Siesta Garden Controller

Software Requirements Specification

SRS Version 3.0

Team T06
20 April 2021

Ashley Krattiger
Justin Lusby
Daniel Sherwood
Matthew Zamora

CS 460 Software Engineering

Table of Contents

1 Introduction **2**
- 1.1 Purpose . . . 2
- 1.2 Scope . . . 2
- 1.3 Definitions, Acronyms, & Abbreviations . . . 2
- 1.4 References . . . 3
- 1.5 Overview . . . 3

2 General Description **3**
- 2.1 Product Perspective . . . 3
- 2.2 Product Functions . . . 4
- 2.3 User Characteristics . . . 6
- 2.4 Constraints . . . 6
- 2.5 Assumptions & Dependencies . . . 7

3 Specific Requirements **7**
- 3.1 External Interfaces . . . 7
- 3.2 Control Logic . . . 10

4 Design Constraints **13**
- 4.1 Software Constraints . . . 13
- 4.2 Hardware Constraints . . . 14
- 4.3 Security Constraints . . . 15

1 Introduction

The introduction section outlines the purpose and scope of this document, as well as provides a list of common definitions, acronyms, and abbreviations used throughout the document. Additionally, an overview of the structure for this document is provided, which describes the layout of the other sections included therein.

1.1 Purpose

The purpose of this document is to provide a detailed description of the requirements for the Siesta Gardens Controller (SGC). This document will illustrate the purpose, features, and interfaces of the SGC system. It will also explain the constraints under which the system must operate. The intended audiences of this document are the users, project managers, and the developers of the system.

1.2 Scope

The Siesta Gardens Controller is a security software system designed to ensure Siesta Garden's visitor and employee safety and maintain a secure space for park operation. The SGC is a single unified platform that integrates a kiosk that generates and manages token, employee tablets that validate tickets and monitor locations of the visitors, a self-driving vehicle that takes the visitors to and from the T-Rex exhibit, electronic surveillance, alarm monitoring, and access control.

1.3 Definitions, Acronyms, & Abbreviations

The following acronyms and abbreviations will be used regularly throughout the document and are defined here for convenience:

`SGC`	Siesta Gardens Controller
`SRS`	Software Requirement Specification
`GUI`	Guided User Interface
`OMT`	Object Modeling Technique
`UUID`	Universally Unique Identifier
`UI`	User Interface
`RFID`	Radio Frequency Identification
`T-Rex`	Tyrannosaurus Rex

Additionally, the following terms will also regularly be used and are defined as follows:

Administrator	The user(s) responsible for the management and control of the SGC system.
JavaFX	A Java software library for creating and delivering GUI-based desktop applications.
Zulu JDK	A version of the Java Development Kit containing all necessary components to build and run JavaFX applications.

1.4 References

The recommended practice is used in conjunction with the following publication:

IEEE Std 830-1998 IEEE Recommended Practice for Software Requirements Specifications. IEEE Computer Society, 1998.

1.5 Overview

The remaining document includes three chapters which entail a general description, specific requirements and design constraints of the SGC system. The General Description chapter provides a brief overview of the system's functionality. It describes the overall requirements and establishes a context for technical requirements specification in the following chapters. The specific Requirements section describes the different system interfaces and functionality of the system in technical terms or details. It also includes a System Interface Block Diagram depicting different components of the SGC system as a whole, as well as OMT diagrams that define semantics and relationships existing in the system. This part of the document is designed primarily for the developers of the system. The design constraints section defines the constraints on the software caused by the hardware and the environment that it exists.

2 General Description

Following is a general description of the Siesta Gardens Controller which discusses the functionality of its components in broad terms. This section is divided into the following subsections: *Product Perspective*, which provides brief descriptions of what each component is; *Product Functions*, which describes what each component does; *User Characteristics*, which defines assumptions about the different kinds of users who are expected to interact with this system; *Constraints*, which discusses the limitations of this system; and *Assumptions & Dependencies*, which details the prerequisites of implementing this system.

2.1 Product Perspective

The SGC is divided into several important subsystems, each connected (usually wirelessly) through a Central Management System. The components are as follows: a token management system, a vehicle management system, and an alarm management system. Since the Central Management System is the main component of this system, it will be discussed first; where-after, a discussion of each of the aforementioned subsystems will follow.

The Central Management System is responsible for the effective relaying of information to and from each of the other subsystems. Each of the subsystems is connected wirelessly to this system, and can send it information about their present statuses so as to be monitored by relevant staff. The central management system is used to monitor and control the subsystems in a way that it helps to maintain the smooth operation of subsystems. Central Management System can activate the manual alarm, vehicle override button, and modify the vehicle route. The central management system will have a database to send and receive data from different subsystems.

The Token Management System is the subsystem that is responsible for walking visitors through the token acquisition process, accepting their payment (debit or credit card only), and generating and dispensing a unique token which grants the visitor access to the park. Every token generated will possess its own Universally Unique Identifier (UUID) will be sent to the database which can be accessed by subsystem like vehicle management system to track the user location. This subsystem will be present on each of the kiosks located at the east side entrance to the park. When a visitor is ready to leave the park, the dispensed token is to be returned to a Kiosk to be recycled.

The Vehicle Management System is the subsystem that controls the self-driving vehicles which travel around the island on a periodic basis. The Central Management System is able to control these vehicles remotely if need be, or let them follow the predetermined course around the park. Each vehicle in the park will have an employee chaperone aboard to guide and manage the visitors. Each chaperone will be equipped with a tablet-computer that they can use to track each guest's token as well as communicate with the Central Management System. There are at least two self-driving vehicles operating at all times during park hours.

Finally is the Alarm Management System, which is the subsystem responsible for issuing, processing, and communicating the various emergency signals that the SGC is capable of sending. This system is an integrated part of the Central Management System. Alarm signals can be manually sent via this system, or signals sent from other subsystems can be monitored via this one.

2.2 Product Functions

The functions of each of the above-mentioned subsystems are discussed in this subsection, proceeding in the same order as before.

Central Management System

- Send/receive status and monitoring data from every subsystem
- Remotely control the park's self-driving vehicles
- Activate/deactivate an alarm system in case of an emergency
- Activate the emergency override button in case of emergency
- Token RFIDs will be stored in a database managed by this system—the RFIDs will act as keys to each entry in the database
- Database management within the Central Management System is performed autonomously.

Token Management System

- Allow visitors to purchase one or multiple tokens at a time
- Prompt visitors for debit or credit card payment, and validate this payment
- Generate and dispense unique tokens for each visitor
- Token tracking data will be shared periodically with the Central Management System for tracking purposes

Vehicle Management System

- By default, vehicles will travel the predetermined course around the park
- Doors are locked and unlocked when the chaperone indicates to do so (when arrived at the main exhibit, or when each visitor has returned)
- The override button will allow the vehicle to depart its current location and return to start in case of emergency
- Employee chaperone tablets will periodically receive token tracking information from the Central Management System
- Employee chaperone tablets are able to remotely communicate with the Central Management System

Alarm Management System

- Monitor all emergency signals from every other subsystem
- Information from the park's surveillance cameras will be monitored from this system
- All data from this subsystem is able to be monitored from the Central Management System
- Manually initiate an alarm signal

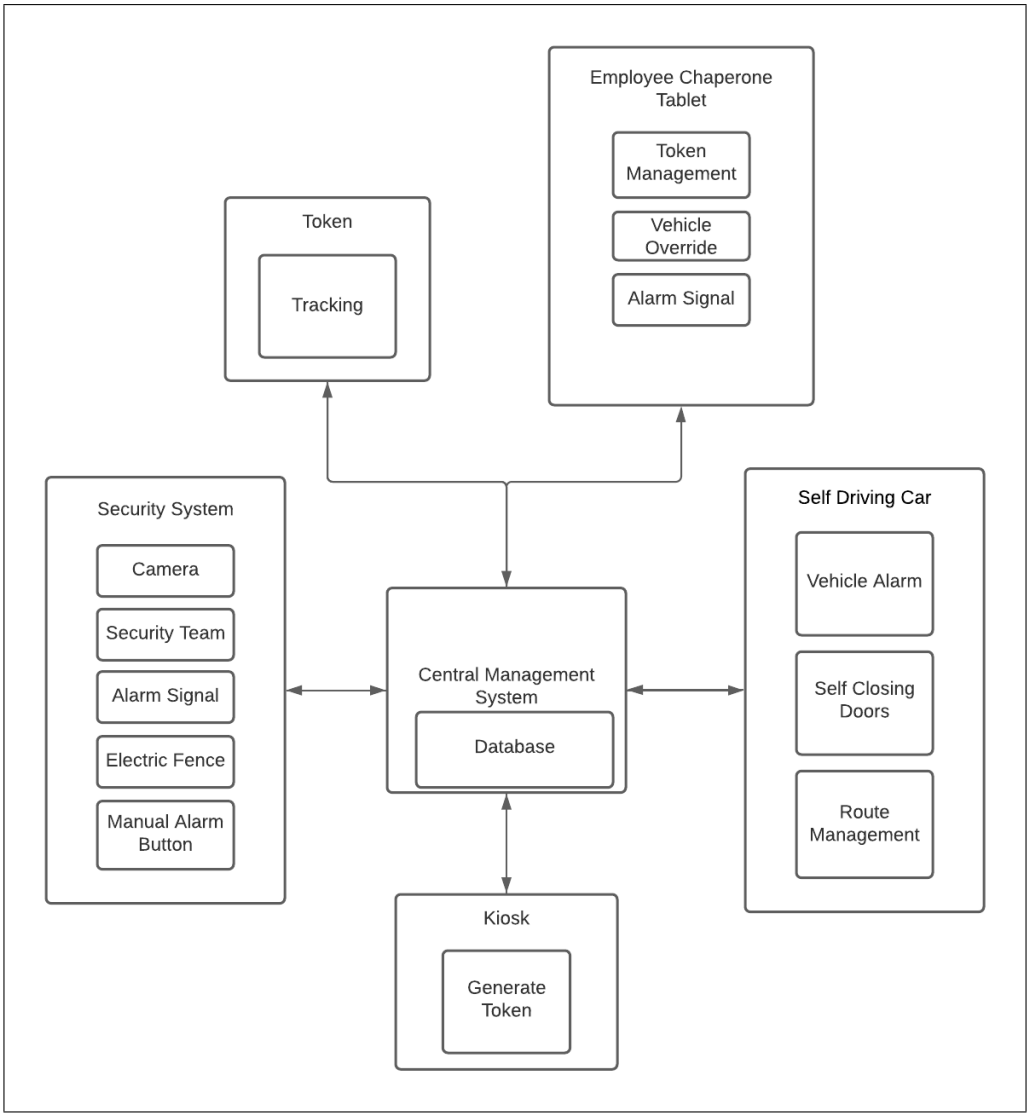

Figure 1: System Interface Block Diagram

2.3 User Characteristics

Visitors are required to follow the security protocol for the duration of their stay in the park. Visitors must purchase tokens at one of the entrance kiosk in order to gain access to the park (payment must be via debit or credit card). There will be an employee chaperone present in each vehicle, and each chaperone is equipped with a tablet allowing them to validate the visitors' tokens, trigger alarm signals, and track their respective visitors.

2.4 Constraints

Constraints are also the limitations of the software and hardware. The central management system is the system that controls all subsystems including the security system, vehicles, and the token generator. Each of the subsections has constraints that they have to communicate to central management system in order to operate fully. The system is composed of physical and hardware components so, each of these component have their limitation. A network failure may result in failure of emergency alarm, fences, vehicle operation and token generation. Similarly, each vehicles are not equipped to handle more

then 10 visitors. The override button in each vehicle is only operable when the administrator at the central management system activates it. The physical emergency button in the vehicle can only be activated by the employee at the central management system. The RFID chip has range of 100m so, we should make sure visitors don't go beyond the range. The assumption of the system is that it follows all the state and national level law for the safety of the visitors and has license to operate the siesta garden. The database in the central management system is accessed by the vehicle management system, kiosk management system to send and receive data but they will not be able manage the database. Only the central management system is authorized to manage the database.

2.5 Assumptions & Dependencies

The SGC system is designed and built to comply with the statutes and regulations (federal, state and local), and assumes that the users will continue to abide by the laws. The T-Rex enclosure along with its level of security is strictly the responsibility of Siesta Gardens. It is assumed that the enclosure will be equipped with an electric fence and sensors as a part of security measures used for the T-Rex enclosure.

In case of breach we have trench to enclose the T-Rex and automatic alarm signal which will allow the system to send signal to the visitors throughout the park to ensure the safety. The self driving vehicles are equipped with visitor tracking, emergency alarm and an employee chaperone to deal with unexpected emergency.In the case of an emergency where the vehicle is not operational or the safety of the passengers is in question, the vehicle should be equipped with a way to override the capabilities of the self driving vehicles including locks and route paths.

The SGC system is equipped with water repellent material for the hardware part like kiosk, vehicles, fences, alarm system, cameras etc. The hardware components can withstand high level of temperature and wind to prevent system failure. The system is equipped to handle any natural disaster but in case of emergency it protects the visitors with appropriate exit process from the SGC.

3 Specific Requirements

This section describes the specific requirements of the SGC related to the external interfaces and control flow.

3.1 External Interfaces

This section describes the controller system's input and output interfaces and the events that trigger particular behaviors for the system. The input interfaces are those with which the user (a general user or a system administrator) interacts, and the output interfaces are those which send signals to other components and users of the system. In the subsections that follow, each interface is listed and described, and events tied to each interface are explained in detail. These interfaces included the central management system, kiosk, security system, employee chaperone tablet, self driving car and override button.

Central Management System The central management system is the main input/output device that administrator monitors and interacts with. The system will utilize a user interface to allow the administrator of the system to monitor ticket sales at the kiosk,

track guests throughout the park, and monitor or activate alarms. Proper functionality of all sub-systems of the SGC requires that the central management system be constantly monitored and controlled by a system administrator.

The central management system receives input from all components of the system as well as provide output to alarm systems. As users operate the kiosk, information they input while purchasing a token is stored within a database of the central management system. Security cameras and fence sensors at the exhibit constantly communicate their current status as well as the integrity of the security system. If any failures of the security system occur, the central management system can activate alarms throughout the park to indicate to guests of a possible emergency. Transport vehicles relay location and occupancy loads to the central management system. The central management system is meant to communicate with all subsystems and respond according to input from these subsystems.

Kiosk The kiosk is the first input device of the SGC that guests interact with and acts as an automated ticket booth. The ticket booth is controlled by the central management system and is responsible for collecting payment and guest information, verifying payment amount, and creating a unique ID to be used to generate a token required for access to the T-Rex exhibit.

The automated ticket booth will utilize an easy to use user interface to allow guests to select an available time slot and input their personal information and payment. The central management system manages time slot availability and guest information within an internal database.

To use the ticket booth, guests will first be presented with a list of available time slots to see the exhibit. Guests can choose any open time slot available for the present day only. Once a time slot is selected, the user will be prompted to enter in their payment information. Payment information includes: the guests full name, address, phone number, and credit card information. Payment information is then validated prior to finalizing the reservation. At any point prior to payment validation if the guest would like to start over they can push a cancel button and be returned to the initial welcome screen displaying the available time slots. If payment cannot be validated, a display message will display to indicate to the guest that their payment has been declined and they will be returned to the welcome screen.

After a time slot has been reserved at the automated booth, the guests name, time slot, assigned vehicle number for the time slot, and the valid until time information will all be communicated and stored at the central management system. A UUID will be generated and loaded onto an RFID chip within a token. The token is required for entry into the exhibit. All RFID information will be communicated to the central management system so that it can be stored with the user's visit information. The RFID within the generated token will be used to track the guest throughout the park and to validate access to the transport vehicle. Transport vehicles and employee tablets contain receivers so the RFID chip can be monitored in all areas of the park. Tokens must remain with each guest throughout the entirety of their visit so their safety can be monitored at all times. Guests cannot exit the park without first depositing their token at an exit terminal. This ensures that an accurate count of visitors at the exhibit is maintained.

Security System The alarm signals are sent from the SGC to each device in the system if there is an emergency. The administrator monitors all alarm signals through

the Central Management System and can activate the manual alarm. In addition, park security can be activated for small scale emergencies. Automatic security features of the T-Rex containment will trigger emergency alarms during a containment failure. This alarm is the same as the Central Management System's manual alarm.

Employee Chaperone Tablet The employee chaperone tablet is the main interactive input device for the vehicle chaperone. Employees will be provided with the tablet so they can interact with the main hub and security system while out in the park. Tablets will be equipped with three applications for this purpose.

The locator app reads signals from the visitor tokens and displays them on a map of the park to allow the employee to locate guests or the tokens themselves should they become lost. To use this app, simply press the application on the home screen and the display will appear. The map allows the user to zoom in to see in closer detail where the tokens are. Tapping a token icon will display the token's identification number. To scan in tokens at the beginning of a tour, press the green button labeled "Scan" in the bottom right corner of the display. This will open a blank screen with the text "Scan tokens now" in the center. Place the visitor tokens close to the tablet to allow it to scan, and the tablet will display the visitor's name for you to confirm their identity. Once scanned, the locator app will show that token's location until the tour is ended and the tokens are deactivated.

The route override app allows the employee to change the route the self driving vehicle will take in the case of an emergency. To use this app, press the application on the home screen to open the display. The display will show the current route of the self driving vehicle. To activate the override, press the orange button labeled "Override" in the bottom right corner of the display. This will clear the route ahead of your vehicle and will enable a drawing mode that will allow the user to draw a new path to avoid the road obstruction. Once the drawn path intersects with the standard path, the rest of the route will default back to its original position. The app will then show a confirmation screen which will lock in the new route. Once confirmed, the self driving vehicle will begin moving along its new path.

The emergency app allows the employee to activate the alarm signal in the case of an emergency where the automatic alarms have not been triggered. To use this app, simply press the application on the home screen to open the display. The display will show a large red button labeled "Alarm." Once pressed, a login screen will pop up asking the employee to enter their ID and confirm that they wish to activate the alarm. Once confirmed, the alarm signal will be sent to the Central Management System where the administrator can decide to activate the, manual, park wide alarm.

Transport Vehicle The transport vehicle is fully automated and is responsible for transporting guests safely to and from the exhibit. The employee chaperone does not control the vehicle and is mainly responsible for acting as a tour guide and monitoring guests. The transport vehicle is equipped to read and track each guests RFID located in their token. Input from the guests tokens and the employee tablet monitor guest occupancy and location. When preparing to return from the exhibit, vehicles need to verify that each guest has boarded prior to closing and locking the doors.

Override Button The override button can be used in the event of an emergency to allow the transport vehicle to leave the exhibit if all passengers cannot return to

the vehicle. The button is initially inactive and can only be activated by the system administrator in an emergency situation. The button is located on the inside door of the transport vehicle. The button acts as a fail safe option if the employee chaperone's tablet becomes damaged or malfunctions. Since the button is inactive until activated by the administrator, accidental pushes will have no result. The doors will only close and lock if the administrator has activated the button.

3.2 Control Logic

The control logic is divided into 4 parts system, user, employee, and administrator. The first diagram outlines the system as a whole, the second diagram outlines how guests interact with the SGC. The third diagram outlines how employee's interact with the SGC through their employee tablet. Lastly, the fourth and fifth diagram outlines how administrators interact with the security component of the SGC and the vehicle.

The below diagram is for the administrator of the system and is meant to display the control logic of the entire system and how it interacts with each component. The administrator overseeing this system can interact with the tokens, tablet's, security, vehicle, and kiosk subsystems.

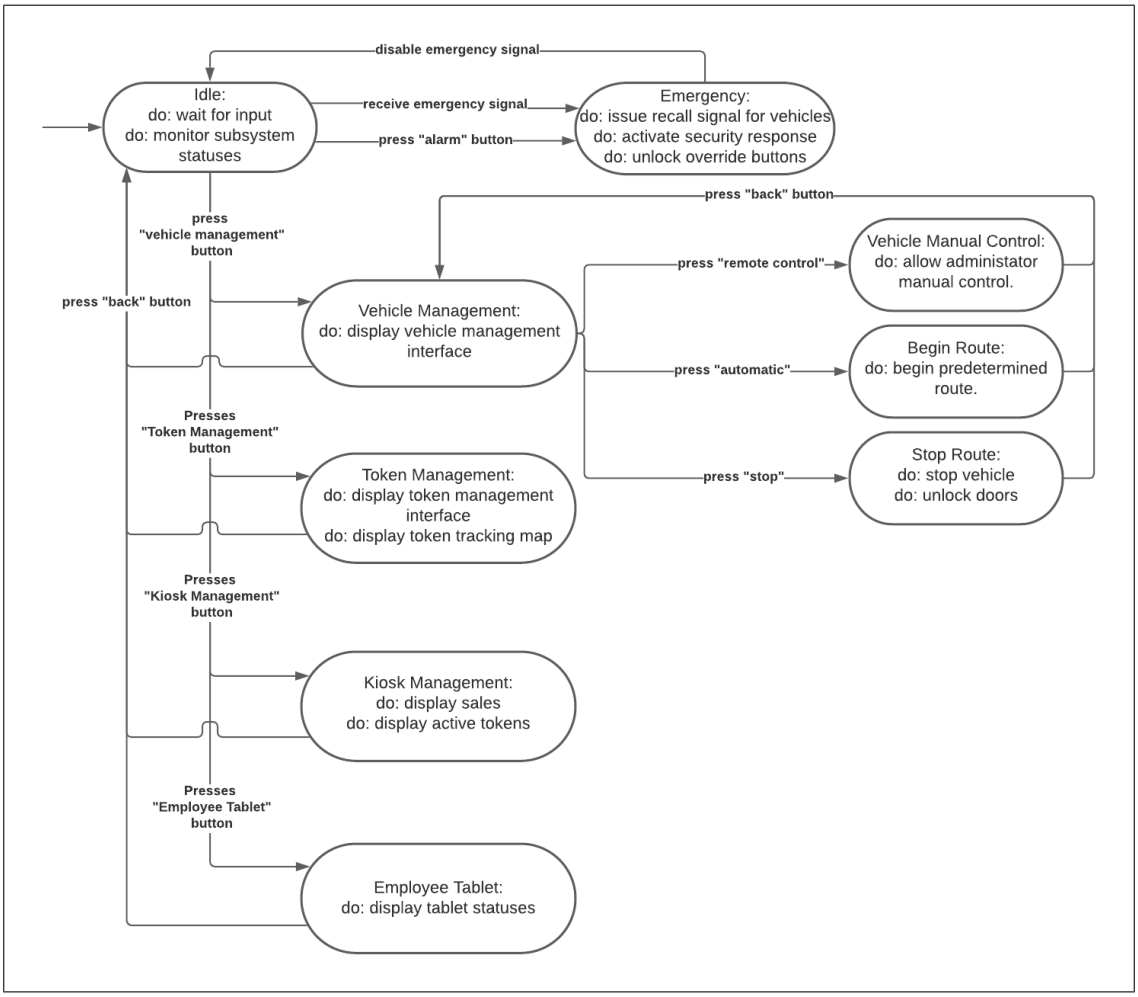

Figure 2: General System OMT Diagram

The below diagram is for the users and details the logic resulting from user input at

the Kiosk. The kiosk starts at the idle state and waits for input from the guest. The kiosk moves between states based on user input. The kiosk returns to its idle state once guest input is completed(token dispensed).

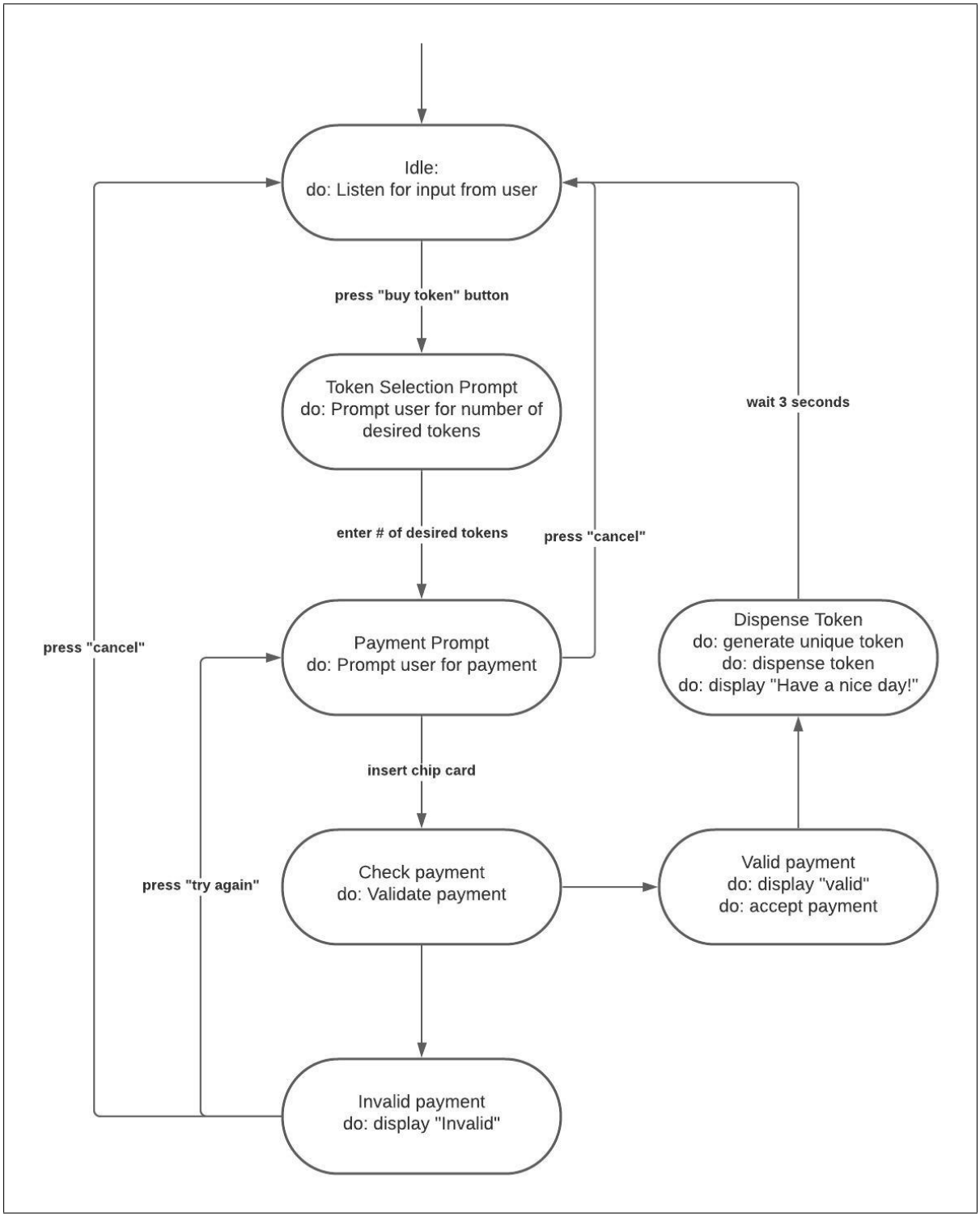

Figure 3: General User (Guest) Kiosk OMT Diagram

The below diagram is for the employee chaperones and outlines the logic resulting from the employee's input into the tablet. Initially the tablet starts at the idle state and waits for input. Based on the employee's input the tablet will transfer to alternate states

related to input and output signals.

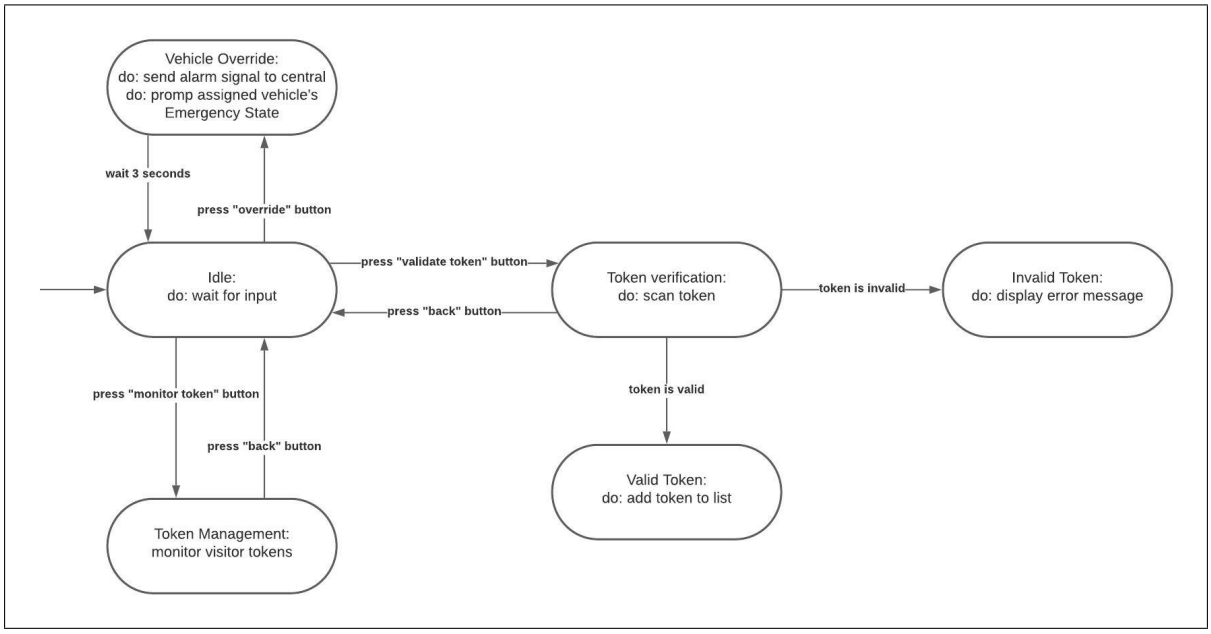

Figure 4: General User (Employee) Tablet OMT Diagram

The below diagram is for administrators of the system and outlines the logic resulting from input to the security system.

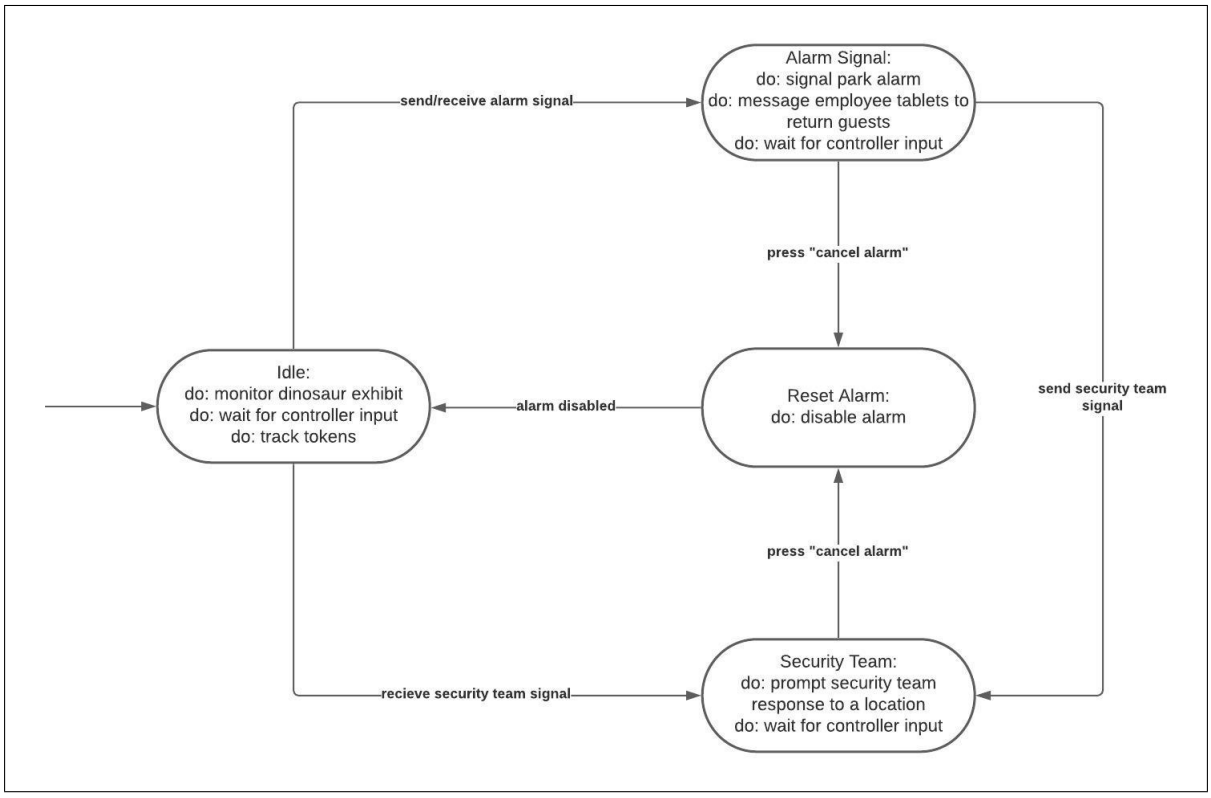

Figure 5: General User (Administrator) Security System OMT Diagram

The below diagram is for the administrator operating the SGC. It allows for precise control over the active vehicles to ensure a safe and fun experience for the visitors.

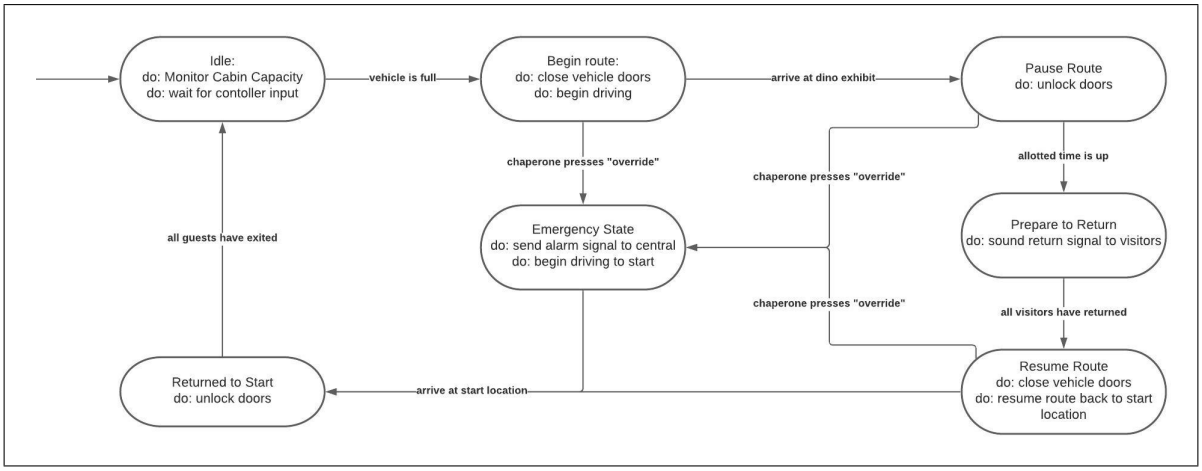

Figure 6: Vehicle OMT Diagram

4 Design Constraints

This section of the document details certain software, hardware, and security constraints associated with the development of the SGC.

4.1 Software Constraints

The system will be developed using the Java programming language. Specifically Java 15.0.02 in conjunction with the Zulu JDK. Any constraints associated with development of the software are limited to the capabilities of the programming language. The SGC will wirelessly communicate with the security, kiosk, employee chaperone tablet, and self driving car systems.

Tablets The employee chaperone Tablet must contain software that is user friendly and does not conflict with the SGC system. The tablets are unable to override the Central Management Systems. The employee chaperone tablet must be fully-charged and functional to be able to operate the SGC system software and fulfill all the mandatory functions of the tablet, such as validating tokens, monitoring or locating visitors, etc. Additionally, employees must be technically proficient and have a good understanding of the SGC system software in order to achieve the expected performance of the system. Additionally, trained I.T. staff should be available during opening hours to resolve any issues caused by the software of the tablets. Each related subsystem will be unavailable if the tablets software fails.

Vehicles The self-driving cars must be outfitted with up to date software to safely operate along their predetermined paths. The administrator of the park must be able to monitor the vehicles path and be able to take manual control should an emergency occur. Each vehicle should have maintenance at least once a week to ensure all on board software is running properly and updated. If the maintenance of the vehicle is not done in timely manner, it can cause the breakdown of the vehicle while in route. If the employee chaperone is not well trained to operate the table that might cause the delay or system failure in vehicle management subsystem.

Tokens Each token must have the ability to store information as well as communicate their location to nearby employee chaperone tablets and receivers. Tokens will be limited by its range to a receiver. when outside its range the tokens will be untraceable to the related subsystems.

4.2 Hardware Constraints

The SGC is a monitored from a central hub that is located near the entrance to the park. From this Hub an administrator will be provided with a screen that displays all the necessary subsystems. The administrator interacts with the SGC through mouse and keyboard.

Manual Alarm In a situation where the manual alarm is unable to be activated, the result could be catastrophic. the manual alarm can only be activated through physical interaction, so an administrator must be present. Without regular maintenance to the device, there is a chance that the device may not function at all. Park staff should be aware of the importance of this device and be responsible for its maintenance.

Network Subsystems of the SGC are wirelessly connected so the quality of the network they are connected to is a major priority. In a situation where the network is damaged or interrupted the overall system may fail to operate properly putting the visitors in danger. Before opening the park, the Network needs to be tested to ensure that all the subsystems will function properly. The park should remain closed until the administrator is confident in the Networks ability.

RFID Many of the tokens operate through the use of an RFID chip and as such the tokens have a relatively small range of 100m. If the token is far away form the sensors then they cant be read which can't guarantee the smooth operation of the vehicle management system.

Database Failure of the database could result from multiple issues such as memory errors, system crashes, human error, etc. Database failure will result in limitations of the SGC software system functions of not being able to store and retrieve visitor information.

Kiosk The park Kiosk must be built such that it is resistant to difficult weather conditions to prevent malfunction year round. Payment through the Kiosk strictly takes electronic cards, this is done to speed up and simplify the purchases of tokens for visitors. The kiosks should be monitored by an employee multiple times throughout the day do ensure that the machines are operating properly. If not monitored and the kiosks fails then the visitors can't get inside the siesta garden which will cause loss of money, until repaired.The internal storage tokens should be also monitored to prevent unauthorized access to the tokens. In general, additional Kiosks should be available to replace the malfunctioning Kiosks.

Vehicles Self driving vehicles require the park to have well maintained roads to drive on to prevent damage to the vehicle and for the safety of the visitors. Failure to maintain the roads may result in the failure of the vehicle, which limits the smooth running of

vehicles. If the vehicle has more then 10 passengers vehicle can't operate smoothly, with extra load it might break. Each vehicle should have the override button conveniently placed where a guest or employee can access it in an emergency. Also a trained staff of mechanics must be available to do maintenance on the self driving vehicles. Without this available staff, the system will be slowed down due to vehicle issues and guest safety may become jeopardised.

Tablets Employee Chaperon Tablets are a subsystem of the overall SGC so as such, device failure will limit other related subsystems. The devices run on a limited battery so unless regularly recharged and maintained, they will be unable to function for a full day. In addition, the software used on the tablets require some technical competence so the efficiency of the tablet will be limited by the proficiency of its user.

4.3 Security Constraints

The SGC is responsible for activating emergency alarms around the park and safely escorting visitors back to the barge that got them onto the island. In situations where the T-Rex is able to escape its enclosure, the SGC is not responsible for re-containment. The SGC don't have required manpower or systems for the containment of T-Rex.

The administrator of the SGC must have the ability to signal for local park security for small scale issues such as a fight, however the SGC is not responsible for the creation of the local park security.

Additionally, the SGC will be interacted with by many users, mainly the administrator and employees with chaperone tablets. As a result, improper use of SGC subsystems may result in false alarms and other accidents if not properly monitored. Staff is expected to be well disciplined to prevent unauthorized access to these subsystems. in addition, improper use of the override button may occur because of its ease of access, but the device will only be active during emergencies to reduce False alarms.