Driverless occur when there are software glitches which

Driverless vehicles also known as autonomous vehicles is an Artificial Intelligence(AI) vehicles capable of navigating, sensing its environment input and designed to travel between different destinations without any form of human intervention. Ultrasonic, Radar and Light Detection and Ranging(LiDAR) are some examples of how advanced technology will assist to build a driverless vehicle.

For example, an image sensor will help to detect colors and fonts, giving the capability to detect traffic lights, signs and lane markings. LiDAR on the other hand measures the distance from the car to its surrounding objects allowing the vehicles to notice nearby hazards. Autonomous technology might be one of the many solutions to overcome shortage of manpower and increase productivity in the near future, however there are many other factors to be taken into consideration before the implementation of driverless vehicle on Singapore roads, some of which are; Safety, Cyber Security and Privacy. On 9th of November 2017, a self-driving bus ended in a crash less than two hour after its launch in Las Vegas. Thankfully there were no fatality involved. On 19th October 2016, an autonomous car was involved in an accident with a lorry while changing lane in Biopolis Drive at one-north. A nuTonomy spokesman mentioned such cases only occur when there are software glitches which affects the performance of an autonomous car in terms of its detection and response to surrounding hazards. The accident raised many concerns about the safety of an autonomous car in the Facebook group (Lin, 2016) however nuTonomy released a statement mentioned that they have made necessary improvements to the software and relevant authorities are aware that trial run has resumed on public roads.

Safety must be of paramount importance due to the rise of aging population and high traffic flow during peak hours on Singapore roads. GPS applications, car audio system are a few examples of how technology communicate with the outside world to get necessary information to work for us. This in turn provides a series of opportunities for hackers to penetrate our system. Computer area networking(Cans) is the immediate challenge that we must overcome to prevent hackers from taking control of the car remotely even though automotive makers have installed gateway as a solution.

The gateway is not a guaranteed solution as skilled and patience hackers can find loophole to penetrate and steal sensitive information. To allow autonomous vehicles to operate freely, sufficient security measures must be enforced to ensure that we are well protected by different group of hackers. Personal Data Protection Act(PDPA) was established to protect the rights of an individual when it comes to personal data collection.

As autonomous testing is picking up speed in Singapore, data privacy remains a concern. Autonomous vehicles require real-time communication between its surrounding and its user, sensitive data such as passenger’s or driver’s information, driving patterns may be collected and stored for authentication purpose or customization of safety and comfort. Such information is extremely valuable to marketers as it can be used by retailers to push notices such as offers and discount to consumers who are in the vicinity. To ensure users are secured from privacy violations, autonomous vehicles might need to give user a choice to store or permanently delete the data after a certain period.

Singapore is moving towards a Smart Nation goal, a $3. 6million facility has been jointly developed to put autonomous vehicles to test in a safe and well controlled simulated environment to ensure autonomous vehicle has the capabilities to adapt and react on Singapore roads. Some features of the simulated environment like the flood zone will allow researchers to analyze how autonomous vehicles will react to the situations. As with any newly implemented technologies, there will be teething issues to iron out. Singapore may work towards having driverless cars on our roads in the rear future by tackling the above-mentioned factors systematically.

Precautionary measures should always be taken, and security threats should always be anticipated. Lastly, data privacy of an individuals should not be taken lightly at the expense of modernization.