Autonomous Vehicles: Are they Safe?
Byron A. Ellis – April 15, 2018

Many believe that autonomous, self-driving or robotic vehicles are the future of the automobile industry and a source of profit for the ride-sharing industry. Some proponents of autonomous vehicles (AVs) argue that these vehicles will increase safety, lower insurance rates, reduce crime, improve traffic flow and so on. Others, such as Solomon, are aware that "Autopilot controls are not yet fully capable of functioning without human intervention – but they're good enough to lull us into a false sense of security."

Ramos reported that in May of 2016, Tesla's Autopilot software failed to detect a white tractor-trailer against a background of a bright sky and the car fatally collided with the tractor-trailer. In March of 2018, Uber had a fatal accident, with an AV SUV struck and killed Elaine Herzberg in Tempe, Arizona. And, as of April 6, 2018, the California Department of Motor Vehicles received 65 Autonomous Vehicle Collision Reports. Additionally, a 2017 study by Favarò et al. indicates that "…accident frequencies computed for all manufacturers showed that conventional vehicles drive one order of magnitude more miles compared to AVs before encountering an accident, with a mean mileage before a crash for conventional vehicles of about 500,000 miles, compared to 42,017 miles for AVs."

AVs use technology, such as radar, laser light, GPS, odometry, and computer vision to detect their surroundings and software programs to identify appropriate navigation paths, such as destination, obstacles, and so on. Therefore, AVs control systems must be able to analyze sensory information inputs to avoid collisions accurately.

The three basic elements of AVs technology are sensing, mapping, and negotiating the road. The last two elements are complex. The maps must be highly detailed, accurate, and constantly updated. Additionally, for AVs to negotiate the roads, they require robotics on the vehicles to act like humans, which is constantly learning.

Some AVs manufacturers plan for their cars to communicate with each other and even with traffic signals. Thus, requiring constant online data connectivity. However, limited or non-existent online connectivity in certain regions would require human control of the car. Constant online connectivity can be a potential weakness for AVs. In 2015, security researchers demonstrated that AVs connected to the Internet could be hacked. Thus, hacking could be a significant possible terror threat, where AVs could be taken over and used as weapons.

Environmental factors, such as snow, ice buildup, or even heavy rain, as well as unpainted lanes on roads and highways, could impair the robotics, lenses and radars. Additionally, the software could become temporally corrupted and machine learning and pattern recognition might not work as effectively as predicted. AVs can expose passengers to electromagnetic frequencies that could adversely affect their health.

Finally, if a collision impairs any camera or sensor on an AV, its drivability will be in peril, and repairs are likely to be expensive.

Copyright of TJP is the property of The Jethro Project, and its contents may not be copied or emailed to multiple sites or posted to a listserver without the copyright holder's express written permission. Users, however, may print, download, or email articles for individual use.