LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com

WEDNESDAY, SEPTEMBER 6, 2017

PERSPECTIVE

Solutions needed as self-driving cars speed toward the next level

By Jonathan Michaels

The future is already here in many respects, at least as it relates to autonomous vehicles. While fully autonomous "level 5" vehicles are still some time out, scores of automakers are already introducing level 2 (partial driving automation) and level 3 (conditional driving automations) vehicles to the consuming public.

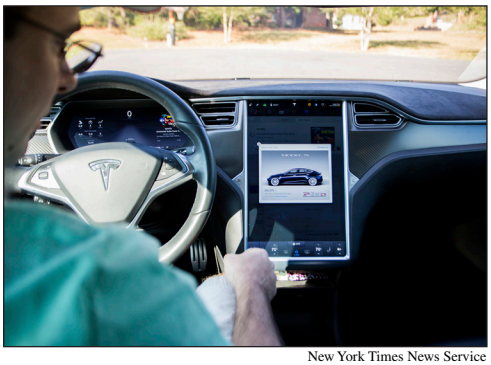
This year, the redesigned Cadillac CT6 will exhibit GM's new "Super Cruise" technology, a Level 2 autonomous system that will allow the driver to take his hands off the steering wheel in limited highway settings. The system uses a small camera located on the top of the steering column to track driver head position, signaling that driver input is required if the driver has turned attention away from the road ahead for too long.

The top of the hill, however, belongs to Audi, whose new A8 will be the first production vehicle with level 3 autonomy. At speeds of up to 37 miles per hour, the vehicle will accelerate, steer and brake on its own, without requiring the driver to take back control on regular brief intervals; when the vehicle can no longer ensure safe operation, such as in hazardous driving conditions or at higher speeds, the car will signal that the driver will have 10 seconds to take back control.

Audi claims that in 2020, it will introduce a level 4 vehicle, which will offer hands-free driving at posted highway speeds, with the vehicle being capable of executing lane changes and passing cars independently.

On the face of it, the benefits of autonomous technology are tremendous. Aside from allowing multi-tasking and the transportation of ambulatory citizens, Audi claims that automated vehicles will eliminate 94 percent of all car accidents that are attributable to human error.

Yet the technology is not without incident. Many will recall the May 2016 incident where Joshua Brown, a former Navy SEAL, was killed when his Tesla Model S collided with a semitruck, while the vehicle was being operated in autopilot mode. The National Transportation Safety Board concluded that Brown was at fault, as he ignored seven warnings from the vehicle to retake control. But the incident underscores a manifest problem of consumers misusing — or misunderstanding — the limited nature of an "autopilot" system.



New York Times News Service

A Tesla owner operates the Autopilot system, in Hickory, North Carolina, Sept. 6, 2016.

And there is a much larger issue looming. From a macro sense, autonomous cars operate on LIDAR (Light Detection and Ranging) technology, combined with other sensory-receiving devises, such cameras, radar and ultrasonic sensors. Here is where the problem arises.

In a series of white-hat attacks, hackers have demonstrated just how susceptible an autonomous car can be to a variety of attacks. In one of the most shocking incidents, researchers at UC Berkeley figured out how to hack self-driving cars by putting innocent-looking stickers on street signs. By calculating the algorithms used by a vehicle's LIDAR system, the researchers learned that strategically placed stickers on a stop sign tricked the autonomous car into reading the sign as 45-mile-per-hour sign.

What is most troubling about the experiment is the ease at which it was conducted, and the subtle nature of the intrusion. To the human eye, the stickers looked like harmless graffiti, not the LIDAR-jamming algorithms they truly were. And the experiment was not alone.

Other white-hat attacks include sending beams of light to the car's LIDAR system on the same wavelength that the LIDAR uses. With this, the hackers were able to erase stationary objects in the LIDAR's sensory output. In another attack, researchers captured the laser pulse emitted by a LIDAR, added delay, and then sent back a corresponding pulse using their own laser, causing the vehicle to think that objects were in its path when they were not.

Other researchers have shown that the inter-related cameras used by self-driving cars can be blinded by a series of LED lights, causing the vehicle to immediately stop; and still others have tricked LIDAR systems into believing objects are not present by wrapping them in acoustic dampening foam.

While much of the industry has, correctly, focused on the cyber-hacking of autonomous vehicles, crude, physical manipulation of LIDAR systems has gone largely unnoticed. And it is here, where countermeasures are perhaps the most difficult to employ, that the danger is the greatest. With every advancement in LIDAR and radar technology, hackers will try to find algorithmic ways to disrupt the system.

Counter-cyberattack company Security Mentor suggests that the auto manufacturers place "bug bounties" on their cars, offering rewards to anyone who can hack into their systems, with the hope of building more resilient systems. The current wisdom for countermeasures includes outfitting cars with redundant systems and employing random emitting signals.

Whatever the solution, the need is paramount, as terrorists' cells have focused heavily on using automobiles as methods of mass destruction. Few can forget the Bastille Day massacre that occurred in Nice last July, where 86 people were killed and 434 more injured when a 19-ton cargo truck drove into a crowd of celebrating citizens. Or the cargo truck driven into a crowded Christmas market in Berlin last December, killing 12 and injuring 56.

It has been said that technology has advanced more in the last 30 years than in the last two thousand, and perhaps nowhere is this more true than with the advancement of the automobile. The simple, yet reliable concept of an internal combustion engine being used to propel a family of four has morphed into a journey that not long ago would have been considered pure fiction. It is now up to us to prevent this advancement from being our ultimate transportation downfall.

Jonathan Michaels *is the founding member of MLG Automotive Law, APLC, which specializes in representing clients in the automotive industry. You can reach him at (949) 581-6900 or jmichaels@mlgautomotivelaw.com*