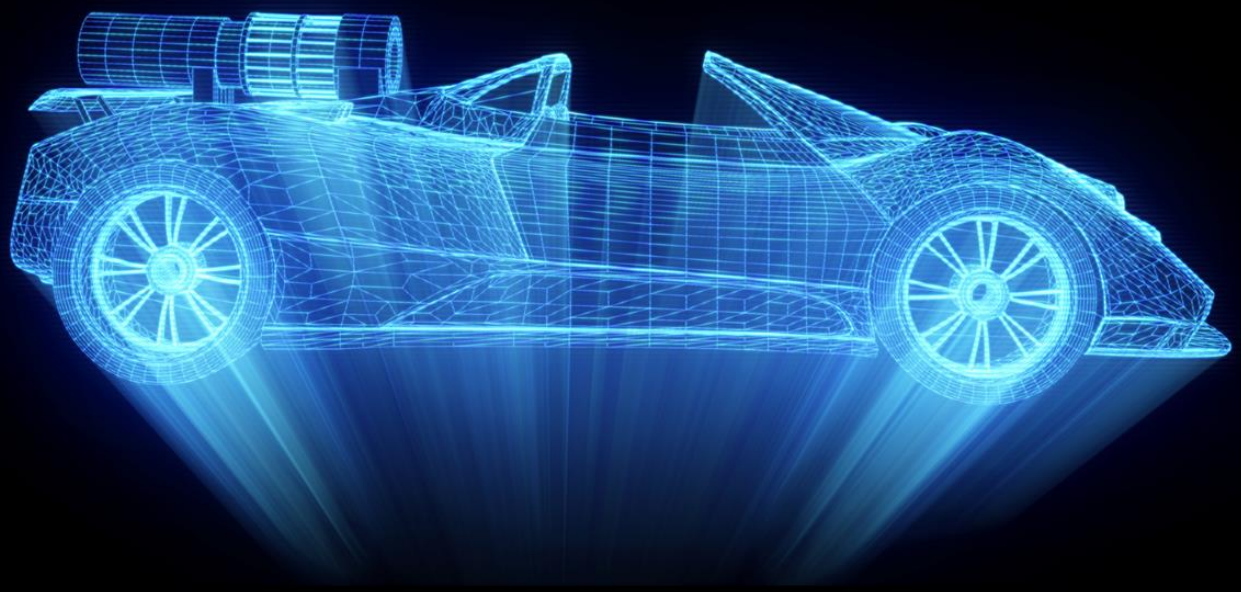
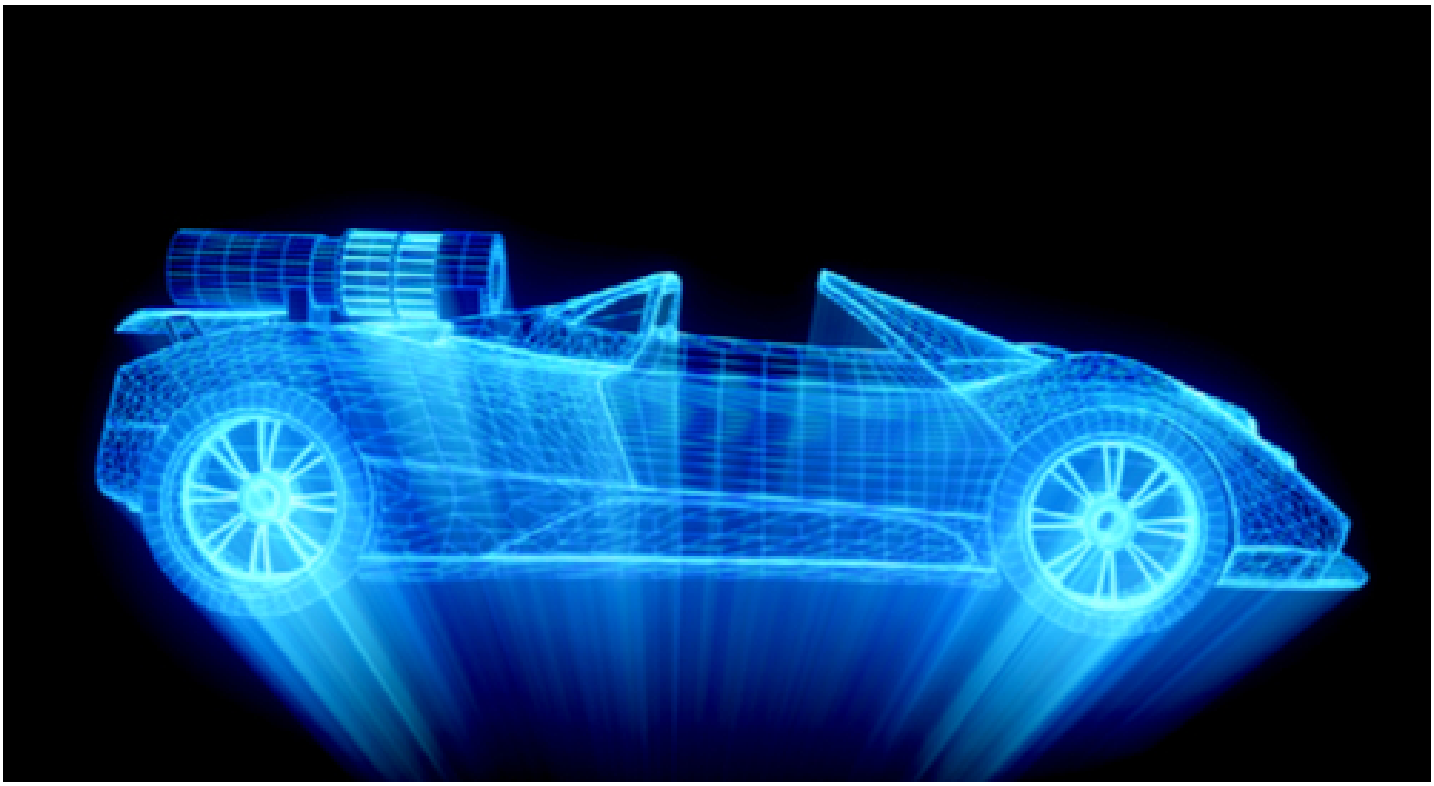
Altium®

Autonomous Vehicle





AUTONOMOUS VEHICLE

When it comes to self-driving cars, or vehicles with autonomous systems or advanced driver assistance systems (ADAS), the stakes are a bit higher. If someone hacks into your vehicle they could disable it, or even worse, crash it and possibly harm any passengers inside. This risk is a difficult one but it can be managed. Learn more about autonomous vehicle security and ways to build security from the inside out.

Join us as we discuss a variety of topics to help you decide if Autonomous Vehicle is for you, including:

- Autonomous Vehicle Cyber Security: Safety Within and Without
- Survey of Autonomous Vehicle Tracking with GPS Navigation Systems
- How Autonomous Vehicle Map Building Benefits ADAS Vehicles

AUTONOMOUS VEHICLE CYBER SECURITY: SAFETY WITHIN AND WITHOUT

Cybersecurity is of the utmost importance. Approximately 143 million Americans were reminded of this when Equifax, a credit company, was hacked and their data was compromised. If Equifax had followed industry best practices, this breach could have been avoided. Since they didn't, millions of Americans are now at risk of identity fraud. When it comes to self-driving cars, or vehicles with advanced driver assistance systems (ADAS), the stakes are a bit higher. If someone hacks into your vehicle they could disable it, or even worse, crash it and possibly harm any passengers inside. This risk is a difficult one to tackle but it can be managed. If you ignore it, you might end up like Equifax, with a big mess on your hands and no excuses to cover you.

HIGH STAKES SECURITY

Two security researchers have been hacking vehicles for years in an attempt to expose vulnerabilities and raise awareness about safety problems in the automotive industry. They've been continuing that work, and have also started speaking more publicly about the cybersecurity risks that come with self-driving cars. Autonomous vehicles will present hackers with the unique opportunity to physically interact with a target vehicle without having to buy or steal it. Once physically plugged in, hackers could use increasingly ubiquitous ADAS features to control the car with disastrous consequences.

Not too long ago they remotely hacked into a Jeep Cherokee and were able to activate or deactivate important components like the brakes and transmission. Soon after the hack was shared with Chrysler, the company patched the car's software so that the researchers couldn't hack it remotely. They've since been doing more work that involves physically breaching the car's security systems. Being in the car allowed the researchers to hack into the vehicle's CAN network, an internal network that allows for

communication between components. Once someone has access to this network they can use it with disastrous effect. In their previous hack, the researchers took over individual components and were able to activate or deactivate them. Using this method they were able to disable the central controller with safety features that could prevent them from doing too much damage. With that electronic control unit (ECU) out of the way, they could hijack the entire system instead of interfering with individual components. Other researchers have also been able to use the CAN network to simply disable components. They corrupt data coming in from sensors or microcontrollers to the central processor, and eventually, the primary controller thinks the component is damaged and cuts it off. There's always the risk that your components can fail in the field by chance, but this kind of attack could shut down all ADAS features simultaneously.

This could become a very real image.

This raises the question of how will hackers ever have physical access to your vehicle? Well, if you're designing a self-driving car that could be used as a taxi the answer is, all the time. Charlie Miller, one of the researchers who hacked the Jeep, has spoken out to highlight this risk after working for Uber. Any passenger in a driverless Uber would be able to hack into your car. They can gain access to a car's internal systems using easy targets under the dashboard, like the OBD2 port.

Once inside a car's network, a hacker could use the CAN network's security flaws to tamper with any part of the vehicle that is controlled by computers. In older cars that may have just been cruise control or a few other features. Now in ADAS enabled cars, everything from the brakes to steering can be controlled by ECUs, and are thus vulnerable to attack. Autonomous vehicles pose a particularly dangerous risk, because the user may not be able to physically override computer controls. For example, in the Jeep hacking the researchers could activate cruise control to accelerate the car, but if the driver tapped the brakes cruise control would disengage. In a self-driving car that doesn't have brakes, an accelerator, or even a steering wheel, the user does not have the features to override such a hack.

SECURITY PRECAUTIONS

The stakes are high when it comes to securing autonomous vehicles. First you can physically secure your car's systems to prevent a rider from accessing them. Then you can focus on software safety by implementing failsafes and self-checks.

It can be difficult to physically secure a modern day car. It's illegal to permanently disable the OBD2 port that I mentioned earlier. However, you can try to guard your systems or make them tamper-evident to mitigate these concerns. Manufacturers should try to make ports difficult to access. A rider shouldn't be able to easily pop off a section of the dashboard and access critical circuitry. Masking components can mitigate some of that risk, as it's more difficult for a hacker to enter a system if they don't know what kind of components they're dealing with. In addition, using things like tamper-evident tape can help you know when someone has opened something they shouldn't have.

You're much more likely to foil hacking attempts with software than with physical protection. In the original Jeep hack, the researchers were only able to interfere with a few features because the central ECU had safety checks that prevented further meddling. Once they disabled that ECU, it was a free for all. Using software checks to make sure your components are still working can alert you to intrusions. If your controller is in update mode while driving, you will know that there's a problem and can park the car until the issue is fixed. Checking components can help foil attacks like the disabling hack mentioned earlier. Maybe someone has used the CAN network to trick the processor into thinking sensor aren't working. If those sensors are self-checking they can tell the controller that they are, in fact, operational and trigger some kind of failsafe. If you know an attack is happening you can mitigate it. The problem comes when you don't prepare for a breach and let the hacker run amok in your system. You should also try to segment your system as much as possible to prevent cascading failures. If someone hacks into the entertainment system in your car they shouldn't be able to use it to disable the entire system.

Cars without steering or brakes leave the user at the mercy of electronic controls.

Cybersecurity is a very complex problem that can be difficult to solve, however it must be addressed. Ignoring this issue in ADAS

enabled vehicles could lead to injury or death, so the risk is high. When designing your software you should assume that hackers will have physical access to the network, knowing is half the battle. Then you can focus on designing software that checks components, and itself, to detect when an attack is happening. Once you know something is wrong you should have fail-safes in place that can either stop the attack or park the car so that no one gets hurt.

If you're going to design impregnable software you're going to need the best tools at your disposal. TASKING makes products like standalone debuggers that can speed up your development time and static analyzers that can help you check your memory and prevent cascading failures.

Have more questions about cybersecurity? Call an expert at TASKING.

SURVEY OF AUTONOMOUS VEHICLE TRACKING WITH GPS NAVIGATION SYSTEMS

I for one, am very thankful for the Global Positioning System (GPS). While most animals in nature are born with an innate sense of direction, I was born with natural misdirection. That's why I use my phone's GPS to get everywhere I'm going. GPS is a relatively old technology that could find new uses in autonomous vehicles or cars with advanced driver assistance systems (ADAS). Everyone is busy trying to find the right mix of sensors to navigate by, and GPS is certainly going to be one of them. Once you know exactly how GPS works you can better understand its limitations and potential. That promise is shown in several emerging technologies that could use GPS to help automobiles drive themselves.

HOW DOES GPS WORK?

The United States government developed GPS back in the 80's through the air force and maintains it to this day. Originally this system was only made available to the military and was used to guide boats, aircraft, or other vehicles. It uses a constellation of satellites that transmit data at precise times, which allows receivers to determine their position. In the past, the government degraded the signals available to the general public to reduce its accuracy. Now, that policy has ended and we are able to utilize the network to its full potential.

There are at least two dozen satellites that form the backbone of GPS. These satellites transmit three different signals: their ID codes, Ephemeris data, and Almanac data. Receivers on the ground need Ephemeris and Almanac data from at least 3 satellites to

determine their location. The Almanac information gives the receiver a general idea of where satellites are in the sky and lets it estimate which ones should currently be visible. Once the receiver has connected with 3 or more satellites it uses the Ephemeris data, which contains a much more accurate location and time, to find its position. At least three satellites are required for that because the receiver's 2D whereabouts are triangulated. In order to get a read on 3D location you'll need to connect to a 4th satellite. Receiving data from more than 4 satellites will increase the accuracy of your tracking.

Before the 2000's that accuracy was purposely limited by the US government. They didn't want anyone to be able to use this system against them, so they attenuated the outgoing data randomly in order to limit its veracity. Back then a civilian GPS receiver could only calculate position to within 100 meters. Today the Air Force no longer interferes with GPS signals and we can use the satellite constellation to calculate location within 3 meters.

The GPS constellation orbits the Earth constantly.

GPS LIMITATIONS

GPS is an incredibly useful technology that has revolutionized travel worldwide. It does, however, lack some things that would make it particularly useful for autonomous vehicles. The first shortfall is its accuracy, which makes it unsuitable for most ADAS applications. The second problem is that it requires line of sight to satellites, which is not always possible when driving in cities.

While an accuracy of 3 meters is more than adequate for general navigation systems in cars, it's not quite enough for ADAS features. If my car is going to change lanes by itself it can't miss the lines by 9 feet, it needs to be within inches. There is no easy solution for this problem, though many people have worked out possible fixes.

There is also the problem of "urban canyons." In many large cities tall buildings can block GPS signals. Since a receiver needs a line of sight to at least 3 satellites in order to calculate a rough location this is a big issue. If my car is piloting itself using GPS and suddenly loses 4/6 satellites I could crash. This problem is also a hard one to solve, but fortunately neither of these are insurmountable.

Urban canyons can block or distort incoming GPS signals.

NEXT GENERATION GPS

Despite its flaws, GPS is far too useful to give up on using. That's why several technologies have been developed to solve, or at least mitigate, some of the accuracy and line of sight problems. These include things like: differential GPS, Precise Point Positioning, and multiple sensor fusion.

- Differential GPS - This kind of scheme uses a base station with a known position to increase the accuracy of GPS. By using a signal coming from a precise point near the ground a receiver can determine its location within centimeters instead of meters.

- Precise Point Positioning (PPP) - This method focuses on the calculation aspect of GPS in order to improve its accuracy. In order to enable PPP, you'll need to use a dual-band receiver. By using two layers of satellite signals you can get centimeter-level precision. The downside is that PPP takes a lot of processing and time.

- Multiple Sensor Fusion - Multi-sensor fusion is already common in the automotive world, and can also be applied to GPS. In this case an accelerometer can be paired with a receiver to keep tracking location when satellites are lost. This arrangement is already used to track units through tunnels and can be easily implemented for urban canyons.

GPS has been helping us get around since its inception. First tracking users down to 100 m and now to within 3 m, these receivers help me drive every day. Someday they might be able to drive for me, but some problems will have to be solved first. In order to be reliably used for ADAS features a GPS receiver will need to have centimeter accuracy and be able to continue tracking position even when it loses satellites. There are a variety of fixes available, but differential GPS requires physical base stations, and PPP takes a little

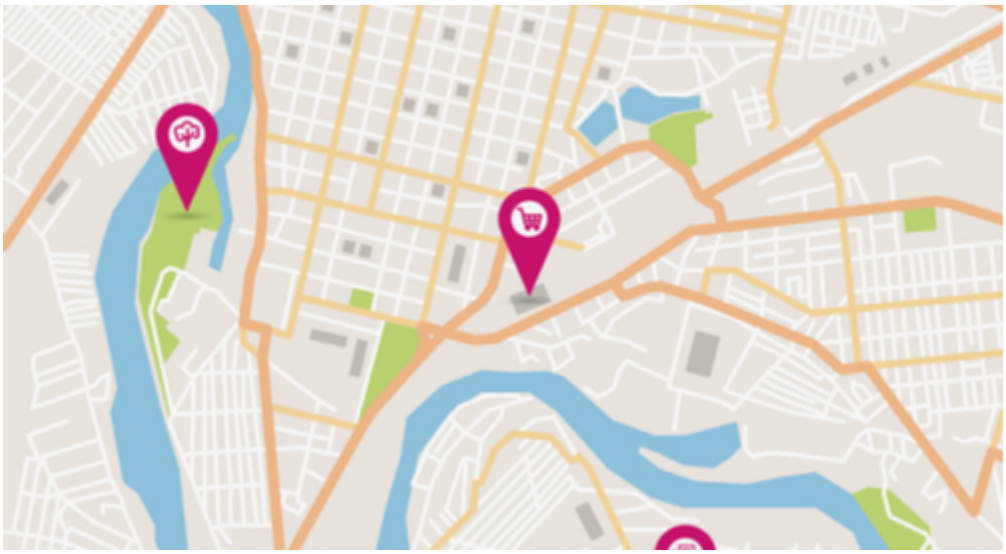
too long to come up with results. At least the tracking problem should be solvable by integrating other sensors with GPS.

The problems that GPS faces are nothing compared with the complexities of developing software for ADAS enabled vehicles. Luckily there's an easier fix for that than for GPS. TASKING has developed a variety of software tools that are specifically targeted for the automotive industry. Their products like standalone debuggers and static analysis tools can help you speed up your development and make your programs more efficient.

Have more questions about GPS? Call an expert at TASKING.

HOW AUTONOMOUS VEHICLE MAP BUILDING BENEFITS ADAS VEHICLES.

It's always been interesting to me that the explorers of the past were cartographers. It makes sense, there was no point in exploring something new if you weren't able to map it out and show it to the people back home. Even today map makers are still on the edge of the unknown, although this time the frontier is autonomous navigation. Vehicles with advanced driver assistance systems (ADAS) are becoming more numerous each day, and most of them need high definition maps in order to operate. Interestingly, they're not only used by ADAS vehicles but can also be created and updated by connected cars. These maps won't just show roads and bridges but will model streets down to curbs and potholes with centimeter accuracy. High definition outlines of roads will give future vehicles something to rely on when their onboard sensors aren't working. They may even eventually reduce the need for complex multi-sensor arrays on ADAS enabled cars.



Current maps are not high enough resolution to bed used in ADAS cars.

WHAT IS AN HD MAP?

The maps needed by modern-day ADAS enabled vehicles are like the ones your old TomTom or Garmin used, only much more detailed. Where the maps that we use daily on our mobile phones are accurate within a few meters, these will need to outline the streets in terms of centimeters. They'll also have to be updated daily or weekly since cars will be using these charts as part of the backbone of their navigation systems.

I have to admit that I occasionally take a turn too sharp and hit a curb now and then. When I'm driving I may find that acceptable, but if I'm in a self-driving or semi-autonomous vehicle bouncing off things will make me a bit nervous. That's why new HD maps are moving from meter resolutions, down to centimeter accuracy. Users will want their cars to navigate effortlessly, and that will mean roads modeled down to every curb, pothole, and sign. In order to do this, most companies use things like LIDAR and other sensors found in ADAS vehicles to accurately map roadways.

As Bob Dylan might say, the roads they are a-changin', which is why they need to be re-assessed on a regular basis. Many companies have already taken to the streets to do just that. Some develop and run their own systems to chart out highways, while others are planning to contract out that work to people with ADAS cars or the requisite sensors. These updates will give us constantly changing maps that evolve or devolve in the case of potholes, as our roads do. They could also replace user reported events, like traffic delays, that are already integrated into navigation apps.

New maps will help us avoid potholes like this one.

HOW DO THESE MAPS FIT INTO VEHICLES?

Autonomous vehicles have been driving the streets for years already, so why do we suddenly need these high-quality maps? Well, some of those cars have already been using those maps to find their way. Even if a car uses a large and diverse sensor array to navigate, it will still need detailed charts to use as a backup system. Beyond physical driving, these maps let companies simulate scenarios during development. This allows them to investigate potentially dangerous circumstances on a computer rather than out in the real world.

- Primary Navigation - We all know that Google has had self-driving cars on the roads for years. What you may not know is that they did this by using highly detailed maps. The problem with using these outlines as the main means of travel is the car won't work when there aren't maps. That's why those companies are working on mapping every pathway they can.

- Backup System - One of the main challenges for ADAS vehicles is ensuring safety. A car may use a suite of sensors and their data to explore its environment, however, those sensors may not always work. LIDAR can be inhibited by rain or snow, and then your vehicle can have an accident. Highly detailed maps coupled with advanced GPS can provide a secondary system in case the main sensor array fails.

- Simulation - It's always better to test a system in simulations before risking a costly prototype. That's what Waymo is doing with their HD maps. They use data gathered in the real world to simulate roads and then drive virtual cars on them for testing. This allows them to come up with a viable solution to counteract difficult conditions before experimenting with a real car.

All of these are reasons that we need detailed virtual maps, and together they become an imperative. Google started the detailed mapping, but now other companies have joined the fray in a race to see who will control the virtual landscape of the world's roads. Once streets have been mapped ADAS vehicles can drive on them safely, either using the map as part of a primary or secondary navigation system.

While others are intent on developing HD maps of the world, you're focused on developing programs for the cars that will use them. Just like those vehicles need a map to guide them, you could use software to help you during development. TASKING has developed a variety of products, like a standalone debugger and static analysis tool, that are made specifically for the ADAS industry.

Have more questions about HD maps? Call an expert at TASKING.

ADDITIONAL RESOURCES

Thank you for reading our guide on Advanced PCB Layout. To read more Altium resources, visit the Altium resource center here or join the discussion at the bottom of each original blog post:

- Autonomous Vehicle Cyber Security: Safety Within and Without
- Survey of Autonomous Vehicle Tracking with GPS Navigation Systems
- How Autonomous Vehicle Map Building Benefits ADAS Vehicles