STPA Analysis of Fully Autonomous Robotaxi
Maddie Golison
12/02/22

Part 1

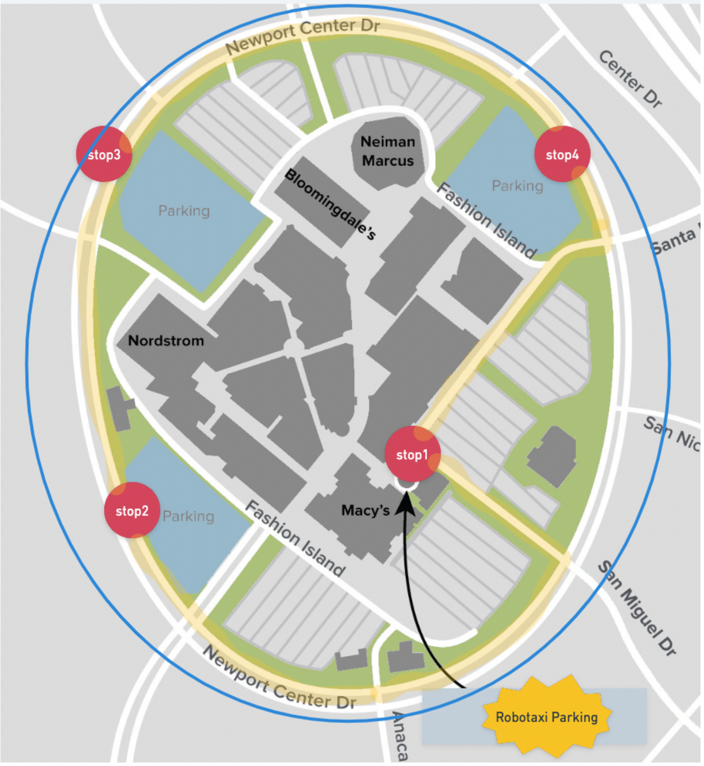
System:

- The system includes a fully autonomous robotaxi within a geofenced semi-public loop.
- The actors in the system include the robotaxi, passengers, semi-public roads, weather, pedestrians, bikers, local businesses, other non-autonomous vehicles and other robotaxis.

In the rest of the analysis the developer and supplier of the robotaxi will be referred to as RoboGo, but the vehicle and its capabilities will be based off of the Cruise robotaxi (https://getcruise.com/).

This system, in other contexts (https://techcrunch.com/2022/06/30/cruise-robotaxis-blocked-traffic-for-hours-on-this-san-francisco-street/), has had accidents. These accidents are related to an incorrect understanding of the environment by the software system.

System Boundary:



System Image 1: sourced from https://lincolnexperiencecenter.com/Content/img/FashionIsland_LECMap.jpeg

The blue line represents the boundary, which is a geofencing mechanism that prevents the robotaxi from navigating from outside this area. The highlighted area is the predefined route of the robotaxi, where it can go from stop 1 to stop 4, and then ends back at stop 1. This is a hypothetical space where the robotaxi might be used on a semi-public route. This is a large, outdoor mall in southern California that has a loop around it, which is a road where visitors can navigate to either the surrounding business or the mall directly.

Goals:

- To provide fast, convenient and safe transit between areas of the outdoor mall
- Reduce the amount of other cars driving between areas of the mall to reduce traffic and increase safety
- Reduce the amount of time people spend walking to different shopping areas to improve the shopper satisfaction and increase the amount of money they spend
- Reduce foot traffic on busy streets and intersections to increase pedestrian safety

Part 2

Define the accidents (losses) and hazards of importance to the stakeholders. Write the related system constraints. Select one or two important ones to analyze.

Stakeholders:

- People visiting the shopping mall and businesses at Fashion Island
- The businesses in and around the shopping center
- Company that has provided the robotaxis - RoboGo

Potential Losses:

- L-1 Damage to vehicles or other physical property
- L-2 Loss of human life
- L-3 Loss of time (mission loss - the vehicle does not get the riders to the next destination faster than walking)
- L-4 Loss of business to the shopping center (loss of reputation)

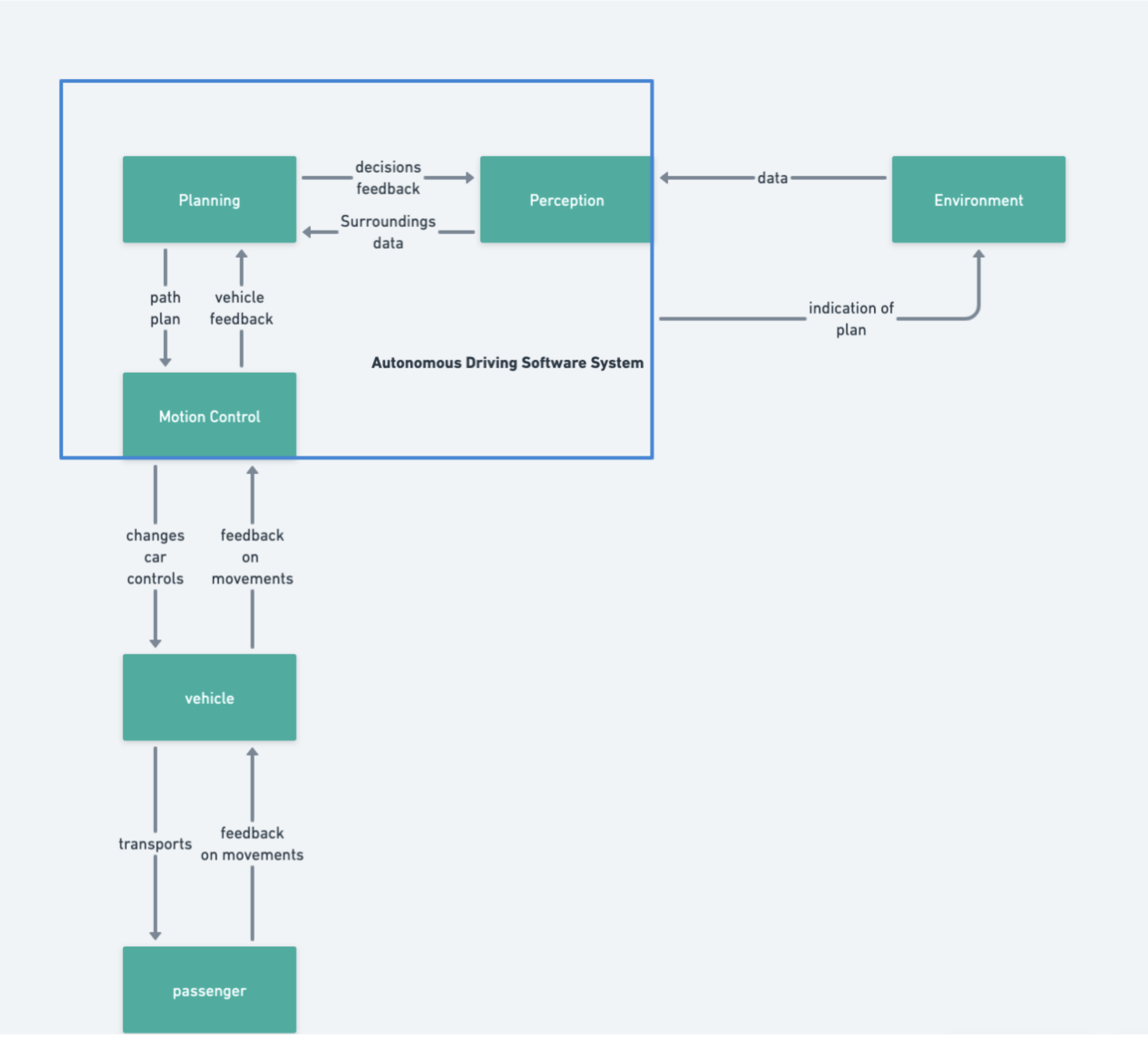
Hazards:

- H-1 Robotaxi does not maintain safe distance from nearby objects [L-1, L-2]
- H-2 Robotaxi does not move as expected on the predefined route (moving too slowly, randomly stopping, or other unexpected behaviors) [L-3, L-4]

System Constraints:

- The robotaxi must only operate in the predefined route
- The robotaxi must maintain a safe distance from objects and other system participants
- The robotaxi must not operate over 25 mph

Part 3
Control Structure



The "environment" includes all non-passenger participants that interface with our robotaxi system. This includes the following:

- Traffic system: stop signs, street lights, crosswalks, etc
- Motorized participants on the following: motorcycles, e-bikes, semi-autonomous cars, manual cars
- Non-motorized participants: bicyclists, pedestrians
- Natural system elements: weather (rain, wind, sun), earthquakes

When considering the unsafe control actions we can think of the above when considering the overall operating environment.

Part 4
Potential Unsafe Control Actions

Human Operator: Passenger

UCAs	Not providing causes hazard	Providing causes hazard	Too early, too late, order	Stopped too soon/applied too long
Enters vehicle	Passenger does not enter vehicle when the vehicle is expecting a boarding [H-2]	Passenger enters vehicle when vehicle is not expecting [H-2]	Passenger enters vehicle before the car is in park or after the car has begun driving [H-2]	Passenger does not definitively get into the vehicle (leaves door open, halfway out, etc) [H-2]
Exits vehicle	Passenger does not exit vehicle when the vehicle is expecting an exit [H-2]	Passenger exits vehicle when vehicle is not expecting [H-2]	Passenger exits vehicle before the car is in park or after the car has begun driving [H-2]	Passenger does not definitively get out of the vehicle (leaves door open, halfway out, etc) [H-2]

Automated Software: Autonomous Driving Software System

UCAs	Not providing causes hazard	Providing causes hazard	Too early, too late, order	Stopped too soon/applied too long
Indicating plan	ADS does not indicate when stopping/slowing or changing lanes/turning [H-1]	ADS indicates slowing or changing direction when the vehicle does not intend to [H-1]	ADS indicates too late for other traffic participants to know the vehicle's intent. ADS indicates before behavior intent is decided [H-1]	ADS stops indicating before vehicle change has completed [H-1] ADS continues to indicate after intent has completed [H-1]
Accelerating	ADS does not signal for acceleration when the light is green and	ADS signals for acceleration when approaching obstacles/stop	ADS signals for acceleration later than other vehicles when the light is green or when the	ADS does not continue to accelerate until meeting the flow of traffic.

	the flow of traffic is increasing [H-1,H-2]	sign/yellow or red light [H-1,H-2]	flow of traffic is increasing. ADS signals for acceleration before the vehicle in front begins moving or accelerating [H-1,H-2]	ADS continues to accelerate past the speed of the flow of traffic [H1,H-2]
Decelerating	ADS does not signal for deceleration when approaching obstacles/stop sign/yellow or red light [H-1,H-2]	ADS signals for deceleration when the light is green and the flow of traffic is increasing [H-1,H-2]	ADS signals for deceleration later than the vehicle in front begins slowing [H-1,H-2]	ADS does not continue to decelerate until meeting the flow of traffic. ADS continues to decelerate to slower than the flow of traffic [H1,H-2]
Changing Direction	ADS does not change vehicle direction when there is an obstacle or when the road curves [H-1,H-2]	ADS changes the direction of the vehicle when there is no change in the road or environment [H-1,H-2]	ADS changes the direction of the vehicle before the road changes direction. ADS changes direction of the vehicle after reaching the obstacle or road direction change [H-1,H-2]	ADS does not change direction enough to follow the direction of the road (or to miss an obstacle). ADS continues to change direction after the vehicle has reached the correct trajectory[H-1,H-2]

Requirements

UCA	**Procedure**
UCA-1: Passenger does not enter vehicle when the vehicle is expecting a boarding [H-2]	**P-1:** Vehicle must indicate to passenger that they will wait for a short, predetermined period for boarding unless otherwise specified by the user [UCA-1]
UCA-2: Passenger enters vehicle when vehicle is not expecting [H-2]	**P-2:** Vehicle must stop when passenger gets too close (or tries boarding) without indicating [UCA-2]
UCA-3: Passenger enters vehicle before the car is in park or after the car has begun driving [H-2]	**P-3:** Vehicle doors must remain securely closed unless the vehicle is in park [UCA-3]
UCA-4: Passenger does not definitively get into the vehicle (leaves door open, halfway out, etc) [H-2]	**P-4:** Vehicle must remain in park when the doors are open [UCA-4]
UCA-5: Passenger does not exit vehicle when the vehicle is expecting an exit [H-2]	**P-5:** Vehicle must indicate to passenger that they will wait for a short, predetermined period for exiting unless otherwise specified by the user [UCA-5]
UCA-6: Passenger exits vehicle when vehicle is not expecting [H-2]	**P-6:** Vehicle must keep doors locked while the car is not in park [UCA-6]
UCA-7: Passenger exits the vehicle before the car is in park or after the car has begun driving [H-2]	**P-7:** Vehicle doors must remain securely closed unless the vehicle is in park [UCA-7] (same as P-3)
UCA-8: Passenger does not definitively get out of the vehicle (leaves door open, halfway out, etc) [H-2]	**P-8:** Vehicle must remain in park when the doors are open [UCA-8] (same as P-4)
UCA-9: ADS does not indicate when stopping/slowing or changing lanes/turning [H-1]	**P-9:** ADS must have vehicle indicate when slowing (lights) and before/during changing lanes/turning (blinker) [UCA-9]
UCA-10: ADS indicates slowing or changing direction when the vehicle does not intend to [H-1]	**P-10:** ADS must not make indications when the vehicle does not plan to change course [UCA-10]
UCA-11: ADS indicates too late for other traffic participants to know the vehicle's intent. [H-1]	**P-11:**ADS must indicate slowing immediately and change of course 5 seconds before making the change[UCA-11]

UCA-12: ADS indicates before behavior intent is decided [H-1]	**P-12:**ADS must not indicate before behavior intent has been decided[UCA-12]
UCA-13: ADS stops indicating before vehicle change has completed [H-1]	**P-13:**ADS must not stop indicating before the vehicle change has been completed[UCA-13]
UCA-14: ADS continues to indicate after intent has completed [H-1]	**P-14:**ADS must not indicate after the behavior has been completed[UCA-14]
UCA-15: ADS does not signal for acceleration when the light is green and the flow of traffic is increasing [H-1,H-2]	**P-15:**ADS must signal the vehicle to accelerate when the light is green and the flow of traffic is increasing[UCA-15]
UCA-16: ADS signals for acceleration when approaching obstacles/stop sign/yellow or red light [H-1,H-2]	**P-16:**ADS must not signal the vehicle to accelerate when approaching obstacles or yellow/red traffic lights[UCA-16]
UCA-17: ADS signals for acceleration later than other vehicles when the light is green or when the flow of traffic is increasing[H-1,H-2]	**P-17:**ADS must accelerate with the flow of traffic or if no traffic present then when the light is green, up to the speed limit[UCA-17]
UCA-18: ADS signals for acceleration before the vehicle in front begins moving or accelerating [H-1,H-2]	**P-18:**ADS must not signal for acceleration before the vehicle in front begins accelerating[UCA-18]
UCA-19: ADS does not continue to accelerate until meeting the flow of traffic.[H1,H-2]	**P-19:**ADS must continue accelerating the vehicle until it meets the flow of traffic or the speed limit[UCA-19]
UCA-20: ADS continues to accelerate past the speed of the flow of traffic [H1,H-2]	**P-20:**ADS must not accelerate the vehicle past the speed limit or the flow of traffic[UCA-20]
UCA-21: ADS does not signal for deceleration when approaching obstacles/stop sign/yellow or red light [H-1,H-2]	**P-21:**ADS must decelerate the vehicle when approaching obstacles/stop signs/yellow or red traffic lights[UCA-21]
UCA-22: ADS signals for deceleration when the light is green and the flow of traffic is increasing [H-1,H-2]	**P-22:**ADS must not decelerate when the light is green and the flow of traffic is unchanged or increasing[UCA-22]
UCA-23: ADS signals for deceleration later than the vehicle in front begins slowing [H-1,H-2]	**P-23:**ADS must decelerate the vehicle by the time it reaches the "safe distance" limit with the vehicle in front[UCA-23]
UCA-24: ADS does not continue to	**P-24:**ADS must continue to decelerate until

decelerate until meeting the flow of traffic [H1,H-2]	the speed of the flow of traffic is met (or until stopped at a stop sign/traffic light)[UCA-24]
UCA-25: ADS continues to decelerate to slower than the flow of traffic [H1,H-2]	**P-25:**ADS must not decelerate to a speed slower than the flow of traffic[UCA-25]
UCA-26: ADS does not change vehicle direction when there is an obstacle or when the road curves [H-1,H-2]	**P-26:**ADS must avoid obstacles when possible ADS must follow the road trajectory[UCA-26]
UCA-27: ADS changes the direction of the vehicle when there is no change in the road or environment [H-1,H-2]	**P-27:**ADS must not change trajectory without a stimulus[UCA-27]
UCA-28: ADS changes the direction of the vehicle before the road changes direction [H-1,H-2]	**P-28:**ADS must not change direction of the vehicle before the road changes direction[UCA-28]
UCA-29: ADS changes direction of the vehicle after reaching the obstacle or road direction change [H-1,H-2]	**P-29:**ADS must change direction of the vehicle at the correct time[UCA-29]
UCA-30: ADS does not change direction enough to follow the direction of the road (or to miss an obstacle) [H-1,H-2]	**P-30:**ADS must change direction the correct amount to stay on the trajectory of the road, or to avoid an obstacle if possible[UCA-30]
UCA-31: ADS continues to change direction after the vehicle has reached the correct trajectory [H-1,H-2]	**P-31:**ADS must stop changing direction once the correct path has been achieved[UCA-31]

Part 5

Passenger

UCA-1: Passenger does not enter vehicle when the vehicle is expecting a boarding (within x seconds) [H-2]

Scenario-1:

The passenger has many bags with them (from shopping) and they may spend too much time loading their stuff into the vehicle. They believe that the vehicle will not leave without them in the vehicle if the door is still open. However, if the vehicle only knows to wait a certain period of time for boarding the car may leave without the passenger being in the vehicle.

Scenario-2:

There is a group of passengers planning on boarding the robotaxi. The robotaxi has a set time to wait for passengers before it leaves, but the passengers incorrectly assume the vehicle will wait for all passengers to be loaded. It may leave with just some of the passengers loaded into the vehicle.

Solutions

- The vehicle should have sensors to detect if the doors are still open and if the doors are still open the vehicle should not move
- In the case that all doors are closed while passengers are still boarding (someone gets in on one side, but the other side has not been opened yet) the vehicle should have a method for allowing passenger feedback for when they are ready for the vehicle to move--this could be a button on the center console or a feature built into a companion phone application
- The vehicle can utilize lidar to note if there are objects moving around/closely to the vehicle to understand whether people are still boarding and if it is safe to move

Autonomous Driving Software:

UCA-22: ADS signals for deceleration when the light is green and the flow of traffic is increasing

Scenario 1:

The ADS system detects a small object in the road as unknown. The object is some kind of paper flier that has landed in the path of the vehicle. The ADS system incorrectly categorizes the object as one that must be avoided and so the vehicle slows to a stop even though the upcoming light is green. The abrupt stop with the light still being green causes the vehicle behind the robotaxi to rear-end the robotaxi.

Scenario 2:

The ADS system detects pedestrians in the intersection as bad actors have hacked and sent false data to the ADS system that has tricked the perception software to believe there are pedestrians when there actually are not. This causes the vehicle to stop in the middle of the intersection, blocking traffic in all directions and restricting access to the shopping center.

Solutions

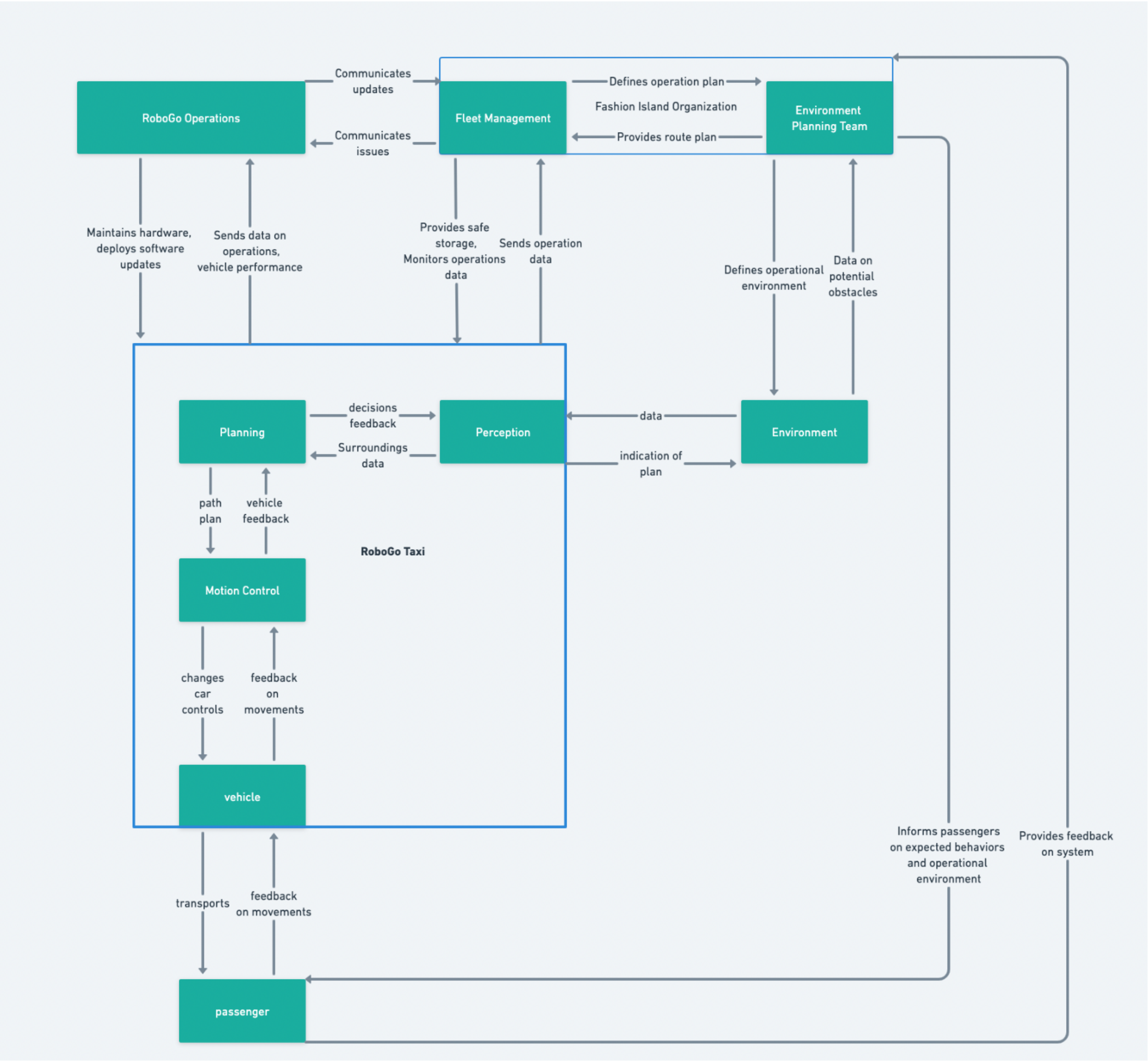
- The vehicle should have redundancy in the sensors to verify the data the ADS system is reading is legitimate (for example, relying on data from multiple cameras instead of just one)
- The ADS software should be closed to outside networks and should not allow for communication with bluetooth, internet, etc, in order to improve the security of the software
- Train the ADS perception to identify flat object/paper goods as not needing to stop or slow down for
- Train the ADS perception to recognize objects that commonly end up in the middle of a road
- Train the ADS perception to recognize most objects that could end up in the middle of the road

Part 6
What information should be passed to operations that you have created in your analysis? Create a plan for operators to use that information.
Most of the uncertain behaviors that can cause accidents in this system come from the environment. Therefore, it is important to consider unexpected human and environmental behaviors in the operation of the system. While the software can be well defined, having the operations team understand what that definition is is critical for determining what will be a safe operational environment for this system.

The safety and engineering teams should coordinate to create a shared understanding of the limitations of the system and those limitations must be communicated to the operations group. Additionally, operations should be given the STPA analysis to better understand the possible unsafe control actions and example scenarios that could unfold from the unsafe control actions. Because the operations team interfaces with the system and its users, they should be aware of the situations that could create an accident, and how the system has been engineered to try and prevent unsafe control actions.

Theoretically, this system should not have a human operator, but it is possible that human passengers and the environment could trigger the unsafe control actions. However, the plan should not just be geared towards educating passengers on the expected behavior of the system because humans will always have the potential to make errors. The plan will be to guarantee the operating environment fits within the constraints in the STPA analysis so that there should not be potential unexpected unsafe control actions from the ADS system.

Part 7
What recommendations do you have for the overall safety control structure for the organization that will use this system?



The organization that uses this system should have a control structure that is similar to the one modeled above. The key components of this control structure are the controls between RoboGo, the Fashion Island Fleet Management team, the RoboGo fleet at Fashion Island,

and the Fashion Island Environment Planning team. These are the important system components to pay attention to because there might be a higher possibility of having process model inconsistencies between the different organizations. The goal of the control structure is to create a shared understanding of how the RoboGo vehicles function between RoboGo operations and the Fashion Island operations teams.

The control structure includes the following:

- RoboGo operations communicates updates with Fashion Island Fleet Management
- Fashion Island Fleet Management communicates fleet issues to RoboGo
- RoboGo manages hardware fixes and software updates to the fleet
- The fleet will send back vehicle and fleet data to RoboGo
- The Fashion Island Environment Planning team provides a route plan to the greater organization, including the Fleet Management team
- The Fashion Island Fleet Management team then defines the operation plan of the fleet
- The Fashion Island Environment Planning team defines and manages the operational environment (and constraints)
- The Fashion Island Environment Planning team receives data from the environment on the operational environment
- The greater Fashion Island Organization informs passengers of the operational environment and vehicle limitations
- Passengers provide feedback on the system to the Fashion Island Organization

Part 8

Is there an existing hazard analysis for this system? If so, compare the results with what you got using STPA.

There is an STPA analysis for a similar system; however, it is not exactly the same because the system still requires a human driver as a component whereas this system does not. This makes comparing both analyses interesting because we can better understand where the software is more likely to cause problems versus the human operator. While the system I analyzed still has a human passenger, they really should not be considered an operator. Their levels of control are significantly less than those in the compared system.

When looking at both, what I found to be the biggest difference is the control structure levels. In this analysis the passenger is at the bottom of the control structure; however, in the other analysis the human operator is a driver and they are in the middle of the control structure. They have significantly more control over the system and have more potential for unsafe control actions. This is interesting because it implies that systems with less human operator control should be safer. These autonomous vehicles are not known for this, yet, and I think most people would say the opposite is true.

Theoretically, if the autonomous driving software was proficient, then fully autonomous vehicles should be safer as their behavior would be well defined. The problem is that the process model for the autonomous software is incomplete and can also be incorrect. The software cannot handle new situations as well as a human operator, and so if there is still the potential for unknown situations the process model for the autonomous driving software will likely never be fully complete. The question will be, when is it better than a human's?