AMREL

Taking the Point for 25 Years

Cars are the new UGVs

William Finn, AMREL Senior Copywriter & Editor
September 18, 2012

I once read a quote from a futurist that many distinctions that we currently take for granted will be not be valid in the future. Things that seem as different as day and night will be indistinguishable. Day and night, for example. The proliferation of night vision and other sensor technologies will cause future generations to have radically different views about the level of privacy traditionally offered by the cloak of night. Another distinction that is already blurred is the one between manned and unmanned vehicles.

As described in an earlier blog post, A future for manned unmanned vehicles?:

> "Optionally Piloted Vehicles (OPV) are turning up in a variety of places. The US Army, for instance, plans to include some level of autonomy on trucks and other vehicles. It is unknown whether these technological switch hitters will disappear as society becomes more comfortable with unmanned systems."

However, even for vehicles that meant to be primarily manned, the similarities with unmanned systems – especially on subsystem and security levels - are growing. Recent stories in the New York Times and Car and Driver have highlighted concerns about "hacking" cars. In much the same tone as articles expressing fears about GPS spoofing, the authors report on successful efforts by researchers to gain remote access to cars. Even a conventional manned car has numerous computers, which on modern vehicles are linked through a network as a controller-area-network bus, or CAN bus.

> "Currently, there's nothing to stop anyone with malicious intent and some - computer-programming skills from taking command of your vehicle. After gaining access, a hacker could control everything from which song plays on the radio to whether the brakes work." Car and Driver.

Based on a 2010 study, researchers affiliated with the Center for Automotive Embedded Systems Security contend that hacking can be done through a number of vulnerable points in an automobile's computer infrastructure. For example, an inventive hacker could access your car's systems through an MP3 file over WiFi (watch for the future article, "Is your playlist trying to kill you?").

Even though critical systems, such as steering, are not *directly* connected to the less secure systems, such as the radio or music player, they are still at risk. The communication networks of the car are so interconnected that a compromise in one can affect the other.

According to the article, this kind of car hacking is time and labor intensive, so it isn't worth the effort. Is it worth the effort for an enemy to hack an Unmanned Ground Vehicle (UGV)? Will military operations against UGVs develop a hacking methodology that can be used against civilian and manned vehicles? Or will be the other way around? Will the proliferation of autonomous passenger cars create an incentive for hackers to develop a technology that can also be used against military UGVs?

The overlap between civilian automobiles and military UGV security concerns is noted in a press release from Black-I Robotics. When they announced they were awarded a contract with the Air Force for securing robots from hackers, they mention the Car and Driver article. (Read about the DARPA program behind the contract at High-Assurance Cyber Military Systems)

Clearly Black-I sees this research project as impacting civilian cars. One of the contract's deliverables will be a medium-size UGV that is equipped with an anti-collision radar system that, in theory, could be used to safeguard civilian autonomous vehicles.

Much of the current focus of the transition of unmanned system technology to the domestic market has focused on Unmanned Aerial Vehicles. However, as pointed out in UGVs &UAVs in domestic markets, UGVs are much more likely to have an impact on the lives of most people.

Will today's developers of military UGVs be tomorrow's manufacturers of autonomous civilian cars? Probably not. However, it is clear that the technologies developed for one will be adapted for another.