*Technical Article*

# *Securing the Scene*

Chuck Brokish

Out in the suburbs, the businessman walked out his front door, slipped into the back seat of his sedan, and said “To the airport, James! And take the express lane.” James responded, “Right away, Mr. Smith. And with current traffic conditions, you should be there in about 23 minutes.” James guided the car onto the highway entrance ramp, effortlessly surveyed the hundreds of vehicles already on the packed highway, seamlessly merged through several lanes of traffic into the express lane, and Mr. Smith was on his way to an on-time flight departure. After dropping Mr. Smith at the door of the airport, James proceeded to park in the ramp and await Mr. Smith’s return.

Meanwhile, downtown, a car was stolen. The culprit got into the car without breaking any glass or alerting anyone around. He started the car, navigated out of the parking lot and guided it through the busy streets during the lunch hour rush, directing it to the end of an alley on the edge of town, where it was stripped, repurposed and resold. But the thief never even touched the car. Instead, the car was remotely hacked through the network using on-board navigation, and aided by an intricate system of sensors and guidance from both inside and outside of the vehicle.

At first glance, it would appear that these two vehicles and two scenarios were not linked or associated with each other in any way. But they were: they were linked to the same network: a fully-integrated traffic network with information about real-time traffic conditions, all of the other vehicles on the road, and computer precision that is capable of navigating through complex traffic, without a moment’s hesitation. The same technology that enabled James, a fully integrated autonomous vehicle, to get Mr. Smith to the airport on time and with no needed human assistance also enabled someone to steal a car without even being present.

Now, before you start screaming to stop the insanity and rip out all of the connected systems in your car, you must recall that anything created for good could be used for the wrong purpose. This has been true for all of history. The simple knife that was created to feed a family by being used as a tool for hunting and cropping, has been used as a murder weapon.

We cannot stop progress out of fear. But rather, we can progress with caution. We cannot prevent someone from having ill intentions, but we can protect ourselves from those intentions. The many comforts of life that we enjoy today are the result of technology used for good.

While there may be deliberation as to what level of autonomous driving we can ultimately achieve, we know that the underlying technology can be used to ease our lives and to save our lives. There is no question that such capabilities as anti-lock braking, traction control, and airbags help to save lives. Cruise control and electronic shifting allow cars to gain much better fuel efficiency, and GPS navigation allows us to save time and money. Continuing this trend, adaptive cruise control, automatic emergency braking, lane departure warning, automatic traffic routing, and many other technologies will continue to make our lives easier and safer, while allowing us to more efficiently utilize our existing highway infrastructure to handle more traffic with fewer accidents.

So, how do those working on these autonomous driving systems enable the advancement of driver assistance, automated driver services, and more autonomous capability without enabling malevolent use of such technology? They start with security in mind from the very beginning! Security cannot be an after-thought. Security must be embedded within the product, within the design, and within the silicon used in the product.

At Texas Instruments, we have been working on silicon for use in a variety of automotive technology applications for decades. TI has deep experience in automotive safety as well as strong capabilities in embedded security.

TI’s recent high security versions of the “Jacinto 6” family of infotainment processors are designed to help car-makers who need sophisticated and robust features.  The high security versions of “Jacinto 6” include features that help the car-maker authenticate the software during the boot process, update the software, and strengthen the security of run-time applications and transactions where sensitive personal or vehicle information is present. Additionally, the high security versions of “Jacinto 6” provide a strong foundation of security on embedded silicon that customers can then augment when implementing their specific security requirements in their system-level solutions. Watch this video to learn more about the available security features on “Jacinto 6” processors.

It is through intelligent design, and considering security as a fundamental embedded capability, that the next generation of vehicles can be enabled in a safe and secure manner.

# IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265