Assignment 1:CAST Analysis Report

Maddie Golison

10/21/2022

Accident:

Collision between vehicle controlled by developmental automated driving system and pedestrian

This accident was the 2018 collision between Uber's Advance Technology Group's vehicle and a pedestrian in Tempe, Arizona. The vehicle (a modified 2017 Volvo SC90 sport utility vehicle) contained an automated driving system, which was active at the time of the crash.

Pick an accident report that you will use in your CAST analysis and answer the questions provided below:

1. **What was the cause identified in the report?**

The cause identified in the report was the distraction of the driver by looking at her phone. They also include the idea that there were more factors including

- inadequate safety risk assessment procedures
- ineffective oversight of vehicle operators
- lack of adequate mechanisms for addressing operators' automation complacency

The report mentions the lack of a good safety culture at Uber being the cause of the above three bullets. They also note two additional issues as (1) the impaired pedestrian's crossing of N. Mill Avenue outside a crosswalk, and (2) the Arizona Department of Transportation's insufficient oversight of automated vehicle testing.

2. **Is there a chain of events described? What was it? Do you see anything missing?**

The chain of events are as follows:

1. The SUV was completing the second loop on its test route

2. The vehicle had been operating about 19 minutes in autonomous mode

3. The vehicle was approaching the collision site at 45 miles an hr in the right lane

4. The pedestrian began walking across the street (with no crosswalk) while pushing her bicycle on her side

5. The ADS detected the pedestrian 5.6 seconds before the collision

6. The ADS continued to track the pedestrian, but the system did not classify her as a pedestrian and was not predicting her path

7. Once the ADS determined that a collision was imminent, the situation exceeded the response specifications of the ADS braking system

8. System disabled ADS emergency braking because the system because the system did not know how to handle the situation

9. ADS was off and was relying on intervention from the driver

10. Operator was looking at her phone, but looked up 1 second before crash

11. ADS data showed that the operator began steering left 0.02 seconds before hitting the pedestrian, at a speed of 39 mph.

12. The pedestrian was killed in the crash and the vehicle operator was uninjured

It would have been helpful to know the status of the ADS system once the crash occurred. Was it on? Was it turned back on after the collision? Why was it disabled?

3. **Do you see any hindsight bias? If so, who or what was blamed and what type of bias was involved?**

One strong case of hindsight bias was noting that the Uber ATG team lacked a strong safety culture. It is easy to say that after an accident has happened, but how would they know if the culture was sufficient before? If this accident had not happened, they would assume that their safety culture was sufficient.

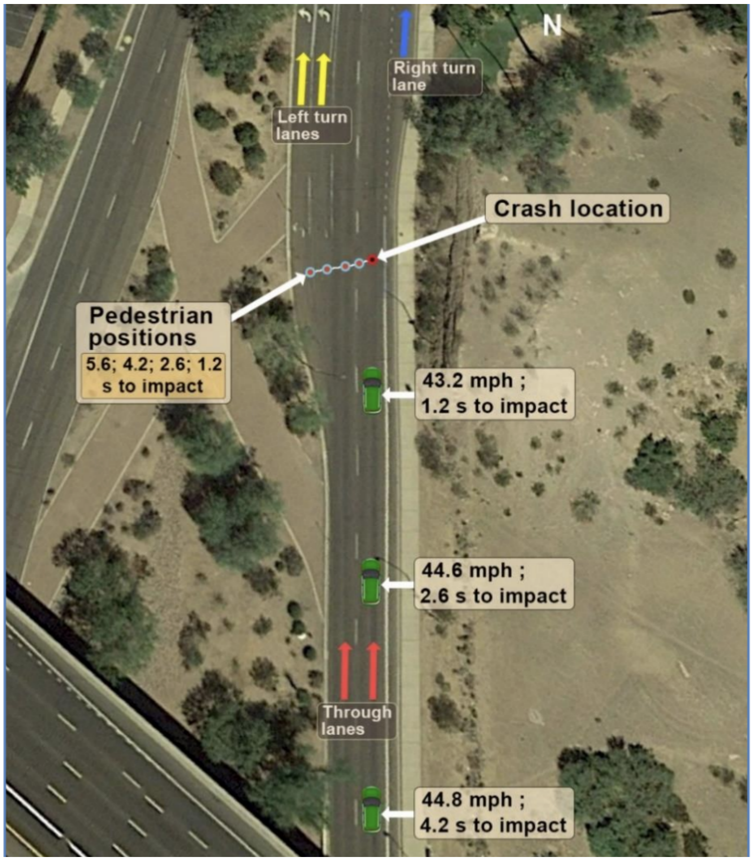
They also mentioned that if the vehicle operator was not distracted she should have had enough time to stop the crash. This is not something that can be known for sure, as Volvo tested their ADAS system in a simulation of the same situation and passed the majority of cases, but not all.

Third, they note that federal and state governments did not have good enough safety standards for these ADS vehicles. There really was no way for the non-technical governments, who have no experience in this area, to know what the safety standards should be.

4. **What role did the report say the human operators played? Were there extenuating circumstances that might explain the human operators' behavior?**

The human operator was meant to watch the vehicle actions as it navigated its test route. The operator was partly blamed for the accident as she was not looking at the road before the accident occured, and instead was looking at her phone. However, I am thinking that the operator has spent many hours doing this job and has never had to pay attention. The problem with having a human overseeing the operation of the autonomous vehicle is that they become accustomed to not needing to pay attention. They needed a better way to engage the operator in the driving of the car.

CAST Analysis


N
Left turn lanes
Right turn lane
Crash location
Pedestrian positions
5.6; 4.2; 2.6; 1.2 s to impact
43.2 mph ; 1.2 s to impact
44.6 mph ; 2.6 s to impact
Through lanes
44.8 mph ; 4.2 s to impact

(The above is an image from the accident report -- cited on the last page)

Part 1

System Involved

The system in this accident includes the retrofitted 2017 Volvo XC90, the vehicle operator, custom ADS software, lidar, radar system, camera system, positioning system, dashboard inward and outward facing cameras, the tablet interface with the ADS, the highway, and the pedestrian. We will limit the boundary to these system elements; however, there will be elements that interface with the system that may be relevant (i.e. Uber ATG organization, the operator's manager, etc).

System Loss

This accident was the 2018 collision between Uber's Advance Technology Group's vehicle (the retrofitted 2017 Volvo XC90) and a pedestrian in Tempe, Arizona. The pedestrian was jaywalking with her bicycle when the vehicle failed to recognize her as a pedestrian until it was too late, and the car fatally hit her. The vehicle operator was not injured.

System Hazard

System Hazard 1: Vehicle does not maintain safe distance from nearby objects.
Safety Constraints:
1. Vehicle must keep a safe distance from all nearby objects
2. Vehicle maneuvers roads safely
3. Vehicle alerts driver when automated driving system is disabled

Proximal Events

Event	**Questions Raised**
Vehicle was completing a second loop of the predefined route; it had been in autonomous mode for 19 minutes	Was the first loop driven autonomously? Was 19 minutes long enough to have been in this spot before?
The vehicle was approaching the collision site at 45 miles an hour in the right lane	Was this the appropriate speed for the time of day, conditions and location?

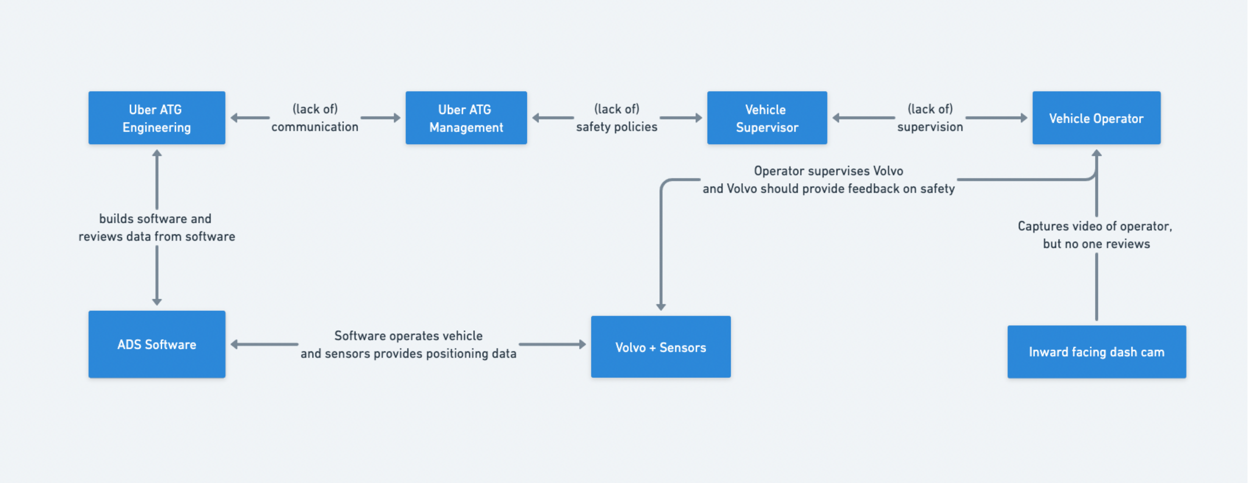
The pedestrian began walking across the street (with no crosswalk) while pushing her bicycle on her side	Was the bicycle on her right or left side? Were the cameras on the vehicle able to make out the bicycle?
The ADS detected the pedestrian 5.6 seconds before the collision	If the ADS detected the object with 5.6 seconds to spare, why was the operator not notified sooner?
The ADS continued to track the pedestrian, but the system did not classify her as a pedestrian and was not predicting her path	Why was the path not predicted if the object was being tracked?
Once the ADS determined that a collision was imminent, the situation exceeded the response specifications of the ADS braking system.	Why didn't the ADS braking system have a specification for imminent collisions?
The software disabled ADS because the system did not know how to handle the situation	Why would the ADS be disabled late enough that it would be too late for the operator to safely take over?
Operator was looking at her phone in the center console, but looked up 1 second before crash	Why was the operator not alerted sooner to the potential collision? Why was the interior facing camera not alerting the operator or her manager that she was distracted? Why was the operator so distracted?
ADS data showed that the operator began steering left 0.02 seconds before hitting the pedestrian, at a speed of 39 mph.	Why hadn't the ADS slowed the vehicle down at all when it initially detected the object? Why was there no emergency braking?
The pedestrian was killed in the crash and the vehicle operator was uninjured	Did the operator end up stopping the vehicle? Did the ADS?

Physical Losses

- Loss of human life (the pedestrian)
- Loss of pedestrian's bicycle
- Physical damage to the vehicle

The physical losses show the cost of the failures (life).
However, they are not as useful in understanding how the accident occured.

Part 2
Safety Control Structure


Uber ATG Engineering
(lack of) communication
Uber ATG Management
(lack of) safety policies
Vehicle Supervisor
(lack of) supervision
Vehicle Operator
builds software and reviews data from software
Operator supervises Volvo and Volvo should provide feedback on safety
Captures video of operator, but no one reviews
ADS Software
Software operates vehicle and sensors provides positioning data
Volvo + Sensors
Inward facing dash cam

Part 3
Loss of Each Component

Component: Vehicle Operator

Safety Responsibilities:

- Monitoring and recording ADS actions
- Monitoring planned route
- Reporting incorrect actions of the ADS
- Emergency takeover of vehicle in case of ADS failure

Role in Adverse Event:

- Was not monitoring the planned route
- Did not take over vehicle control fast enough when ADS stopped

Process/Mental Model Flaws	**Questions**
The operator was not aware of the importance of keeping attention on the road. They believed that the car would always alert them when an unknown state occurs.	How could she have known that the vehicle would not alert her with enough time? Why did she not know the importance of keeping her focus on the road?

Contextual Factors	**Questions**
Went from two vehicle operators to one. There was no additional training to go from passenger to operator. Interior facing cameras did not capture the whole line of sight. The vehicle operator's manager never reviewed car footage to ensure the operator's focus on the road.	Why did they remove the second vehicle passenger? Why was there no training to go from passenger to operator? Why did the manager or Uber organization never review the footage from inside the vehicle? Why was there fatigue in focus? Were the shifts too long?

Component: Vehicle Operator Supervisor

Safety Responsibilities:

- Managing the vehicle operator
- Communicating to upper management about the vehicle operator actions
- Implementing actions prescribed by upper management

Role in Adverse Event:

- Failed to monitor safe actions by vehicle operator in the car
- Failed to retrain new operators when they came from the passenger side

- Failed to identify or make known concerns with removal of 2nd passenger in the test vehicles

Process/Mental Model Flaws	**Questions**
The supervisor believed that the interior facing dash camera footage did not need to be reviewed. The supervisor did not see a problem with moving a vehicle operator from the passenger to the driver seat without additional training.	Why did the supervisor not check the car footage? Was there any concern from the supervisor about changing roles of the vehicle operator without additional training?

Contextual Factors	**Questions**
The business decided to go from two people in the car to one, and they did this without improving training for those who went from the passenger seat to the driver's seat. Organization did not require reviewing the dash cams from the vehicles.	Was there a high ratio of operators to supervisors? Was there too much footage for the supervisors to review? Did the culture not allow supervisors to voice concerns to upper management? Had they already voiced concerns to upper management?

Component: Uber ATG Engineering Group

Safety Responsibilities:

- Building a safe automated driving system with software and sensors
- Build in redundancy for potential errors in the ADS
- Communicate the status of the system to the business and ensure the information gets to the operations side of the business

Role in Adverse Event:

- Disabled the Volvo's emergency braking system as they believed it was redundant, but would have likely stopped the accident from happening.
- Not explicit about the limitations of the system

Process/Mental Model Flaws	Questions
The engineering team believed their software was as robust (or moreso) than that of the emergency braking system that the Volvo comes with. They also believed that the emergency braking system would not work well with the ADS	Why did the supervisor not check the car footage? Was there any concern from the supervisor about changing roles of the vehicle operator without additional training?

Contextual Factors	Questions
The business decided to go from two people in the car to one, and they did this without improving training for those who went from the passenger seat to the driver's seat. Organization did not require reviewing the dash cams from the vehicles.	Was there a high ratio of operators to supervisors? Was there too much footage for the supervisors to review? Did the culture not allow supervisors to voice concerns to upper management? Had they already voiced concerns to upper management?

Component: Volvo, Sensors, and its Emergency Braking System

Safety Responsibilities:

- Physically protect the operator
- Straightforward in operation to not confuse the operator
- Physical systems act reliably
- Emergency brake when the operator does not

Role in Adverse Event:

- The emergency braking system was able to be disabled

Process/Mental Model Flaws	Questions
The belief that the Volvo emergency braking system was not compatible with the ADS system.	How could the engineering teams do a better job of trying to keep the emergency braking system and make sure that it did not conflict with the ADS?

Contextual Factors	**Questions**
Volvo allowed the car to be "hackable".	Did Volvo know how the vehicle was being used? Could Volvo have helped Uber ATG implement both the Volvo emergency braking system and their ADS?

Component: ADS Software

Safety Responsibilities:

- Find correct position of car and its surroundings
- Utilize this information to safety move the vehicle autonomously
- Refrain from colliding into any tracked objects

Role in Adverse Event:

- Did not correctly identify and label objects
- Did not alert operator that there was an object detected
- Did not keep track of object history in order to predict movement
- Had no emergency braking behavior (if it had correctly identified the object it would have gradually slowed the vehicle to a stop, not immediately stop, even if the collision was impending)
- ADS shut off when it knew it could not prevent a collision

Process/Mental Model Flaws	**Questions**
ADS shutting off when it knew an accident was unavoidable was a flaw in that the behavior thought a human operator would be better suited to take over at that point, even though they would not be able to avoid a collision either. ADS was designed to not alert operators of obstacles early because it would have been too frequent. Believed they did not need to predict object path for a static object; however, when the static object begins to move this is a problem.	Why was there no emergency braking system developed in the ADS? Why did the system not alert the operator about the object as they approached it, especially since the system could not identify it?

Contextual Factors	**Questions**
Various obstacles can be frequent and it would be easy to overwhelm the operator with information.	Could the system notify the operator of moving objects? If a collision is imminent, can the system notify the operator at that point?

Component: Inward Facing Dashboard Camera

Safety Responsibilities:

- Keep track of the status of the interior of the vehicle by recording video
- Send the data to the vehicle operator's supervisor

Role in Adverse Event:

- Video footage was never reviewed
- The view was not sufficient to see the center console, where the driver kept looking (where her phone was stored).

Process/Mental Model Flaws	**Questions**
Taking the footage is enough to prevent incorrect behavior of the vehicle operator. The supervisor would review the footage to ensure the operator was performing their duties.	How could the inward facing camera system alert the supervisor and the operator when it detects lost focus? What other processes could be put in place to incentivize supervisor reviews and operator attention?

Contextual Factors	**Questions**
The operator had been a passenger before they went to just one person in each vehicle. She had not been given additional training for the operator role. There were no consequences for being distracted, even though the cameras were recording.	Why wasn't the presence of video recording enough to keep the operator's attention?

Component: Uber ATG Management

Safety Responsibilities:

- Keep an open line of communication between engineering and operations
- Implement procedures that increase the safety of the systems
- Be aware of knowledge gaps when things change (and fill those)
- Ensure reportees are fulfilling their safety responsibilities

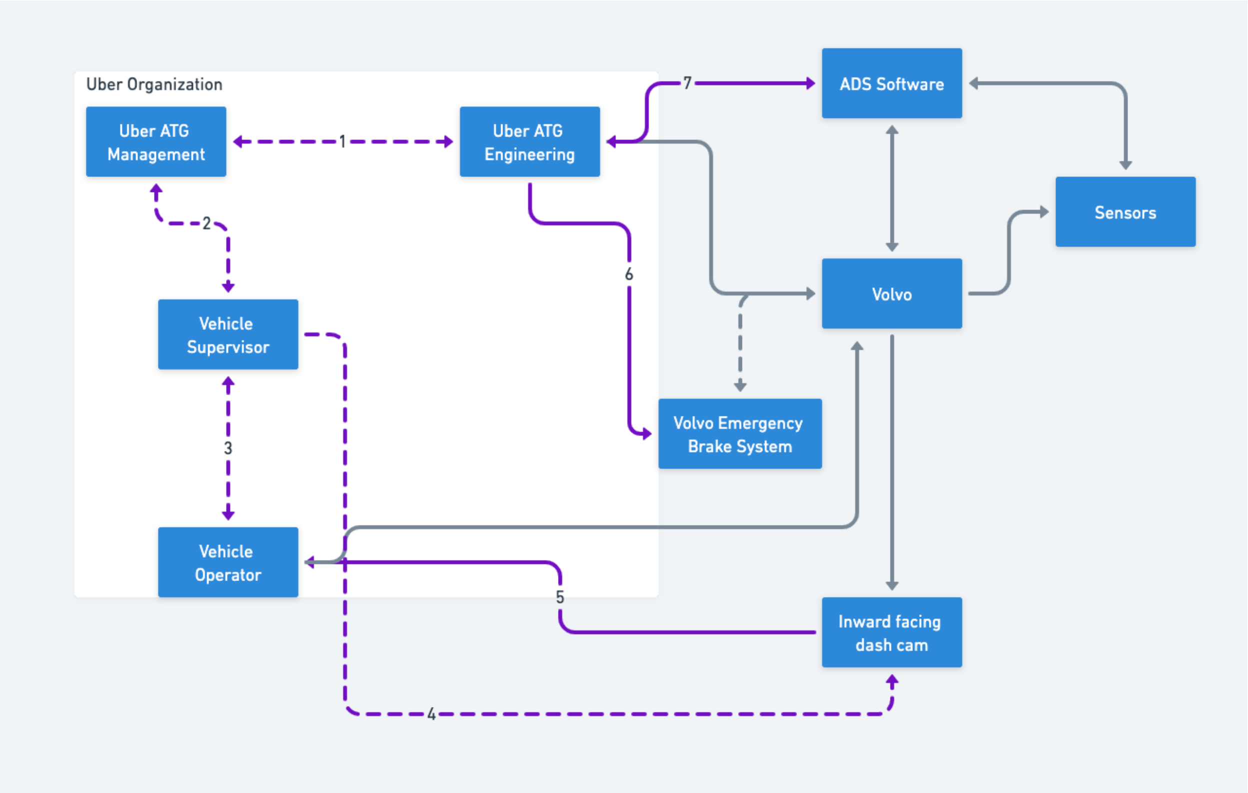
Role in Adverse Event:

- Did not prioritize safety
- Did not keep accountability for safety in the management chain, down to the vehicle operators
- Failed to communicate the actual limitations of the ADS

Process/Mental Model Flaws	**Questions**
The business management did not believe they needed to actively manage the safety of the systems. The business did not realize there were different understandings of the limitations of autonomy in the engineering side and in the operations side.	How could engineering have influenced management to take safety more seriously? Why did management not verify that the vehicle supervisors were making sure their vehicle operators were working safely? Did management understand the technical limitations of the ADS?

Contextual Factors	**Questions**
There were no members of the organization explicitly dedicated to ensuring the safety of the product.	Why was safety not a concern before the accident? Why was no one held accountable for verifying the activities of the vehicle operators?

Part 4
Control Structure Flaws



In the above control structure there were a few main flaws that are outlined below:

1. Lack of communication between management and engineering
2. Lack of communication between management and vehicle supervisors
3. Lack of communication between vehicle supervisors and operators
4. Failure of vehicle supervisor to actually review dash cam footage
5. Failure of dash cam to actually capture the full interior of the car
6. Engineering removal of the "redundant" Volvo emergency braking system
7. Incorrect behavior developed in the ADS software

We will elaborate on these in the following sections:

Communication and Coordination

There were three major control structure flaws related to communication and coordination. All of them stem from a similar issue.

- The first is the most concerning, and it is the lack of communication between management and engineering about the capabilities of the autonomous driving system. Without this knowledge transfer, there would be no way for a vehicle supervisor or a vehicle operator to know how imperative it is to maintain attention at all times in the vehicle. "Autonomous" in the context of vehicles can mean a lot of different things and those without the technical background to understand limitations of the system need to be briefed on what is possible in terms of failures.

- The second and third issues came from the lack of communication and coordination between management and the supervisors and the supervisors and the vehicle operators. This is apparent in that there was no communication around potential failures with the autonomous systems. Because management did not have the correct mental model, there was no way for their management chain to have the correct mental model around how the ADS software worked. This led the vehicle operator to not be concerned about keeping her attention on the road--she believed that the software was more advanced than it was.

Safety Information System

At the time, there was no safety group at Uber. What this meant was that there was no accountability for safety initiatives and no expertise about systems safety more generally. While there were attempts to place safeguards, no one was responsible for verifying the quality and robustness of these.

- For example, the inward facing dashboard camera was implemented, but it did not have a view of the entire front row of the car
- There was no sensible way to review all of the camera footage, so it was not really useful data
- Initial trainings were created for vehicle passengers and operators, but not when they move to only having one person in the vehicle
- There was no policy around length of the driving shift and no understanding of when an operator's fatigue would set in
- Engineering was able to just disable the Volvo emergency braking system, without having to answer to anyone on why it was done and why they could not keep the redundancy
- Finally, there was no policy in place for how emergency situations should be handled by the ADS. The way the ADS software was built it was not meant to handle emergency situations or imminent collisions, and there needed to be better guidance on the design of the software in these scenarios

Culture

The control issues related to culture stem from the lack of accountability in implementing safety mechanisms. The culture at Uber could be seen as the Culture of "Swagger," which is true for many similar companies.

- No one verified the inward facing dashboard camera footage of the vehicle operators. Because no one in the management chain actually verified this, it seems there was no pressure on upper management or vehicle supervisors to do this.
- Because the vehicle operator did not seem to be concerned about using her phone in the car, it appears that she understood there would not be someone checking the footage to make sure she was not doing this. It was not difficult for her to have her phone outside the line of sight of the dash cam and the dash cam did not automatically alert anyone of the lack of operator attention, so she was not concerned with not paying attention to the road.

Changes & Dynamics

There was one significant change made to the operation of Uber's test vehicles, which lacked solid change management policies. The test vehicles initially had two operators, one in the driver's seat and one in the passenger seat. The person in the driver's seat had one main role of keeping their eyes on the road and being ready to take over control of the car at any moment. The passenger then was responsible for keeping track of incorrect actions of the car on the in-car tablet. When management moved away from this, there was just one operator in the car and they became responsible for both activities. The lack of the second passenger may have removed a crucial layer of redundancy for the operation of the vehicle.

Economics and Environmental

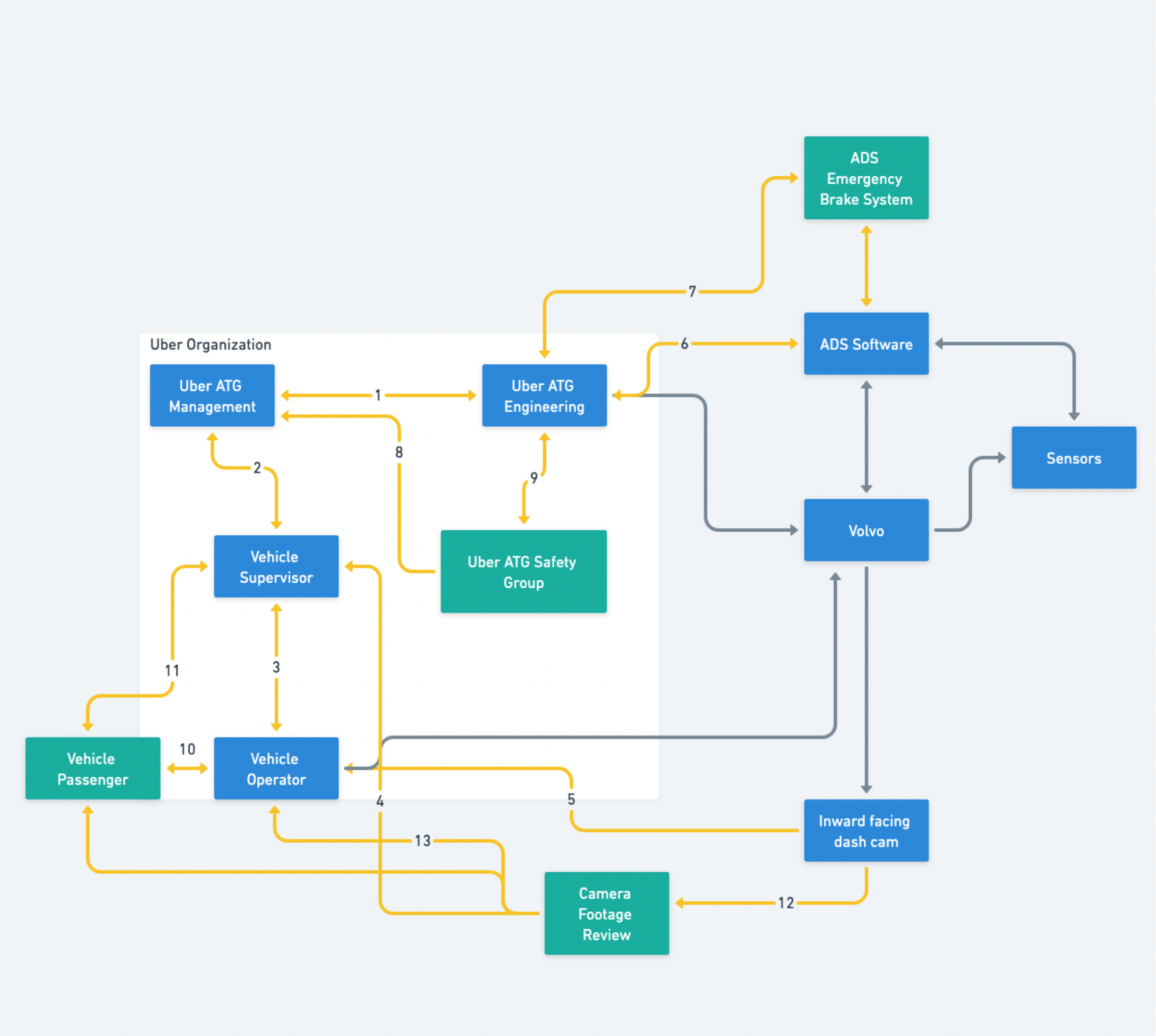
A control flaw between upper management and their management chain was the removal of the second vehicle operator, which was done for cost reasons. There was no additional training provided for those who went from passenger to operator and while management would not "feel" this change, it did present a risk for the lone vehicle operator as they had to maintain attention on the road without a back-up operator.

Questions

- How unaware was management of the limitations of the ADS software?
- Were all vehicle operators as inattentive as the one involved in the accident? (For example, removing eye sight from the road for 25+ seconds at a time)
- Were there any resources in the engineering team dedicated to safety?

Part 5
Recommendations for Improvement

Proposed Control Structure:
(Green boxes are new elements and yellow lines are changes made)



The following suggested changes map to the numbers in the diagram above:

1. There should be increased communication between engineering and management on the current capabilities and limitations of the ADS software
2. Management should verify supervisors are reviewing curated dash cam footage
3. There should be supervisor action taken with the vehicle operator if the footage shows improper attention to the road. There should also be communication from the supervisor to the operators about the current capabilities and limitations of

the ADS software. Operators should be submitting feedback to supervisors about inadequate ADS behaviors. Supervisors should limit shift lengths of vehicle operators.

4. Supervisors must be automatically notified if dash cam footage shows operators not paying attention to the road
5. Camera vision must be that of the entire front row of the car (no blind spots)
6. Engineering must track static and dynamic objects to better predict object trajectory
7. Engineering must build an emergency braking system/software safety system as robust as the Volvo one they needed to disable.
8. There must be a creation of a group responsible solely for safety of the product
9. The safety group must communicate plans with management and develop requirements for engineering
10. Uber should reinstate a second passenger in the test vehicles
11. Vehicle supervisor should communicate roles to the passenger as well as the operator and how they should be working together
12. Camera footage review system should be developed to automatically and immediately notify operators and supervisors when attention is not on the road (auto curated video content instead of sending all video content along)
13. Vehicle operators should be alerted immediately if the camera review system detects they are not currently paying attention to the road

Conclusion

The main theme of the issues presented in this analysis is that there were not sufficient safety measures within and between elements of the control system (outlined above). The original safety report explains that the probable cause was the failure of the vehicle operator to monitor the ADS and her surroundings. While it is easy to point this out, the real question is why was the vehicle operator able to remove attention from the road for such an extended amount of time? And why was she not alerted about an imminent collision more than a second before it happened?

What this analysis should have illustrated is that there were failures at the majority of the system controls and the only way to understand how the accident occurred was to understand the system level failures. What the issues boil down to is that Uber had no group dedicated to safety and therefore no accountability for safety. The accident report *does* highlight this and I believe that the addition of a safety organization would fix many of the control issues we analyzed here.

References

National Transportation Safety Board. “Collision between Vehicle Controlled by Developmental Automated ... - NTSB.” *Ntsb.gov*, NTSB, 18 Mar. 2018, https://www.ntsb.gov/investigations/AccidentReports/Reports/HAR1903.pdf.