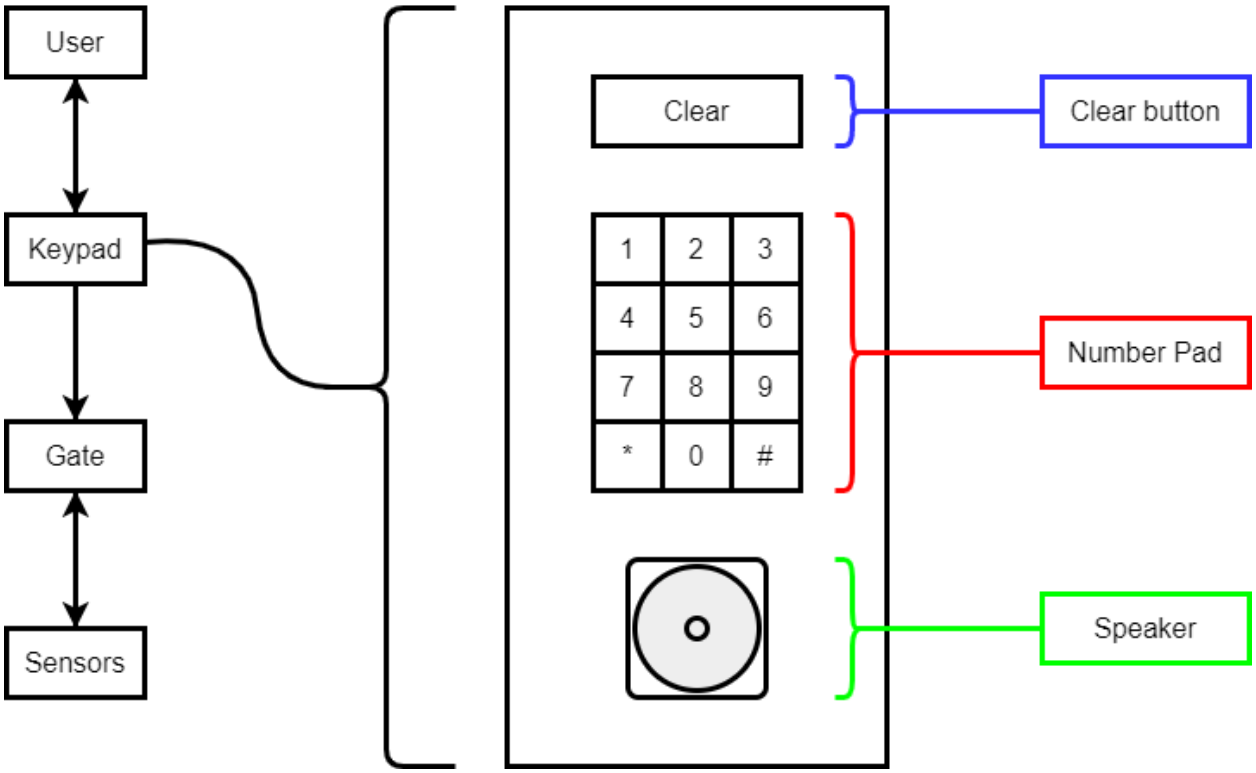

Fig 1 - System Diagram

4 Capabilities

This section will identify the different functional and nonfunctional requirements for the keypad to be successfully operational. For this document there will be two distinct categories for the keypad's capabilities: essential functions and omitted or supplementary functions. The essential functions define the components of the keypad that are necessary to successfully operate. Without any of these components the keypad would not be able to successfully achieve the functional objectives listed in section two. Omitted/supplementary functions are any components that were chosen not to be implemented. These components were deemed unnecessary due to limitations described in the design constraints or time limitations. Supplementary functions are the components that are not necessary to meet the functional objectives listed in section two but would enhance the interaction experience for the keypad user.

The keypad system should be functional and dependable for those who have authorized access while also ensuring that the keypad doesn't allow unauthorized visitors (those without the code) to open the gate. The main responsibilities of the community gate keypad will be opening when the correct code is input, containing an administrative mode for password changes and debugging, having an audible notification when unlocked, and to have the keypad be physically secure.

4.1 Essential Functions

- The keypad must accept input from the user via the buttons on the front of the keypad. If the buttons on the keypad do not work then the user cannot unlock the gate.
- There will be two passwords stored initially with one being used for administrative and emergency uses and another being used by the general population of the community.
  - Both passwords will be four digits long.
- When the correct four digits are entered followed by pressing the (#) button a signal will be sent to the gate to unlock it.
  - If the user fails to press the (#) button to confirm the password within a given timeframe, the system will clear the current password input.
  - The keypad must have some form of internal timer mechanism. This timer is used to ensure that the keypad can reset after 15 seconds of inactivity.
  - If the user inputs the wrong password, the system will reset.
  - The user can manually clear the password input by pressing the “clear” button.
  - Once the gate has been unlocked and opened, the system will defer to the default system already placed with the gate as to when the gate will close. Upon closing, the gate will re-lock.
- The administrator will be able to change the passwords that are accepted:
  - The administrator will be able to change the user password by entering the administrative password, pressing the (*) button, and then entering a new four digit password.
  - The administrator will be able to change the administrative password by entering the administrative password, pressing the (*) button, then the (#) button, then entering a new four digit password.
- The keypad will emit a sound to indicate that the gate is currently in the unlocked state. This sound will start once the correct password is entered and end when the system either times out or the gate is closed and re-locks..
- The keypad will be hardwired to the gate to ensure a stable connection is always maintained.

5 Design Constraints

This section lists the specific constraints that are placed on the design and implementation of the keypad and that will inform that work moving forward. These constraints include specific design requests made by the client and physical limitations imposed by the structure of the overall system.

5.1 Interface

- The keypad must be usable by cars, service trucks, and an administrator.
- The keypad must have buttons to enter the password and debug (the buttons are listed in sections 2.1 and 3.5).
- The buttons must be visible and easy to press from a car or truck.
- The passwords must be four digits.

- There must be a way for users to correct mistakes and try again (clear button).
- There should be clear indication if the code is valid or not valid (audible confirmation).
- The keypad must receive input signals directly from the gate, indicating the state of the gate. When a correct code is entered, it must be able to send a signal to open the gate. This signal is received through a physical connection between the keypad and the gate.
- The administrator must have a unique code and special privileges such as the ability to change the community code.
- The keypad must have a speaker that is loud enough for the user to hear. If there is no speaker then the user will not receive an audible indication if their code was entered correctly or not.
- The keypad must have a link between itself and the gate to ensure proper communication.

5.2 Performance

- Once a valid code is entered, the signal to open the gate should be sent immediately so that the user does not have to wait.
- The keypad must consistently check for a valid code and open once it receives a valid code. The keypad will not send a signal to open the gate if a code is not entered or if an incorrect code is entered.

5.3 Security

- There may be safety concerns regarding emergency personnel needing to gain access to the community. Access to all outside essential users will be accommodated through the use of the administrative passcode.
- The housing for the keypad must be locked.

5.4 Implementation

- The keypad must be implemented using Java 8 or higher.