SGC - Siesta Gardens Controller

Software Requirements Specification

SRS Version 1.2

Team 03
27 April 2021

Brandon Stringham (manager)
Shreeman Gautam
Tanner Hunt
Amun Kharel
Cody Crane
Krista Conley

CS 460 Software Engineering

Table of Contents

1 Introduction

"B-STACK" is a software design group consisting of Brandon Stringham, Shreeman Gautam, Tanner Hunt, Amun Kharel, Cody Crane, and Krista Conley. In this Software Requirements Specifications (SRS) document, B-STACK details the project plan for the development of the "Siesta Gardens Controller" software (SGC). This project is funded by billionaire philanthropists who have given the team an unlimited, spare-no-expense budget. Therefore, Siesta Gardens will be an amazing vacation experience with all the state-of-the-art technology and an advanced scientific feat of a real live T. rex for the viewing pleasure of the guests, for a nominal fee. The purpose of this project is to design a theme park control system to track and transport guests safely to and from the T. rex exhibit. This document is intended for developers, designers, and testers working on the "Siesta Gardens Controller". This document is split into five sections:

- Section 1 is the introduction.
- Section 2 provides a general description of the system.
- Section 3 outlines the specific requirements of the system and is split into two sections.
  - Section 3.1 describes the external interfaces with input/output events with the physical devices.
  - Section 3.2 gives a technical approach to the system/system overview by showing the control logic with OMT diagrams.
- Section 4 describes the design constraints that the system will face.
- Section 5 will include the references.

2 General Description

The Siesta Gardens Controller (SGC) is a security and automation system that handles the logistics and safety of the Siesta Gardens Theme Park. The SGC has a central controller, the heart of the system, which coordinates and displays information to central controller operators from three subsystems that handle the park's integral tasks. These three subsystems include the token subsystem, the transportation subsystem and the security subsystem.

The Token subsystem will be responsible for the distribution of unique smart devices to park guests that are used as access tokens to transportation vehicles while also providing real time location data and a means of contacting and informing individual guests.

The Transportation subsystem controls the park's fleet of self-driving vehicles, tracking their passengers, location, and status, and is capable of dispatching extra vehicles to pick up stranded guests in the event that their vehicle breaks down or stalls. The new vehicle will pick up the guests and drive them to their original destination. Park maintenance personnel will handle the retrieval of stranded or broken down vehicles. These vehicles each have their own unique identifier and will register their passengers when they board, via the passengers' unique tokens, and will not leave the exhibit without all of their passengers being accounted for, unless in the case of an emergency.

The Security subsystem monitors the security measures for the exhibit itself. It displays all security camera footage in the central control building, monitors heartbeat data, and monitors logs from the security cameras, electric fence and the T. rex monitor. It also monitors security cameras from around the park and the location data of all visitors, and is also equipped with a PA system. The security subsystem also has a notification system via the guests unique tokens that it can use to alert all guests in the case of an emergency.

Additionally, the SGC has highly trained park staff which include: medical personnel, park maintenance personnel, and roaming security personnel. These personnel can be dispatched by central controller operators via walkie talkie.

Figure 1 displays the physical layout of the components. The security cameras and PA speakers all around the key communicate with the central control building via buried cables. The electric fence and token kiosks also communicate with the central control via buried cables. The RFID scanners around the park used to locate guest bracelets are connected together via a network of buried cables that then connect to the central control. The RFID bracelets communicate with these scanners and the kiosks using near field radio signals. The self driving cars communicate with the central control via radio signals as they drive around the park.

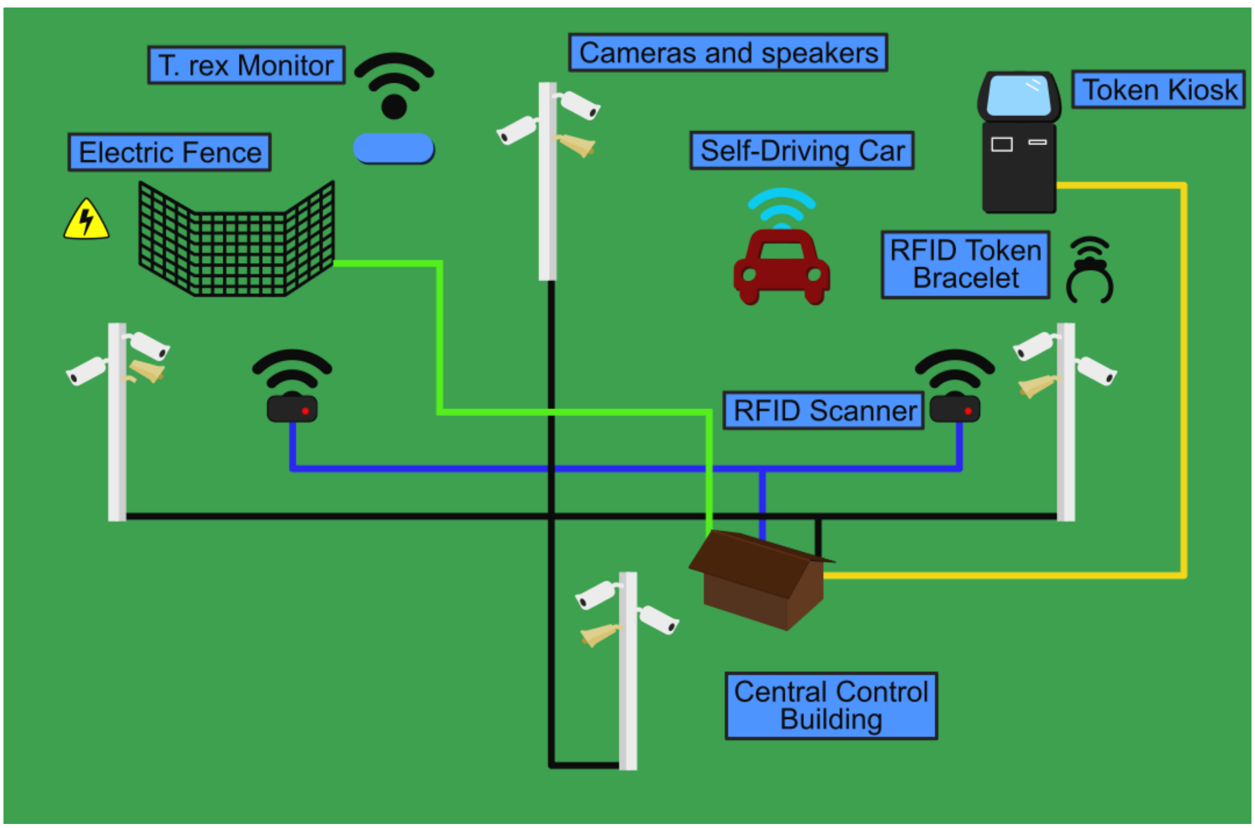

Figure 1 - The physical diagram

3 Specific Requirements

This section details the specific requirements for the system. These requirements include the external interfaces that the system needs to be able to communicate with to accomplish its goal, and the control logic that it needs to implement to function properly. Figure 2 shows the logical diagram of the system.

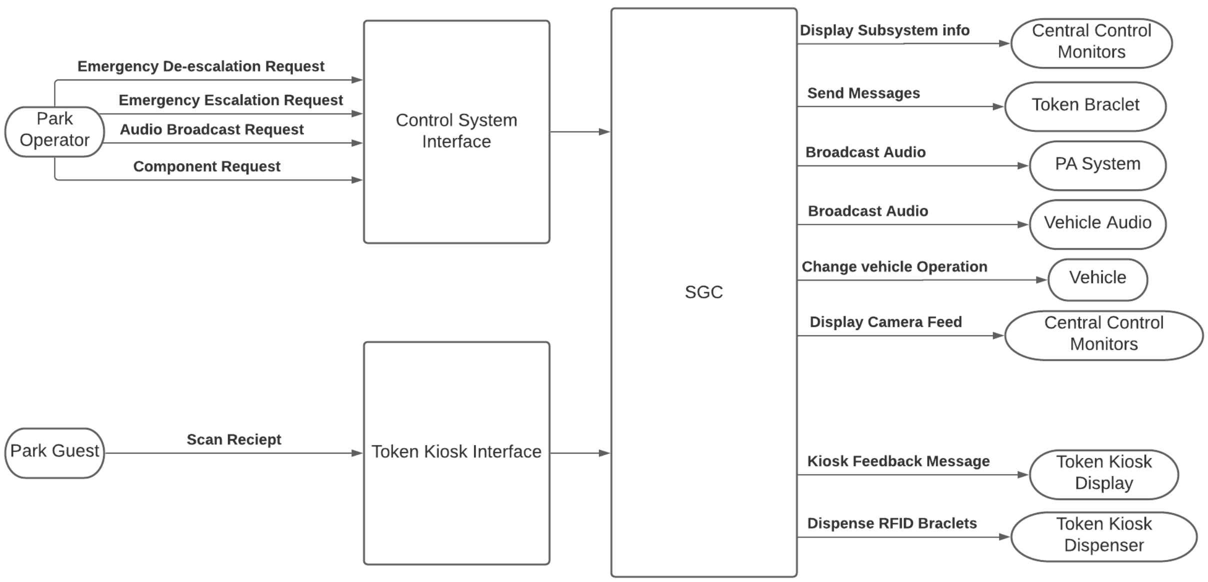

Figure 2 - Logical Diagram

3.1 External Interfaces

The SGC system is a complex system made up of many moving parts. Each of these parts need to communicate with all of their attached devices. These are the external interfaces needed for the central controller: the token system with its bracelets and kiosks; the transportation system with its cars; and the security system with cameras, fence, RFID scanners, the T. rex monitor, and PA speakers.

3.1.1 Central Controller Interface

The Central Controller interface serves as the main hub for monitoring and controlling the various subsystems of the SGC. The interface is to be used by trained Siesta Gardens employee operators. It will be a graphical user interface running on a desktop machine connected to the SGC network and it will be installed in the Siesta Garden's control building.

The Central Controller interface will largely be dedicated to monitoring the operational status of each subsystem. There will be a high-level table that displays each subsystem's overall status. Each subsystem will also be represented with a collapsible lower-level table that provides operators with operational information unique to the individual components included in each subsystem. All of these tables are updated in real time. The interface also has some interactive elements allowing the operators to send commands to the various components of the SGC and also initiate emergency evacuations . Additionally, video feeds from the security subsystem will be displayed on multiple monitors.

3.1.2 Token System

The Token system will consist of the software and the external devices that the park guests first interact with upon arrival on the Key. There is two-way communication between the software system and the Token Kiosk and Token Bracelets external interfaces. The token system uses an API to validate token purchase receipts with the park website where guests pre-purchase their tokens.

3.1.2.1 Kiosk Interface

The token kiosk is the hardware device that will accept receipts from the guests. The guest inputs their receipt into the token kiosk. The kiosk will either accept or deny the guest based on the validity of the receipt. If the kiosk system accepts the receipt, it will dispense the correct number of tokens, which are RFID bracelets, and then send the guest names, dates, and unique identifiers of each bracelet to central control. If the receipt is denied, then the kiosk software will send this error to central control and alerts the guests of this problem.

3.1.2.2 Token Bracelet Interface

The token Bracelets use RFID technology. The bracelets send out radio signals constantly to the RFID scanners located around the park and in the vehicles. This software interface is used to track the guests in real time to ensure their safety. It is also used by the vehicles to track on board guests.

The RFID bracelets have a smartwatch type display that will alert and display messages to the guests. It will also have haptic feedback and will vibrate to get the guest's attention when there is an alert.

3.1.3 Transportation System

The transportation system involves the park's fleet of automated vehicles that transport guests to and from the exhibit. These vehicles are responsible for ensuring the passengers' safety during transit, and they transport the guests back to the barges in the event of an emergency. The vehicles relay their location, passenger list, and vehicle status data to Central Control where it is monitored. The vehicles will have names as identifiers so that the guests can easily remember which vehicle is theirs. The maximum capacity of each vehicle is 10 people. In the event of a stranded or broken down vehicle, central control will receive an alert and can dispatch a new vehicle to pick up the stranded guests. The stranded guests will be registered with the new vehicle upon boarding. The turnaround time is at most 15 minutes in delay due to the efficiency of having cars parked on both sides of the key.

Each car is equipped with a physical interface that handles the guests' interaction with the vehicle and, through the vehicle, Central Control. This interface handles registering a token with a vehicle before it departs for the exhibit and ensuring that all guests that registered with that vehicle are accounted for before leaving the exhibit. To accomplish this, the vehicle uses the installed RFID scanner to scan the bracelets of each of its passengers when they enter the vehicle for the first time. After the thirty minute viewing period, the vehicle will sound an alert to guests in the area that they should begin boarding their assigned vehicles. This alert is accompanied by a message sent to the token bracelets of the vehicles' registered passengers. Once all passengers have boarded, as determined by the presence of their RFID tokens, the vehicle may leave the exhibit. If guests try to board a vehicle that they are not assigned to, the guests are notified by their token bracelet to leave the vehicle. Additionally, central control is notified and can dispatch security personnel in the event that the guest does not comply.

3.1.4 Security System

The security system monitors the fence, streams security camera feeds, and has announcement speakers around the park for the safety of the guests. The electric fence has monitors that alert central control if the fence goes offline, and the whole park is surrounded with security cameras which park staff can use to ensure there is no enclosure breach, or any other security issue.

3.1.4.1 Electric Fence Interface

The electric fence system consists of a main power supply and it includes nodes along the fence that are constantly checking the status of the fence. Each node will send the fence status to the central control via a buried hardline.

3.1.4.2 Security Camera Interface

The security camera system consists of high resolution lenses which are distributed throughout the park to monitor the guests and the T. Rex. Each security camera will send video feeds to central control.

3.1.4.3 PA Speaker Interface

The loud speaker system consists of speakers which are distributed throughout the park to broadcast announcements and alerts from central control.

3.1.4.4 T. rex monitor Interface

The T. rex monitor system consists of a GPS tracking chip surgically embedded inside the dinosaur. The tracking chip sends the dinosaur’s location to central control.

3.1.4.5 RFID Scanner Interface

The RFID scanner system consists of RFID scanners which are distributed throughout the park and in the cars to track guest location. Each RFID scanner will send guest location data to central control.

3.2 Control Logic

The Control Logic of the SGC system explains all the different states that the subsystems have. The subsystems: Token System, Transportation System, and Security System will always start and return to the idle state and will have numerous states of transition. Central control works with all these subsystems to comprise the SGC.

The SGC system first starts up the central controller which will bring all these subsystems online. The park closes to the public for normal maintenance on Sundays and for unexpected inspections by the Florida Wildlife Commission. In the event of park closure, everything except the cameras, the T. rex monitor and the electric fence are disabled from central control. Additionally, the feeds from the cameras and the logs from the T. rex monitor and the fence are monitored by central control operators. The cars will be parked, the kiosks and the RFID scanners go offline and the loudspeakers are turned off. After the park opens up again, the aforementioned disabled components will become enabled again.

3.2.1 Transportation

The vehicles in the system work together to transport guests and have two different modes of operation, normal and emergency vehicle operations. If an emergency override message is received, emergency vehicle operations will be invoked and after the emergency has been handled, normal vehicle operations will be invoked. The transition between normal and emergency operations is laid out in Figure 3.

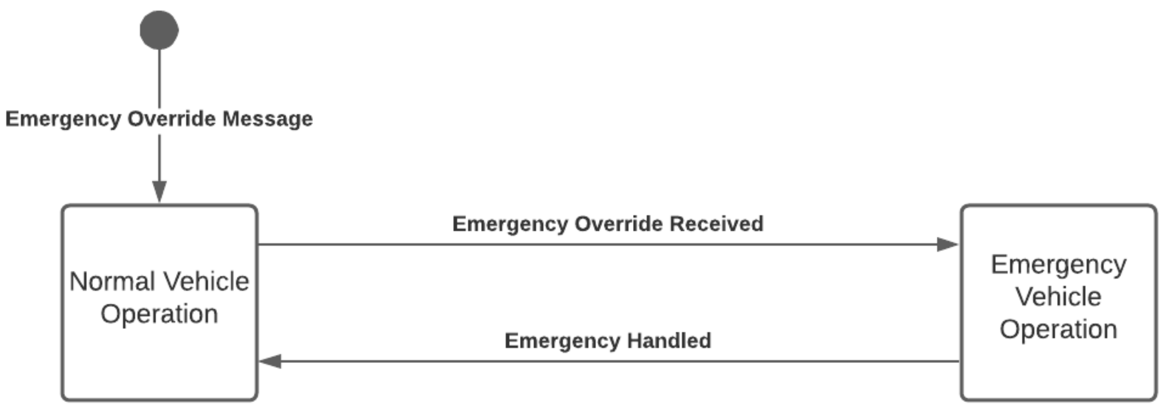

Figure 3 - Normal/Emergency Vehicle Operation Transition Control Logic

3.2.1.1 Normal Vehicle Operations

In normal operations, the functionality of vehicles can be expressed with ten distinct states: Idle, Registration, Capacity Check, Store Passenger Count, Departure, Counting, Authentication, Token Update, Viewing Idle and Travel, laid out in Figure 4.

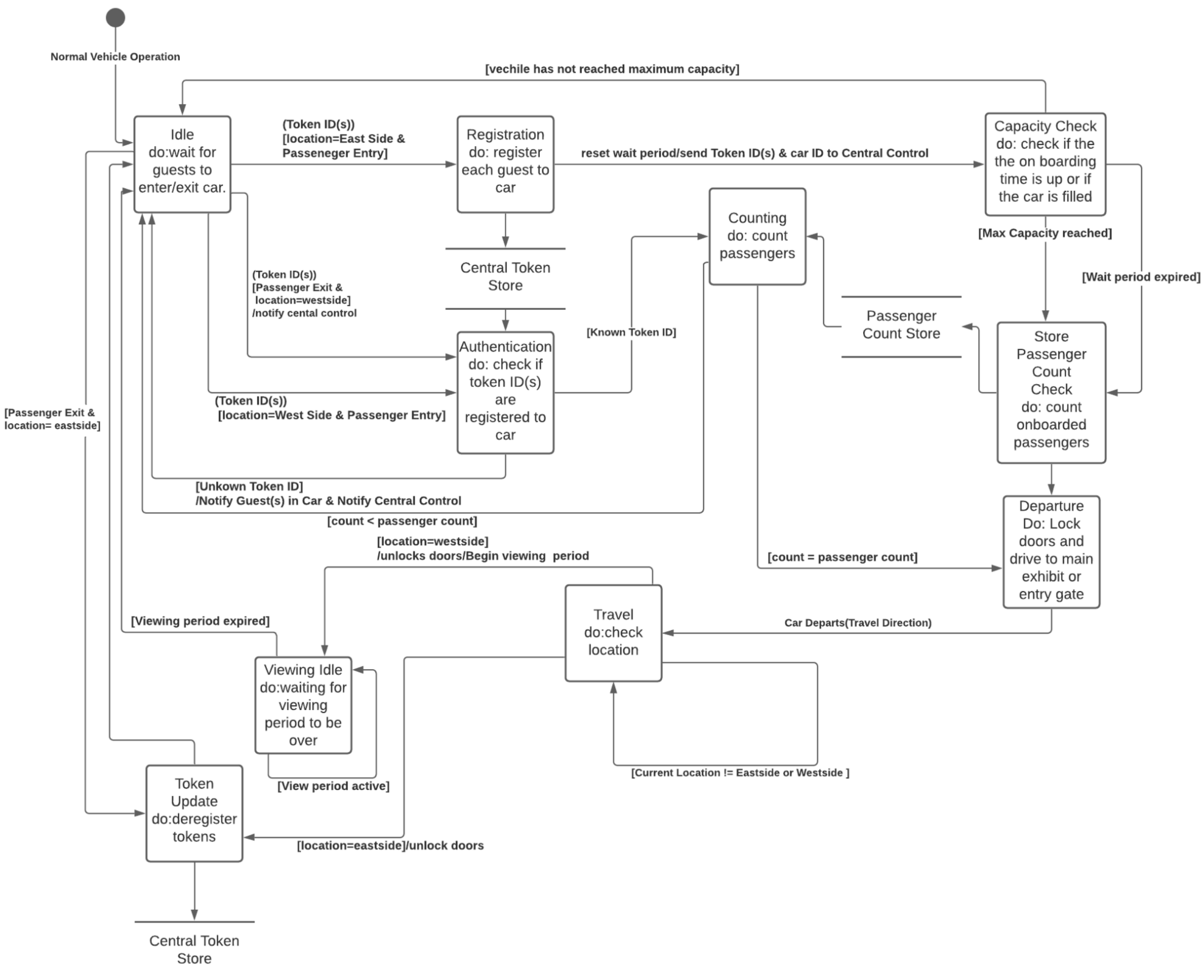

Figure 4 - Normal Vehicle Operation Control Logic

When in the idle state, the system waits for the guests to enter a car. The flow of the diagram now depends on whether the car is at the east side or the west side of the key. If the car's location is on the east side of the key, it means that the guests are going from the main entrance to the main exhibit. Accordingly, these guests need to be registered into the system. So, if the car is on the east side, the registration state registers each guest to a car.

After each registration, a waiting period is reset and the token ID(s) and the car ID is sent to central control. Further, the token store in the vehicle stores the ID(s) registered to that specific car. The capacity check state checks whether the car has reached full capacity or if the waiting time has expired. If maximum capacity has not yet been reached or if the wait period has not expired, control is passed back to the idle state.

If maximum capacity has been reached or the waiting period has expired, control is passed to the store passenger count state. The store passenger count state counts the number of onboard passengers and stores that number in the passenger count store.

Control is now passed to the departure state. In this state, the doors are locked and the passengers are driven to the main exhibit. Control is now passed to the travel state, where the guests are driven through the scenic route into the main exhibit, where the location of the cars are checked. If the location is on the west side, the doors are unlocked and the passengers are dropped off into the viewing area on the west side. While the guests are at the main exhibit, control passes to the viewing idle state where the car waits for the viewing period to expire.

After the viewing period has expired, control returns back to the idle state but the cars are on the west side. If the cars are on the west side, control is passed to the authentication state where the token ID(s) registered to a car are verified with the token store. If the token ID is not registered with a car, the guest(s) are notified to go to their correct car, and control is passed back to the idle state again. At the same time, the number of passengers in that car are counted by the counting state, using the passenger count store.

After the unregistered guest(s) have left the car and if the current number of guests is equal to the previous number of guests and all the current unique token ID(s) match the previous unique token ID(s), control is passed to the departure state, where the doors are locked and the passengers are driven to the main entrance. Control is again passed back to the travel state, where the guests are driven back to the main entrance along the scenic route.

After the traveling time has finished, the car's location is checked and if it is on the east side, control is passed to the token update state. In the token update state, the Central Token Store is updated by invalidating the off boarding passengers unique token ID. The doors are unlocked and the tokens are taken from the guests by park staff, these tokens are invalidated and will no longer be used for that day. After that has been accomplished, the car returns back to the idle state and waits for a new set of guests to start another cycle.

3.2.1.2 Emergency Vehicle Operations

In emergency operations, the functionality can be expressed with five distinct states: Idle, Capacity Check, Departure, Travel and Park, laid out in Figure 5. The control flow begins at the idle state and ends at the parking state. As can be seen, in an emergency situation, authentication is not required because people need to be taken out of the main exhibit as quickly as possible.

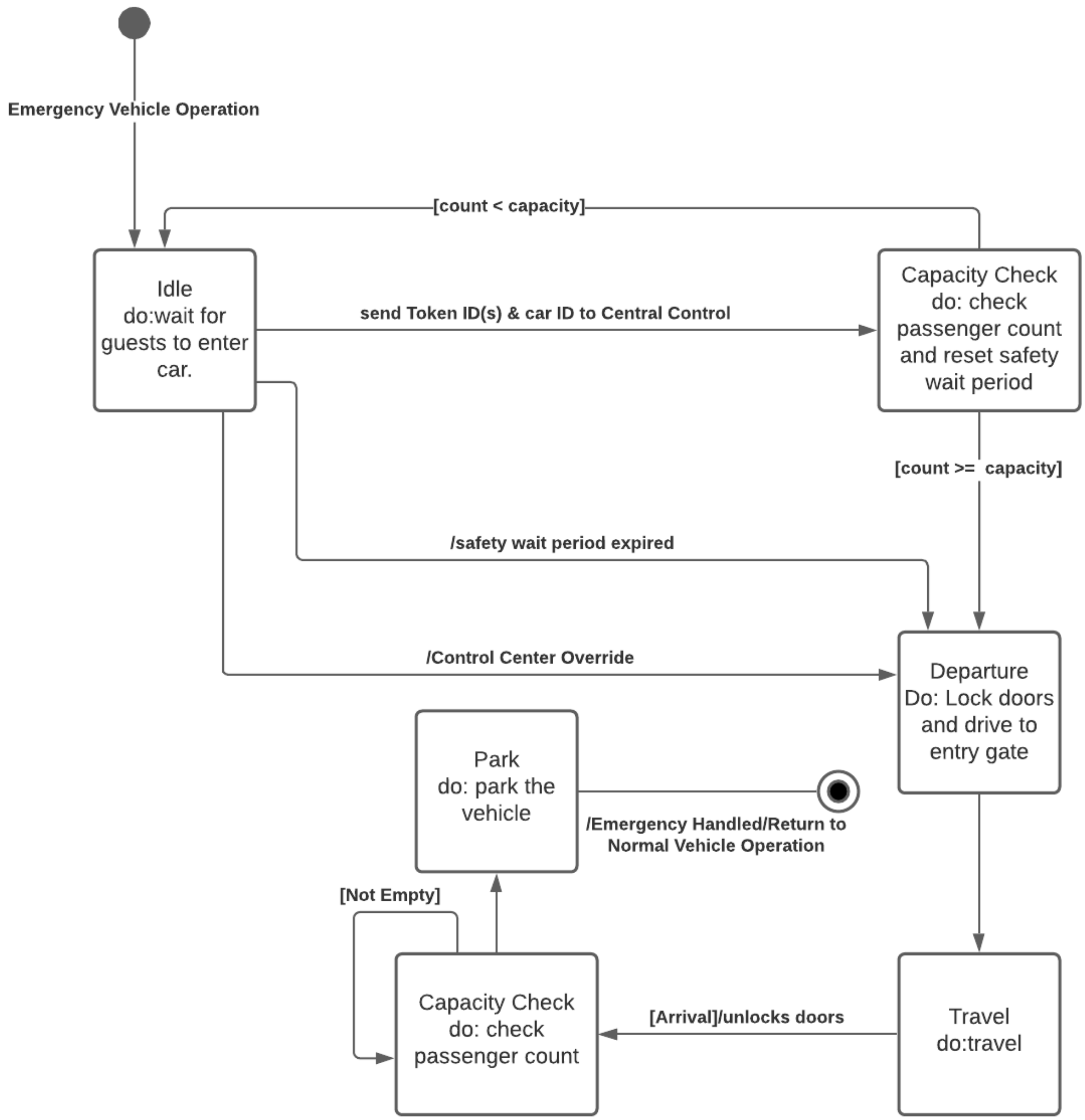

Figure 5 - Emergency Vehicle Operation Control Logic

When in the idle state, the system waits for guest(s) to enter a car. The token ID(s) of the guests and the Car ID is sent to central control.

Control is now passed to the capacity check state where the number of passengers are counted and the safety wait period is reset. If the current capacity is less than the maximum capacity, control is passed to the idle state again. If the current capacity is greater than or equal to the maximum capacity, control is passed to the departure state. If current capacity is greater than maximum capacity, it means that more than 10 guests boarded the vehicle but the vehicle is okay with that because it is an emergency situation. In an emergency situation, the control center overrides the state of capacity check to pass the control from the idle to the departure state. Further, if the safety wait period has expired, control passes from the idle to the departure state.

In the departure state, the doors are locked and in the travel state, the guests are driven back to the main entrance, where the doors are unlocked and the guests are let out.

Control is passed to the capacity check state, where the number of passengers are counted. If the number is zero, control is passed to the parking state, in which the car is parked at the parking lot by the main entrance. If the number is greater than zero, control is passed back again to the capacity check state until the number is zero. After the emergency situation has been handled, the vehicle returns to normal operation again.

3.2.2 Tokens

The token kiosks and the RFID bracelets work together as the token system to validate guests’ purchases, give them access to the park, and help provide a means for the central control to track the guests during their park visit. The kiosks will verify guest receipts with central control and dispense token bracelets to the guests.

3.2.2.1 Token Kiosks

The functionality of the token kiosk component can be expressed with four distinct states: Idle, Authentication, Programming, and Dispense Token, laid out in Figure 6.

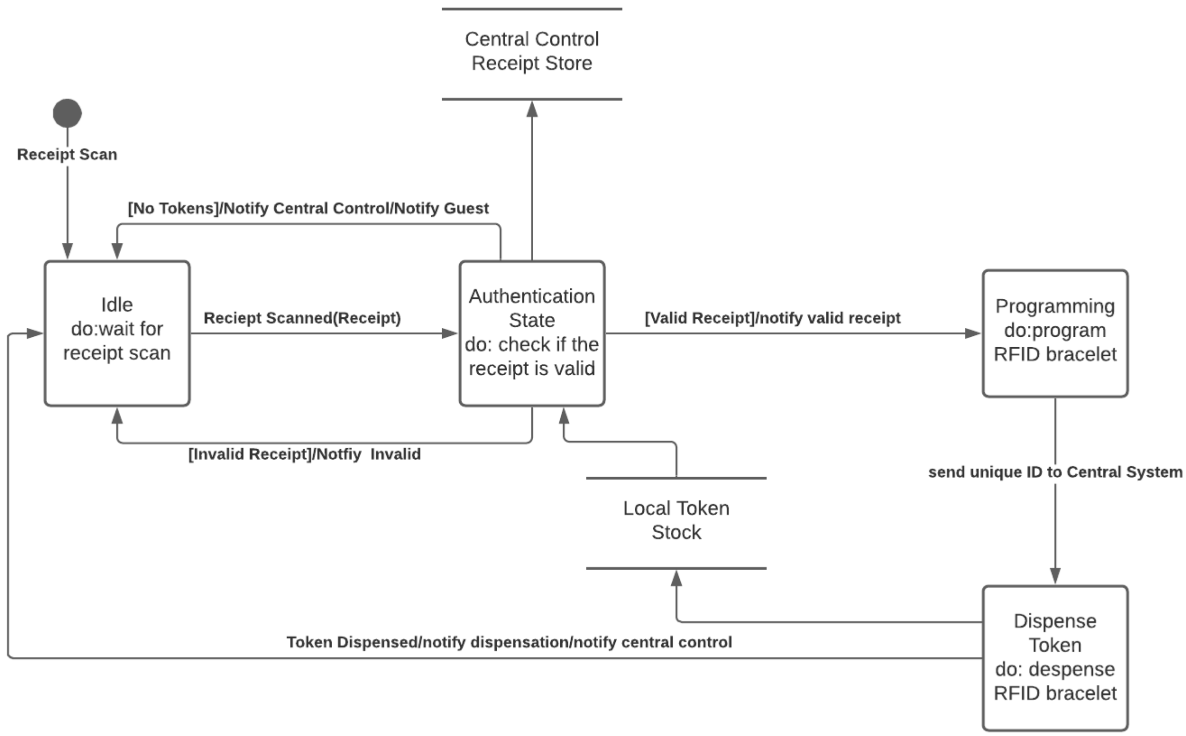

Figure 6 - Token Kiosks Control Logic

When in the idle state, after a receipt has been received and scanned, control is passed to the authentication state. The receipt is checked for validity using the central control receipt store, and if the receipt is invalid, the kiosk displays an invalid receipt message and control is passed back to the idle state.

This system has multiple token kiosks. If a token kiosk runs out of token bracelets, then it will show a “No Tokens” display when a guest attempts to scan a receipt and tell the guest to use another kiosk. If the receipt is valid and token bracelets are available, control is passed to the programming state, where the RFID bracelet is programmed, the unique ID of the RFID bracelet is sent to the token system and control is passed to the dispense token state.

In the dispense token state, a token kiosk accesses the local token stock and since the kiosk has tokens to give, the guests are notified of the dispensation and central control is notified. Control is passed back to the idle state again.

3.2.2.2 RFID bracelets

The bracelet waits for messages from the token system and updates the display message to the guests. The bracelet also sends heartbeat messages to the token system.

3.2.3 Security

The security devices each communicate their status information with central control to protect the park guests. The security cameras are constantly streaming their feeds to the central control where it is viewed by park operators. The electric fence constantly sends the status information of each of its nodes to the central control to ensure that the nodes are still online. The T. rex monitor chip also sends constant updates to the central control with the location and vital signs of the dinosaur. The RFID scanners will constantly send the list of guests that are within their vicinities to central control. Finally, the loudspeakers wait for central control to tell them to play audio alerts and messages to notify park guests.

3.2.4 Central Control

The central control communicates with all other subsystems to operate the SGC. Specifically, central control handles subsystem messages, emergency management, and protected and non-protected requests from control center operators to control the park.

3.2.4.1 Subsystem Message Handling

When in the idle state, after a message has been received from a subsystem, control is passed to the update status table. In the update status state, the subsystem status table is updated and then subsystem status tables are checked for critical faults in the check status state. If there are no critical faults or if there are non-critical faults, which require an operator intervention, control is passed to the idle state. If a critical fault is detected, control is passed to the emergency intervention timeout state. This is shown in Figure 7.

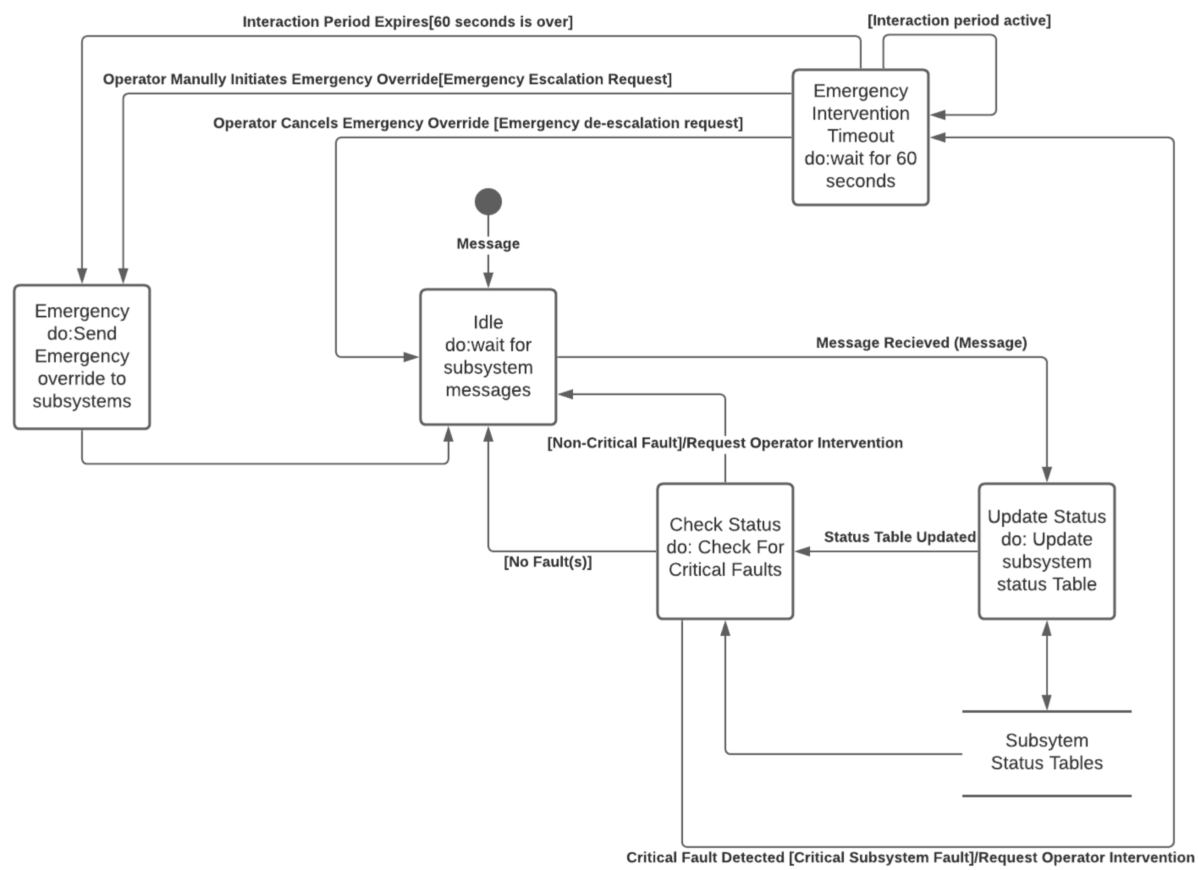

Figure 7 - Subsystem Message Handling Control Logic

3.2.4.2 Emergency management

If central control detects a critical fault in a subsystem, control passes to the emergency intervention timeout state. In the emergency intervention timeout state, the system waits for sixty seconds for an operator to investigate the fault and determine if the event needs to be escalated. If an operator determines the fault requires evacuation, then they will manually initiate an emergency override and control is passed to the emergency state. If the operator determines that the fault is a minor device failure that does not require an evacuation, the operator can cancel the emergency override, and control is passed from the emergency intervention timeout to the idle state. If the operator is incapacitated or otherwise fails to intervene before the sixty second timeout is over, then the control is automatically passed to the emergency state in which an emergency override is sent to subsystems to trigger an evacuation. After a successful evacuation, control is passed to the idle state, in which the system waits for subsystem messages again. This behavior is detailed in Figure 7.

3.2.4.3 Request Handling

The request handling section handles any commands requested by the park operators. Most of these requests would trigger messages to the subsystems. The request handling functionality can be expressed with three distinct states: Idle, Request handling and Authentication, laid out in Figure 8.

In the idle state, central control waits for a request and sends that request to the request handling state. If the request is a protected request, control is passed to the authentication state, where the entered password is checked against a password store. If the password is correct, the request is executed and control is passed to the idle state. If the password is incorrect or the password entering time has expired, there is a failure notification and control is passed back to the idle state. If the request is a non-protected request, a password is not required. The request is executed and the control is passed back to the idle state.

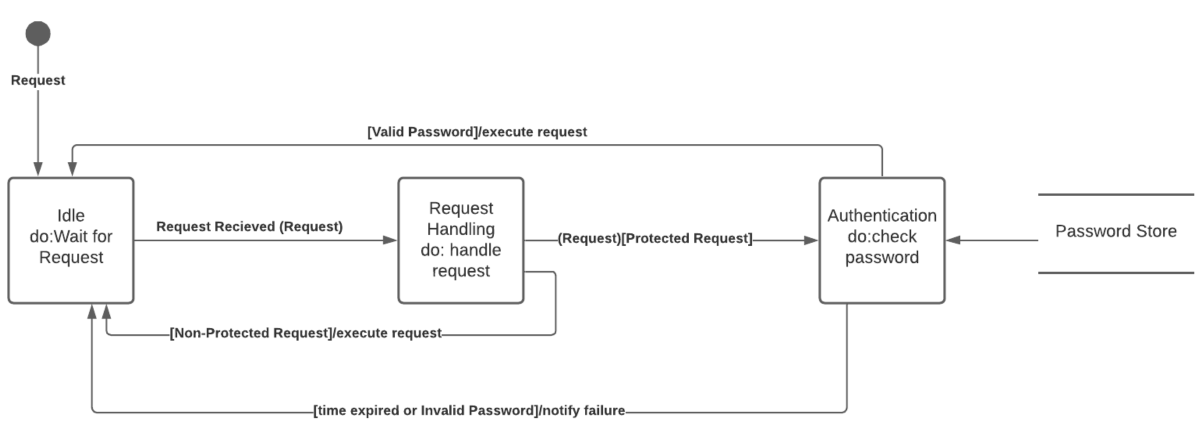

Figure 8 - Request Handling Control Logic

4 Design Constraints

The system has limitations that are enforced on it by the constraints of the system. Some of these constraints are caused by ethical concerns, some by nature, some by engineering and physical space, and others by the demands of the guests.

4.1 Operating Schedule

The park schedule is constrained by the park's need for daylight and occasional maintenance. Because the dinosaur is only visible during the day and we do not want to disrupt its sleep schedule with night lights, the park schedule will be limited from sunrise to sunset. Since the park will need routine maintenance and occasional software updates, the park will only be open from Monday to Saturday. On Sunday, park staff can conduct any necessary maintenance.

4.2 Severe Weather

The park's schedule and equipment are constrained by severe weather. The park will be closed to the public during major weather events, such as a hurricane, to protect the public. However, the SGC control system will still need to operate all security and emergency features to maintain the dinosaur enclosure. This requires the use of surge protectors on all circuits, back-up power generators to run the system, and automatic reboots if the system goes offline. The communication wires between subsystems and the central control building also need to be insulated cable buried underground to protect from the weather. The electrical fence also needs to be designed in a way that it will not be adversely affected by rain. The park will remain open during normal inclement weather such as rain or mild wind. These protections help ensure that the park is fully operational at all times for the safety of the park staff and guests.

4.3 Guest Privacy

The system is required to track guests using cameras and RFID bracelets while they are at the park. To respect guest privacy, after three months, the aggregated data of the guests will be purged from the system. In that sense, the system is constrained by guest privacy to not hold guest information like name, camera footage and payment method after three months.

4.4 Guest Tracking

The system is constrained to have passenger cars, as opposed to letting guests roam on foot, so that they are accounted for while they are in transit to the exhibit, so that they can easily escape in the event of an emergency and so that their time is not wasted and they don't risk getting tired while walking to the exhibit.

4.5 Natural Habitat

Some of the construction of the island is constrained by wanting to keep the feel of a natural habitat and safari for the guests and the dinosaur. This is because the self-driving cars will only follow one predefined road to the enclosure so they do not tear up the terrain and degrade the experience for the guests.

The enclosure design also needs to look natural for the dinosaur, therefore the security cameras inside the exhibit need to be disguised as a part of the local fauna. The exhibit will need to have many lines of visibility so the guests get the best chance of viewing the T. rex, but the enclosure needs to retain a natural look and so there may still be parts of the enclosure that guests cannot see.

4.6 Car Limitations

Due to the limited amount of space on the key, the number of cars is constrained to be ten vehicles that the system can use. For the safety of the park guests, five of these cars must be kept in reserve as spare cars in the parking lot near the enclosure to evacuate guests in the case of an enclosure failure. Each car can hold up to ten people.

4.7 Emergency Automation

Emergency management is constrained such that it cannot trigger an emergency response unless several conditions are met to prevent needless guest hysteria. In the case of a single system failure like the gate or GPS, the emergency management module will alert the control center staff, but it cannot start evacuation procedures without their approval in case it is a sensor malfunction. If however, the staff do not respond to the alert within one minute, the system can begin emergency procedures in case the staff is somehow incapacitated.

Due to the short response time required, there must always be at least two staff in the control center at a time.

4.8 Automated Status Limitation

Not all systems have the capabilities to send constant heartbeat updates to the controllers, thus these systems will need to be manually checked during weekly maintenance. The announcement speakers need to be manually checked each week since they are regular speakers and can only play audio without being able to send back device health updates.

4.9 Animal Welfare

Due to the Animal Welfare Act, there exists a constraint such that the welfare of the animal must be kept in high regards.[1] The habitat will be cleaned and if for some reason the animal needs medical attention then the park will unexpectedly close down but the park will issue refunds to the affected guests. The Florida wildlife commission regulates the cleanliness and the humane treatment of wildlife. [2] Therefore, unexpected inspections may occur and the park will have to shut down temporarily to abide by state laws.

5 References

[1] “Animal Welfare Act,” *NAL*. [Online]. Available:

https://www.nal.usda.gov/awic/animal-welfare-act. [Accessed: 09-Apr-2021].

[2] “FWC Overview,” *Florida Fish And Wildlife Conservation Commission*. [Online]. Available:

https://myfwc.com/about/overview/. [Accessed: 09-Apr-2021].