[G12] Safety

Analysis of the Uber car accident

- ### How did the accident happen

Figure 1. (Left) Location of the crash on northbound Mill Avenue, showing the paths of the pedestrian in orange and of the Uber test vehicle in green. (Right) Postcrash view of the Uber test vehicle, showing damage to the right front side. **[1]**

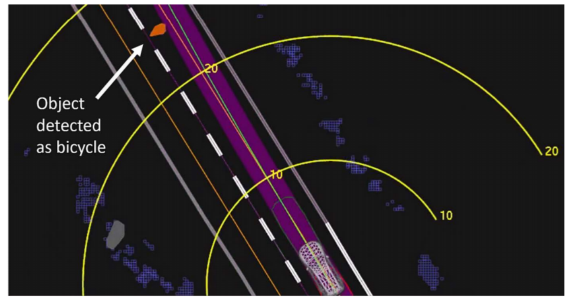

Figure 2. View of the self-driving system data playback at about 1.3 seconds before impact, when the system determined an emergency braking maneuver would be needed to mitigate a collision. Yellow bands are shown in meters ahead. Orange lines show the center of mapped travel lanes. The purple shaded area shows the path the vehicle traveled, with the green line showing the center of that path. **[1]**

The vehicle's radar and LIDAR sensors detected an object in the road about six seconds before impact. As their paths converged, the vehicle's self-driving software classified Herzberg first as an unknown object, then as a vehicle, and finally as a bicycle, with varying expectations of the future travel path. At 1.3 seconds before impact, the vehicle's computer decided that an emergency braking maneuver was needed. But Uber had disabled the Volvo's factory AEB system, "to reduce potential for erratic vehicle behaviour." Moreover, the system was not designed to alert the driver that braking was needed. **[2]**

Uber's software prevented its system from hitting the brakes if that action was expected to cause a deceleration of faster than 6.5 meters per second. That is to say, in an emergency, the computer could not brake.**[3]**

- ### The influence of the accident

Uber:

1. Uber immediately suspended its autonomous vehicle testing across North America and said it shuttered its test program in Arizona.
2. Uber has laid off around 100 self-driving car safety operators in Pittsburgh. Uber plans to create 55 new positions called "Mission Specialists"**[4]**
   ...

Others:

1. *Toyota halts its self-driving car testing*
2. *Nvidia suspends self-driving car tests*
3. *Arizona governor Doug Ducey, who had been extremely friendly toward Uber, revoked the ride-hailing company's permission to test vehicles in the state.*

   ...

The whole timeline can be found here: https://www.theverge.com/2018/3/28/17174636/uber-self-driving-crash-fatal-arizona-update

Who are **Mission Specialists**: The people maintain control of the vehicle during testing is addressed through self-driving system design, training, and operational policies. (more qualified than Safety Operators)

Why safety

Self-driving cars could bring us a lot of convenience and make our lives more efficient only if they are safe enough. Only safe products can be trusted by the public and then have the possibility to influence and change the society.

After this accident, for example, we can find that a lot of people starting to suspect and resist the self-driving car because they did not believe the self-driving cars are safe enough according to a survey of American Automobile Association **[5]**. From the influence of the accident mentioned above, the whole self-driving industry got a huge negative impact due to this accident. Therefore, we can see the importance of safety to self-driving.

Meanwhile, self-driving cars should have the potential to be safe, at least safer than human drivers. For instance, self-driving cars won't be capable of doing risky (and illegal) things like speeding or drinking and driving. Some sensors like LiDAR can even work in the dark circumstance. **[6]**

At present, self-driving technology is not safe enough but has the potential to be safer. Therefore, we, as ICT professionals, need to put more efforts in improving the safety of self-driving technology.

Safety Principles

To improve the safety of self-driving technology, it is crucial in constructing safety principles as a guideline of the whole industry. After the car accident, Uber released new practice approaches in the Uber ATG Safety Report (later only Safety Report). **[7]** I want to analyse the five safety principles in the report with respect to ICT professionalism.

- **Proficient**
  A self-driving system must have good strategy to drive automatically

In the Uber's case:

1. The victim crossed the X-shaped brick-paved walking path across the median before being hit.
2. The self-driving in the vehicle did not classified the victim as a human in time.
3. Vehicle decided it needed to brake 1.3 seconds before striking a pedestrian, but Uber had disabled the Volvo's automatic emergency braking system in order to prevent erratic driving.

Analysis with respect to ICT professionalism:

From the left description, we could find that the self-driving system was not proficient, which means the design of the software and hardware was not competent to the task of detection and reaction. Improvements are needed to achieve this principle.

1. *In Uber's Safety Report, Uber plans to pay more efforts in **Operational Design Domain** (ODD). (P29 **[7]**) ODD is like a map stored in the self-driving cars and gives the basic information about the environment. Uber characterises and constrains the ODD to create and use this technology:*

   - *Characterizing the ODD: Collect the data from the environment and add them to the ODD as tags. Evaluate the ODD with simulation.*
   - *Constraining the ODD: Restrict the routing of the self-driving vehicle in the approved ODD. Mission Specialists are trained to control and report when a scenario is not included in the current ODD.*

   In the Uber's case, developers of the system should collect the information about X-shaped brick-paved walking path beforehand to construct a complete ODD. In that case, the self-driving car could have slowed down before the walking path.

2. *We need to improve the ability of object detection in order to give more time to react. Uber choose to achieve this with the procedure below:*

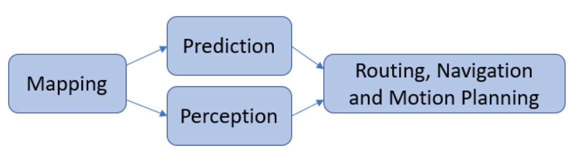

***Figure 3**. The procedure of object detection*

   Mapping uses the existing maps to navigate the cars; Perception recognises the object in the surroundings; Prediction predicts the motion of objects; The last part synthesises the Prediction and Perception in order to generate appropriate route.

3. *In the car accident, the conflict of self-driving car's computer and the Volvo's factory AEB system demonstrates the importance of a combination of self-driving technology with the control of base vehicles. Self-driving technology companies like Uber need to develop the vehicle control system with car manufacturers like Volvo in order to ensure the 'seamless' connection between the self-driving system and base vehicles.*

- **Fail-Safe**
  Fail-Safe means that the self-driving cars must take actions to transition of the vehicle to a minimal risk condition when a failure happens in the system.

In the Uber's case:

1. Vasquez (the Safety Operator) intervened “less than a second” before impact by grabbing the steering wheel. V asquez hits the brake less than a second after impact.
2. The system was not designed to alert the driver that braking is needed.
3. The police report suggested the car's driver was streaming an episode of talent show The Voice rather than monitoring the car's progress.

Analysis with respect to ICT professionalism:

In the Uber's car accident, the Safety Operator didn't take the responsibility of monitoring the self-driving cars. These unprofessional behaviours caused the accident to some extent. The intervene of human drivers is also a key factor of principle Fail-Safe. In order to achieve this principle, Mission Specialists (the Safety Operator in the case) should take control of self-driving cars when a system failure occurs. (looking [G12] Workforce and Skills to get more details)

*Now Uber operates the vehicles with two Mission Specialists instead one. Besides, Uber uses application review, phone screen, homework etc. to improve the procedure of hiring(P36 **[7]**). Meanwhile, Mission Specialists undergo extensive training to ensure the professional operation (P42 **[7]**) and are restricted by*

In my opinion, developers of the self-driving system need to consider more about the human-machine interface (like touch screens) between self-driving cars and Mission Specialists for the present phase in order to promote the communication between drivers and cars. On the one hand, the interface needs to provide sufficient information about self-driving cars, including the alert of danger; On the other hand, the interface will not distract the Mission Specialists.

Principle Fall-Safe also includes the fallbacks of software and hardware. These fallbacks act as redundancies of the equipment in the self-driving system in order to maintain the stability when a malfunction occurs. The table below shows the examples of potential fault mitigation in Uber:

Table 1. Examples of potential fault mitigation in Uber (P40 **[7]**)

Fault	Fault Type	Mitigation Plan
Primary Compute Power Failure	Electrical Power Systems	Backup power turns on, the system detects the fault, and the vehicle is safely brought to a stop.
Loss of Primary Compute or Motion Planner Timeout	Self-Driving Software	If the VIM stops receiving trajectories from the self-driving system, the Mission Specialist will be notified via LED status lights and an audio cue that the vehicle has returned to manual mode. In our next generation vehicle, the VIM will bring the self-driving vehicle to a safe stop along the most recently received valid route, while using IMUs and wheel speed sensors to maintain control of the vehicle.
Wheel Speed Sensor Data Delay	Vehicle Platform	Our systems monitor the data coming from the vehicle’s wheel speed sensors and will detect if the data becomes delayed or stops being sent. The system will then initiate a safe stop.
Door Opens While Driving at Speed	Misuse	Our systems will detect that the door has opened and will safely stop the vehicle.

- **Continuously Improving**
  Automakers need to provide updates and improvements continuously for the self-driving cars.

In the Uber's car crash, it is obvious that the move of self-driving cars had deviated from the normal pattern. It is definitely necessary to correct the system to achieve principle Continuously Improving. However, Uber did not comply with this principle before the accident because the problem (could not brake because of the conflict with base vehicle) revealed is very easy to simulate and test before doing an on-road test.

In order to achieve this principle, Uber now provides different kinds of testing and simulation method (P40 **[7]**) to ensure the events are solved. The figure below shows the simplified the procedure of the improvement:

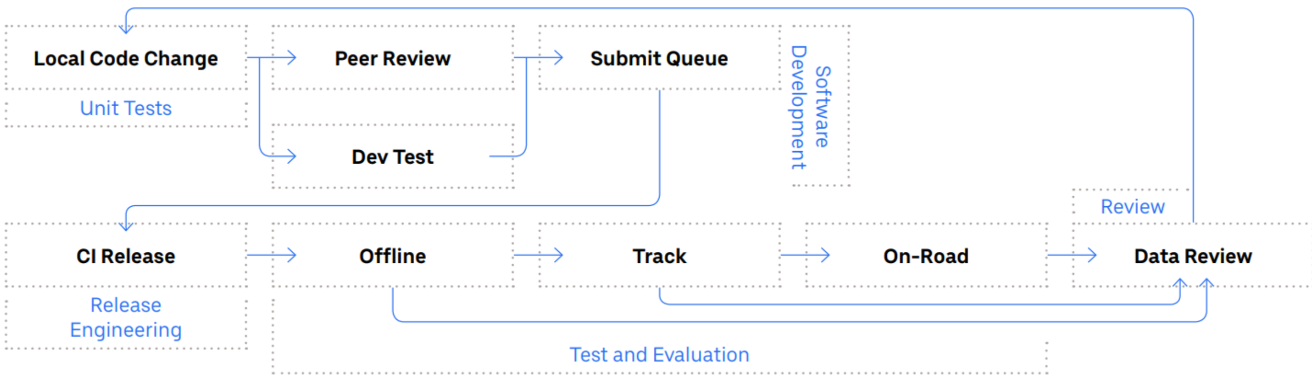

Figure 4. Uber's software development and validation process

However, I think developers also need to consider the self-driving cars' improvement after cars being sold. Maybe it is not a problem for Uber because the Uber owns all the self-driving cars and just offers the service. Uber can keep updating the software and hardware of their self-driving cars. But for other companies which sell the self-driving cars, how to maintain the improvement of their sold self-driving cars is a huge problem. Once some flaws are found in the old software or hardware, the old self-driving cars could be very dangerous not only for the owners of cars but also anyone close to the cars. Software update might be solved by connecting the self-driving cars to the Internet. As for hardware, maybe the government need to issue the laws to force the owners of cars to update the hardware at regular intervals. Nevertheless, updating the hardware is a huge expenditure for the automakers if this kind of improvement is free. On the other hand, self-driving cars are less attractive if owners of cars need to pay a lot to maintain the improvement of the cars.

- ## Resilient
  Self-driving system has the ability to prevent or mitigate the potential harm to avoid system failure.

In the Uber's case:

The vehicle’s self-driving software classified Herzberg first as an unknown object, then as a vehicle, and finally as a bicycle.

Analysis with respect to ICT professionalism:

The detection of the unknown object was an important signal before the malfunction of the self-driving system. If the system could report the abnormal detection to the Mission Specialist in real time, Mission Specialist could have intervened earlier to avoid the accident. Principle Resilient urges ICT professionals to design a robust system which could be tracked and monitored in this case. I think a great solution is the XAI. (from [G12] The Ethics of Autonomous Vehicle Accidents)

Principle Resilient also needs to be achieved in the aspects showed below:

1. **Cybersecurity:**
   Some of the data collected by the self-driving cars are the private information for the customers and other parts of the data are crucial for the control of the cars. These data could be very vulnerable to attacks from the Internet. For example, the data like locations might give away in the cyber attack and the self-driving system might be disturbed by the wrong information from the Internet.
2. **Sensors:**
   The whole self-driving system relies on the precise data collected by sensors. The sensors, however, are easy to get distribution and damages. For example, a leaf could block the light to the camera and small impact might affect the accuracy of proximity sensors. Therefore, it is very significant to give enough protection to those sensors but not to affect their ability to collect precise data. Besides, developers need to prevent sensors from being misled easily by fake signals **[8]** and even influenced by the sensors of other self-driving cars if they choose active sensors **[9]**.

- ## Trustworthy

Self-driving cars should deal with the ethical dilemmas.

Having high processing speed, self-driving cars change the reaction of human beings to the algorithm, which always has the same result in the same situation. It becomes sophisticated when the result could be explained —— the designers of self-driving cars need to decide what the self-driving car will do when an unavoidable accident happens. (looking [G12] The Ethics of Autonomous Vehicle Accidents to get more details) The video below explains the ethical dilemmas in self-driving cars:

Video 1. Ethical dilemmas

Conclusion

These five Safety Principles give the general guideline for the ICT professionals in the self-driving industry. However, I think these principles need to be improved as well as extended with the testing and development of self-driving cars to adapt to new circumstances. We all are very grieved at this fatal car accident, but this also gives us a chance to improve the safety principles and indicates the right way of development.

Further reading:

Uber's use of fewer safety sensors prompts questions after Arizona crash: https://www.reuters.com/article/us-uber-selfdriving-sensors-insight/ubers-use-of-fewer-safety-sensors-prompts-questions-after-arizona-crash-idUSKBN1H337Q

Self-driving car survey before the fatal Uber car accident: http://saferoads.org/wp-content/uploads/2018/01/AV-Poll-Report-January-2018-FINAL.pdf

Reference:

[1] NTSB (2018, May 24). Preliminary Report Highway: HWY18MH010. Retrieved from https://www.ntsb.gov/investigations/AccidentReports/Pages/HWY18MH010-prelim.aspx

[2] Hawkins, A. J. (2018, May 24). Uber self-driving car saw pedestrian but didn't brake before fatal crash, feds say. Retrieved from https://www.theverge.com/2018/5/24/17388696/uber-self-driving-crash-ntsb-report

[3] Madrigal, A. C. (2018, May 24). Uber's Self-Driving Car Didn't Malfunction, It Was Just Bad. Retrieved from https://www.theatlantic.com/technology/archive/2018/05/ubers-self-driving-car-didnt-malfunction-it-was-just-bad/561185/

[4] Hawkins, A. J. (2018, July 11). Uber laid off its self-driving car safety drivers in Pittsburgh. Retrieved from https://www.theverge.com/2018/7/11/17562522/uber-laid-off-self-driving-safety-driver-pittsburgh

[5] AAA: American Trust in Autonomous Vehicles Slips. (2018, May 18). Retrieved from https://newsroom.aaa.com/2018/05/aaa-american-trust-autonomous-vehicles-slips/

[6] Higgins, S. (2018, November 01). LiDAR Superpowers: Ford Prototype Car Sees in the Dark. Retrieved from https://www.spar3d.com/blogs/the-other-dimension/lidar-superpowers-ford-prototype-car-sees-dark/

[7] Uber (2018). Uber ATG Safety Report. Retrieved from https://uber.app.box.com/v/UberATGSafetyReport

[8] Harris, M. (2015, September 04). Researcher Hacks Self-driving Car Sensors. Retrieved from https://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors

[9] NetworkNewsWire. (2018, June 13). Self-Driving Car Companies Face Choice Between Active and Passive Sensors. Retrieved from https://www.prnewswire.com/news-releases/self-driving-car-companies-face-choice-between-active-and-passive-sensors-685358311.html