MENU

SEMICONDUCTOR ENGINEERING

(/)

IOT, SECURITY & AUTOMOTIVE (/CATEGORY-MAIN-PAGE-IOT-SECURITY/)

What's New In Connected Autos

37 380 38

Internet of Things technology will be crucial to automobiles, but connectivity comes at a price.

FEBRUARY 2ND, 2017 - BY: JEFF DORSCH (HTTP://SEMIENGINEERING.COM/AUTHOR/JEFF-DORSCH/)

Connected cars and the Internet of Things go together like peanut butter and jelly. But realizing the future of autonomous vehicles will demand close attention to be paid to cybersecurity, functional-safety standards, and other critical factors.

IoT (http://semiengineering.com/kc/knowledge_center.php?kcid=76) will advance the era of self-driving cars, which currently is dominated by Tesla Motors. At the same time, it will change some of the dynamics in this market. On one hand, it will turn automotive manufacturers into technology companies, which could provide new revenue streams for carmakers. On the other hand, it will open the door for new players that have never had a viable entry point in the automotive market.

(http://semiengineering.com/wp-content/uploads/2017/02/Screen-Shot-2017-02-01-at-8.35.48-PM.png)
LiDAR sensor Source: Velodyne LiDAR, based in Morgan Hill, CA

Consider the case of Velodyne LiDAR, a Morgan Hill, Calif.-based company, which last month opened a factory in nearby San Jose to manufacture its LIDAR product. The company sees the plant making 1 million LIDAR sensors a year in 2018. It also has opened a research and development facility, Velodyne Labs, in Alameda, Calif.

"IoT in one sense is a very, very broad term," said Richard York, vice president of marketing for ARM (http://semiengineering.com/kc/entity.php?eid=22186) Embedded Segment. "Cars sort of inhabit the IoT space, but they're also not an IoT device in the traditional sense of the word. They're starting to be data collection devices. The data that cars can collect is being significantly undervalued today and almost completely underutilized, or untapped. There's an enormous untapped opportunity for vehicles on the road to be collecting very large amounts of interesting data—collecting that data together within the cloud, making sense of that data, and then using that data in interesting ways to offer interesting services, either directly to the things that collected that data or to other people."

Rhonda Dirvin, ARM's director of IoT vertical markets, noted that the data can be used locally or in the computing cloud, but privacy and security will be key considerations to make this model work. "From an overall IoT perspective, there will be IoT-based infrastructure that will help the cars and some of the autonomous driving things, such as sensors in roadways, perhaps depending on how cities want to deploy things," she said.

York noted that functional safety in cars is unlikely to be affected by any of this. "We'll keep the safety aspects and the IoT things pretty separate," he said, adding that privacy issues also will be essential. "You wouldn't want IoT [to have] the ability to collect data from vehicles, or collect data from any piece of equipment, to be a route in to violate or cause safety problems," York noted.

This is true for drones and industrial equipment, as well. "Security is really a spectrum of things," Dirvin added. "In automotive, you have a really tight case where things need to be really secure. The downfalls of someone being able to take over the steering or the brakes or something that can cause people serious injury is much more important, and we're spending much more time and effort and money on the security aspect of that than something kind of more mundane, like my Fitbit."

Self-driving cars

Not everything in a car is connected at the same level, though, and this distinction becomes critical as cars migrate from driver-assisted to self-driving.

"Autonomous vehicles, by definition, need to be operating without external input," said York. "You can't have an autonomous vehicle which is dependent on external data, the IoT data or whatever it might be. They fundamentally have to be autonomous, and able to operate without external connections, because those external connections can never be reliable enough."

IoT still can play a valuable role for autonomous vehicles, such as providing directions or warning of icy road conditions. But determining how a car will react to those conditions and others has to be based upon a set of rules for how the car should behave in a variety of circumstances.

This is where many experts see a growing role for machine learning. "What machine learning can do for IoT is making it more reproducible in other places," said Dirvin. "That's an area we see a lot of application for the IoT space."

But machine learning also has raised some concerns on its own, particularly if changes are made using over-the-air security patches.

"If you look at the IoT, and this is also true for connected car, the problems started once we connected these devices," said Asaf Ashkenazi, senior director of marketing for **Rambus (http://semiengineering.com/kc/entity.php?eid=22671)** Security. "In the past, all these devices were exposed only to local attacks. Once you add Internet connectivity, even if you think the connectivity is limited, it actually eases access to anyone in the world. This makes the device now very vulnerable. Unlike mobile phones and PCs in the past, these devices are actually doing physical things in the real world. If it's a car, it's driving. You can do things that are physically affecting it. And this is true for many other IoT devices, from smart cities to home security. So, on one hand, we suddenly have the vulnerabilities that are added, and the potential damages can be much bigger, because we now add cyber to the physical world. On the other hand, there is almost no security in many of these devices."

Current estimates are that 70% to 80% of installed IoT devices, such as security cameras, do not have secure connectivity.

"We saw what happened to Toyota with the acceleration problem that they had," Ashkenazi noted. "The number of injuries and casualties related to that was quite low, compared to the risk one has to get into the other activities. It got a lot of exposure. But when you add connectivity to cars, somebody can hack into the system and control the connectivity. Even if nothing bad happened, as somebody just demonstrated, it can have a really, really negative effect on people, to the point where they refuse to drive connected cars. The risk of somebody doing that is quite big. I know that the automotive industry had a wake-up call, a little bit late, but I know they are investing a lot in preventing that."

The complexity of cars presents a unique challenge. "People tend to see the car as a mechanical machine, and they don't understand the amount of electronics that gets into a car these days," Ashkenazi said. "In the average car, there are more lines of code than in some of the commercial aircraft. The number of electronic components, the chips, that are running in a car is huge. The potential for an attack as you have more lines and more devices—what we call the attack surface—is much bigger."

While the **SoCs (http://semiengineering.com/kc/knowledge_center.php?kcid=81)** and electronic control units (ECUs) in a car, it's the system of all of these that makes it so difficult to safeguard.

"In the IoT there is also another problem, which is the amount of different platforms and different devices," he added. "At the moment this is in the Wild West stage. At Rambus, our approach is that we will not be able to immediately solve all the problems of the Internet of Things and the vulnerabilities. It will take time."

One of the top methods being suggested, at least for now, is to regulate the access to these devices. The root of trust in hardware is critical for automotive manufacturers, along with securing the Internet connectivity. "Chipmakers need to respond to put the root of trust in the appropriate hardware," Ashkenazi said. "Testing for cybersecurity makes the design cycle quite long. In reality, there is not enough security in chipsets that are going to automotive. Nobody thought of it in advance, and we have some problems today."

Add to that the fact that entire systems are still being developed to sit alongside those that had previously been developed with little or no concerns about security. "Cybersecurity is a moving target," said Olivier Pauzet, vice president of market strategy at Sierra Wireless.

LIDAR vs. I/O

Jeff Hutton, senior director of Automotive Business Solutions at **Synopsys (http://semiengineering.com/kc/entity.php?eid=22035)**, points to three basic steps in the IoT — sense, process, actuate. "We push that into the automotive area, and there's a lot more constraints," he said.

Vehicle-to-vehicle communication is not a reality yet, although the U.S. Department of Transportation has posted an official notice of proposed rulemaking—a first step toward the National Highway Traffic Safety Administration making it a required rule.

"IoT, from a generic standpoint, is an all-encompassing thing," Hutton said. "What we do for automobiles is we add a whole layer of safety onto that. You can't have a failure. The car has to be able to catch if it has a failing component, or if it has a failing braking mechanism or a failing steering mechanism. If something is failing and it can't perform its function of driving, it needs to put itself in safe state, go over to the side of the road, and stay there until the problem either goes away or the problem is fixed. Security is underneath that. We need to make sure that every single car that's talking to each other is talking over a very secure line, and there's no nefarious or no alternative path that someone's coming in and giving us data that isn't correct. There's going to be a lot of handshaking going on."

Among the considerations in designing, developing, and manufacturing autonomous vehicles are whether or not to implement LIDAR, or whether to rely more on advanced vision systems, according to Hutton.

"Vision technology will be providing a lot of horsepower under the hood of a car from a processing standpoint," he said. "The other big thing here is when 5G comes onboard, the amount of data that you will be able to pass and process will be orders of magnitude more than we can do with our current system. That's also going to greatly enhance how fast and how much data these cars that are connected have and can talk to each other. So, 5G is going to also play a role. Do we have to have 5G? Many people say, 'No, we can use the current system. When 5G comes out, it's just going to be a better system.'"

Andrew Patterson, business development director for the Embedded Software Division at **Mentor Graphics (http://semiengineering.com/kc/entity.php?eid=22017)**, said that many cars have their own data plans, and that they can connect through four mechanisms – embedded modems, smartphones, short-range communications (75 megahertz band), and Wi-Fi (5.5 gigahertz band). One-third of cellular subscriptions in the U.S. last year were in vehicles, he noted.

"The challenge, of course, is in a moving car, keeping it connected," Patterson said. "Occupants of autonomous vehicles will expect continuous connectivity. Whether the car is driven or driverless, I don't think it changes the IoT perspective. Occupants will expect to be connected."

Architectural complexity

Advanced automotive electronics present hardware integration challenges, while the necessary software will take in artificial intelligence, deep learning, and **neural networking (http://semiengineering.com/kc/knowledge_center.php?kcid=261)** technology. "Part of it is vehicle architecture, as well," said Patterson, adding that autonomous vehicles will need hypervisors and multi-domain support for silicon.

ARM TrustZone security technology can be implemented in silicon as part of the process. "Safety and security are paramount," he said. "If vehicles fail, people can lose their lives. Consumers have a high expectation that vehicles will remain safe and secure, as well as being part of the IoT. Carmakers scratch their heads on getting that balance right. So, introducing enough innovation to satisfy their customers, but don't compromise safety and security."

Mentor Graphics last month rolled out the Mentor Safe ISO 26262 qualification program, taking in its Nucleus SafetyCert real-time operating system, the Volcano VSTAR AUTOSAR operating system and BSW stack, and **ISO 26262 (http://semiengineering.com/kc/technology.php?tid=31076)**-certified documentation and qualification reports for Mentor system-

on-a-chip design tools.

"As vehicles grow increasingly sophisticated, functional safety has become an essential market requirement for electronics software and hardware design technologies," said Brian Derrick, vice president and general manager at Mentor Graphics. "We established the Mentor Safe program to help our customers rapidly navigate the increasingly complex process of functional safety certification with confidence, allowing them to spend more time creating value-added solutions that help to differentiate and win in highly competitive markets."

Patterson also sees a place for 5G wireless networks in the cars of the future. "Cars will be able to leverage that, of course, and become better connected than they would be on a 4G network. 5G will offer higher bandwidth, better coverage, lower latency for that safety-critical communication. As 5G gets rolled out, it just gets better in terms of connectivity."

The connected driver

Robert Schweiger, director of product marketing for Automotive Solutions at **Cadence Design Systems (http://semiengineering.com/kc/entity.php?eid=22032)**, says at the center of the connected car is the connected driver. "Connection could mean many things," he notes. "The latest connection we can see now coming on line is vehicle-to-vehicle and vehicle-to-infrastructure connection, and that actually the relation of the two to IoT, besides the automotive connection, so you can take more advantage of the cloud."

He continues about the connected driver, "There are lots of connections in the car so that you have the best experience, to get all this information into the car, to enhance your driving experience."

A Cadence customer is using Tensilica digital signal processor intellectual property to design a chip using the IEEE 802.11p standard for V2V communication. Schweiger declined to identify the customer, describing the company as "a large OEM in North America."

He adds, "This could be used for the infrastructure once the infrastructure is ready to talk."

Automotive electronics are advancing to the point where many applications call for more than microcontrollers, according to Schweiger. Camera-based vision, LIDAR, and radar are being implemented, and they need to be used in combination, since each technology has its own faults or shortcomings. "Radar can't read traffic signs," he comments, which can be addressed with vision.

LIDAR can be highly accurate, yet the technology remains very costly at present. "Radar is much cheaper, and it's a mature technology," Schweiger says. "The disadvantage is the accuracy."

Convolutional neural networks bring together these technologies, he adds. "Each system has a disadvantage," he says. "Only the combination of all these sensors will actually provide the required robustness of the system to reliably detect objects correctly."

In advanced driver-assistance systems, "there's lots of development going on because it looks like it is the kind of prestigious race that is going on with OEMs," Schweiger says. "Everybody tries to be the first to release a truly automated car in production."

The "megatrend dilemma" in automotive electronics is meeting government regulations to limit vehicle emissions while implementing power-hungry ADAS in cars, he notes. "The only way to solve this puzzle is really to have a much higher integration leveraging the latest low-power process technologies that are available and try to pass on those chips with only one function running, but multiple functions running in a very contained power envelope."

Where IoT enters into the equation is providing real-time information based on sensor data. "The car needs to instantly react in all kinds of circumstances," he adds.

Conclusions

There are plenty of good ideas about what will work best in a car, how to secure them, and what to do with all of the data that is collected. It remains to be seen, though, whether these ideas keep up with the technology rollouts and the evolving expertise of hackers.

Nevertheless, opportunities for fixing these problems, as well as new ones that come along should keep a large portion of the technology industry busy for years to come. Whether a car is an IoT device or a system that is connected to the IoT is an interesting debate, but the real issue is whether an autonomous or connected vehicle can deliver its passengers to their destination reliably and safely. So far, there is very little data from which to draw a conclusion.

Related Stories

What Can Go Wrong In Automotive (Part 3) (http://semiengineering.com/what-can-go-wrong-in-automotive-3/)

Why power has become so important in car electronics; the challenges in making autonomous vehicles reliable enough; adding margin for safe modes of operation.

Prioritizing Vehicle Data Traffic (http://semiengineering.com/prioritizing-vehicle-data-traffic/)

Challenges grow for classifying and tagging huge volumes of data from connected cars.

Car Becomes A Living Platform (http://semiengineering.com/car-becomes-a-living-platform/)

An entirely new view of all aspects of a vehicle is essential to design moving forward.

TAGS: 4G (HTTP://SEMIENGINEERING.COM/TAG/4G/) 5G (HTTP://SEMIENGINEERING.COM/TAG/5G/) ADAS (HTTP://SEMIENGINEERING.COM/TAG/ADAS/) ARM (HTTP://SEMIENGINEERING.COM/TAG/ARM/) AUTONOMOUS VEHICLES (HTTP://SEMIENGINEERING.COM/TAG/AUTONOMOUS-VEHICLES/) AUTOSAR (HTTP://SEMIENGINEERING.COM/TAG/AUTOSAR/) CADENCE DESIGN SYSTEMS (HTTP://SEMIENGINEERING.COM/TAG/CADENCE-DESIGN-SYSTEMS/) ECU SOC (HTTP://SEMIENGINEERING.COM/TAG/ECU-SOC/) IEEE 802.11P (HTTP://SEMIENGINEERING.COM/TAG/IEEE-802-11P/) IOT (HTTP://SEMIENGINEERING.COM/TAG/IOT/) ISO 26262 (HTTP://SEMIENGINEERING.COM/TAG/ISO-26262/) LIDAR (HTTP://SEMIENGINEERING.COM/TAG/LIDAR/) MENTOR GRAPHICS (HTTP://SEMIENGINEERING.COM/TAG/MENTOR-GRAPHICS/) RADAR (HTTP://SEMIENGINEERING.COM/TAG/RADAR/) RAMBUS (HTTP://SEMIENGINEERING.COM/TAG/RAMBUS/) SECURITY (HTTP://SEMIENGINEERING.COM/TAG/SECURITY/) SYNOPSYS (HTTP://SEMIENGINEERING.COM/TAG/SYNOPSYS/) TENSILICA (HTTP://SEMIENGINEERING.COM/TAG/TENSILICA/) TRUSTZONE (HTTP://SEMIENGINEERING.COM/TAG/TRUSTZONE/) V2I (HTTP://SEMIENGINEERING.COM/TAG/V2I/) V2V (HTTP://SEMIENGINEERING.COM/TAG/V2V/) VELODYNE LABS (HTTP://SEMIENGINEERING.COM/TAG/VELODYNE-LABS/) VISION (HTTP://SEMIENGINEERING.COM/TAG/VISION/)

Jeff Dorsch **(all posts) (http://semiengineering.com/author/jeff-dorsch/)**

Jeff Dorsch is a technology editor at Semiconductor Engineering.