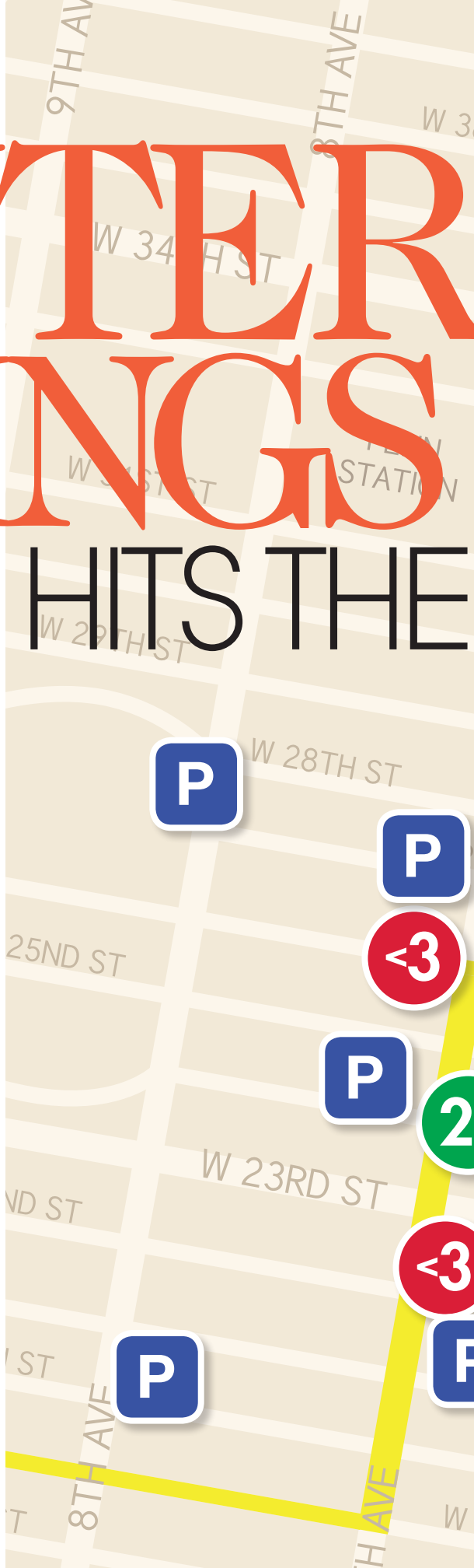
DON TUITE | Analog/Power Editor
don.tuite@penton.com

THE INTERNET OF THINGS HITS THE

Making vehicles part of the Internet of Things opens new design possibilities.



Imagine you're getting into your car and you want to continue a hands-free conference call with people at work. Your kids in the backseat are engaged with their Facebook accounts, watching videos, or gaming online. And, you're in a rush to get to where you really need to be.

Before the Internet of Things (IoT) can support these demands, automotive systems need to allocate bandwidth between high priorities like conference calls and low priorities like Facebook. Security is another issue, especially for communications that affect driving safety. As a result, design opportunities abound *(Fig. 1)*.

BREAKING IT DOWN

Reliability is a key factor. Automotive IoT systems must provide non-stop connectivity based on the strength of their current connection and the potential strength of alternatives. If a user is connected to service provider A and the strength of that connection starts to degrade, the hardware must be able to detect the degradation and switch to provider B well before the link fails.

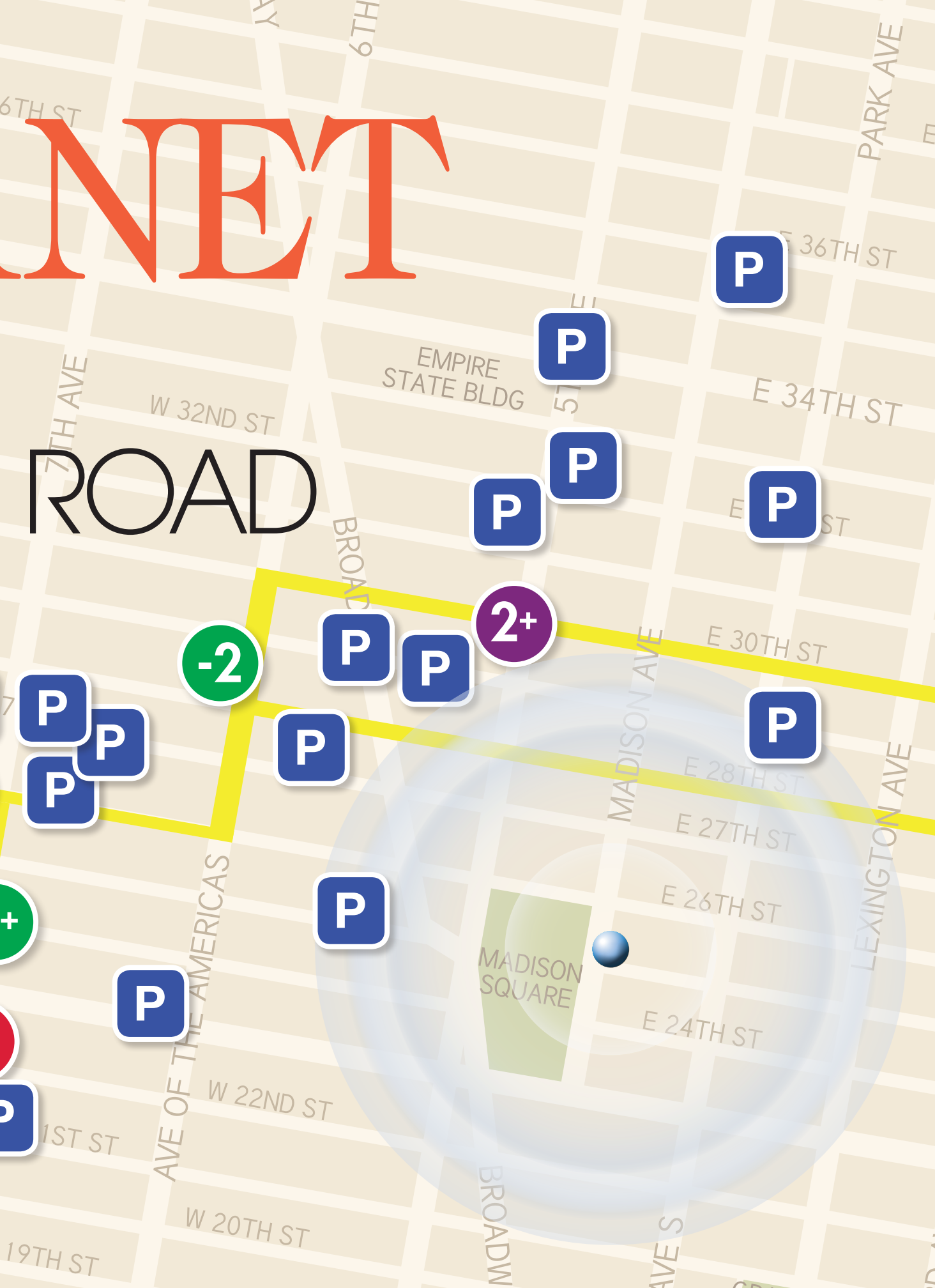
The hardware and software should be able to transparently transition the vehicle's primary connectivity and transfer the link forward to the optimum adjacent cellular provider. In the evolving world of Internet adaptation, though, cellular-to-cellular is only one kind of possible transition. Cellular-to-Wi-Fi is another.

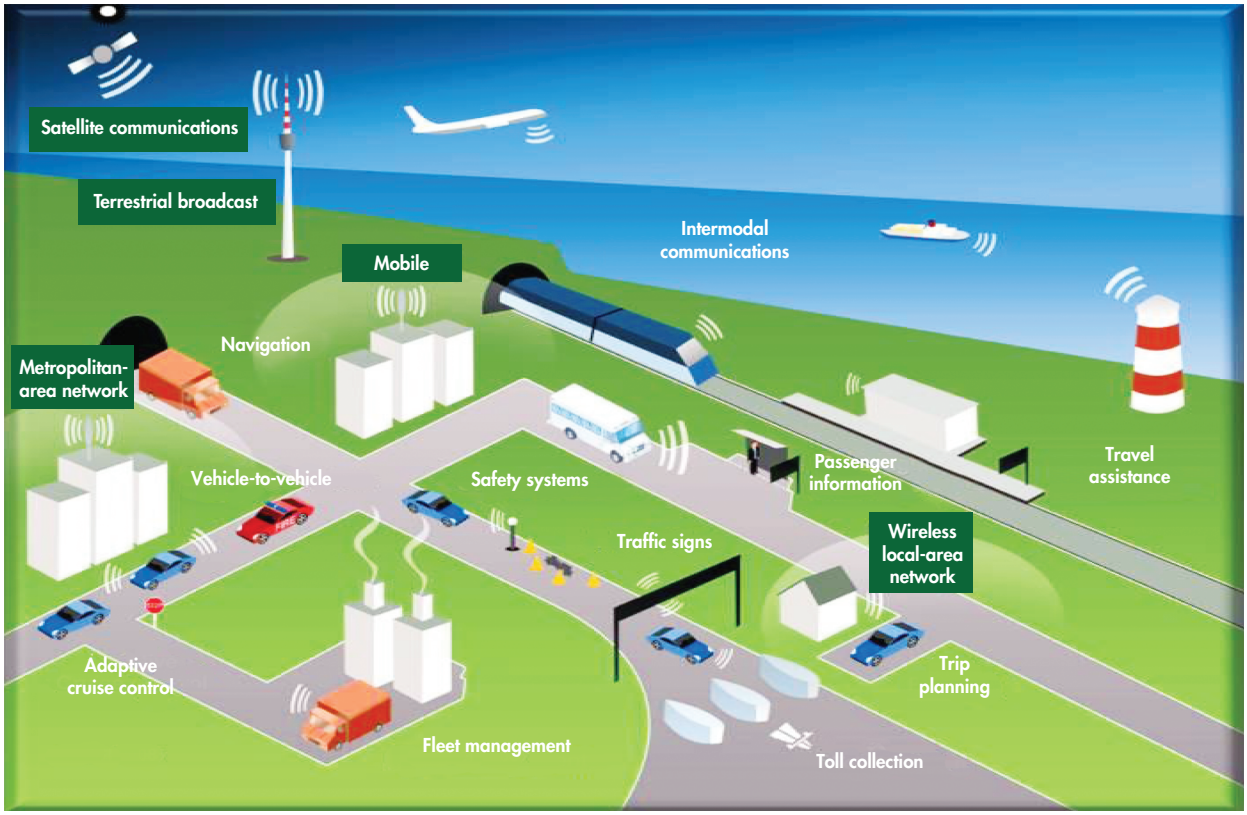
"New mesh Wi-Fi networks that are being created present a huge opportunity to reduce costs to the user," said Mala Devlin, business operations manager of connected industries at Cisco. Best known for Internet routers and switchers, Cisco is staking out vast amounts of territory at the interface between the IoT and transportation.

Dedicated Short-Range Communications (DSRC), defined by IEEE 802.11p, is yet another option. At its roots, DSRC is still Wi-Fi, but some hardware improvements can make it robust. DSRC involves vehicle-to-

NET

ROAD


6TH ST
PARK AVE
E 36TH ST
EMPIRE STATE BLDG
E 34TH ST
W 32ND ST
7TH AVE
BROAD
E 30TH ST
MADISON AVE
E 28TH ST
E 27TH ST
E 26TH ST
LEXINGTON AVE
MADISON SQUARE
E 24TH ST
AVE OF THE AMERICAS
W 22ND ST
1ST ST
W 20TH ST
19TH ST
P
2+
-2



1. For Cisco, a vehicle is just one more thing in the Internet of Things. The key engineering challenges lie in optimizing communications for speed, security, and reliability.

vehicle and vehicle-to-infrastructure communications, helping to protect the safety of the traveling public. It can warn drivers of an impending dangerous condition or event in time to take corrective or evasive actions. The band is also eligible for use by non-public safety entities for commercial or private operations. It operates at 5.9 GHz.

"Moving beyond connectivity issues, security may emerge as the most critical piece of the puzzle," Devlin said. She explained that at Cisco, "Security products and solutions range from VPNs (virtual private networks) to threat defense, to Web filtering, to identity management, and so on." Existing technology could be brought into the vehicular domain in many applications, though it would be necessary to customize it because of differences in scale, footprint, and CPUs, she said.

BUSINESS PATHS

So where are the business opportunities? Cisco is pursuing many possibilities for what could be a common platform with multiple extensions. The key features are high connectivity and speed. Security is important, but it isn't the biggest priority for some people that Cisco works with, Devlin said. Service providers that want to have an aftermarket play represent another business opportunity.

In general, developers for hardware that adds IoT capabilities to vehicles need to look at the situation as a need for a generic platform. "Yes, connectivity is important. But really what we need is an open platform that allows us to securely authenticate and add new applications through which OEMs can monetize various services," Devlin said.

"Looking beyond the feature-level layer, it helps to know what your partners are thinking about in terms of operating systems and silicon. When we work with tier-ones or auto manufacturers… there is a variety of issues that we look at. One is operating systems—what's popular now, what's going to change," she said.

"For example, QNX is fairly widespread today but declining because of its association with RIM," she said. Nevertheless, she added, QNX does have a pronounced market share in the automotive world, so it isn't doomed. However, Linux and Android are increasing in popularity. Similarly, ARM is becoming the predominant CPU architecture because of its low-power requirements.

"When you're building the software stack, you typically start with decisions on which CPU architecture you're going to go with. What's the kernel that you want to have? Then, what are the basic capabilities that are needed?" she said.

"Then on top of that, what level of scalability, reliability, and extensibility must the platform provide? As an engineer, that's how I always work. If I look at a spectrum of requirements, I imagine a Venn diagram to see what it takes to build in as much commonality as possible."

For example, accounting for the broad constraints for a product that will allow intelligent, autonomous switching connectivity options such as multiple cellular services and mesh Wi-Fi, a team could design the part of a system that can opt for the best connection solution at any time, based on cost, reliability, and security. Devlin calls that hardware a "policy engine."

Cisco already knows how to do that in the wired Internet. "This involves hardwired decisions. Under these circumstances, you shall switch between these links," she said, along with the ability to learn from what has happened in the past, being able to collect patterns of experiences that point the policy engine toward the advantages of certain kinds of links.

"For example, if you're commuting on the 880 at 8 a.m., and you need to be at work at the Cisco campus at 9, the particular connectivity that you'd use during that time frame might be different than if you were going someplace else at midday," Devlin said.

"What else is needed is the ability to learn, not just from one car's experience but from the experience of a multitude of cars, and to be able to harness that vehicular crowd source by monitoring and accumulating data on what's happening to other vehicles and applying predictive analytics to a spectrum of situations," she said. "That's more than just creating a logic tree based on time of day and location."

In other words, the experience that strangers are having in their cars a mile up the road can affect communications decisions in your car. That's a whole new sense of community. "It's really crowd sourcing at a different level. We've all been frustrated on the road when we suddenly hit a traffic jam and think, 'Gee, I wish I'd known five minutes earlier. I would've passed up the last exit and gone a different way,'" Devlin said.

"This is knowledge-sharing without human intervention. You don't have to tweet or text that 'Hey, I am stopping, and blah, blah, blah.' Instead, every car senses that traffic has slowed down (or sped up) for them, and in effect, tweets the information by means of DSRC, not to you, not to other drivers, but to other cars," she said. "But it will alert you too so you have control. It's through these protocols that I spoke about, such as DSRC vehicle-to-vehicle communication, vehicle-to-infrastructure communication."

This type of information, coupled with in-car mapping intelligence, can do more than simply let drivers know about backups so they can initiate their own alternative routings. It also can automatically access traffic information on all those alternatives and direct cars to different routes to spread the traffic load and improve travel times for every vehicle.

BYOD IN THE CAR

To the horror of corporate IT managers, "bring your own device" (BYOD) is making its way into North American and European businesses. Essentially, technology workers tend to upgrade to newer and more feature-rich gear faster than companies can afford to match. The newest gear is compact and inconspicuous, and inevitably company resources are exposed to the BYODs, which can potentially carry away trade secrets and infect resources. (Think USB drives, Stuxnet, and Iranian uranium-separation centrifuges.)

Since it's naïve to think that company policies can effectively interdict BYODs, the sensible thing to do has been to build security into the company's internal net. Cisco already offers such security products. Now, extend that protection to airliners, commuter trains, company shuttle buses, and carpool vehicles. That's where security becomes a matter of life and death.

What's at risk is no longer limited to companies' trade secrets and financials. BYOD-introduced malware can turn the tables on DSRC traffic control, increasing driving danger and sabotaging vehicular systems in ways one doesn't want to think about. And at a lower level of paranoia, there are more issues for a protocol engine to contend with.

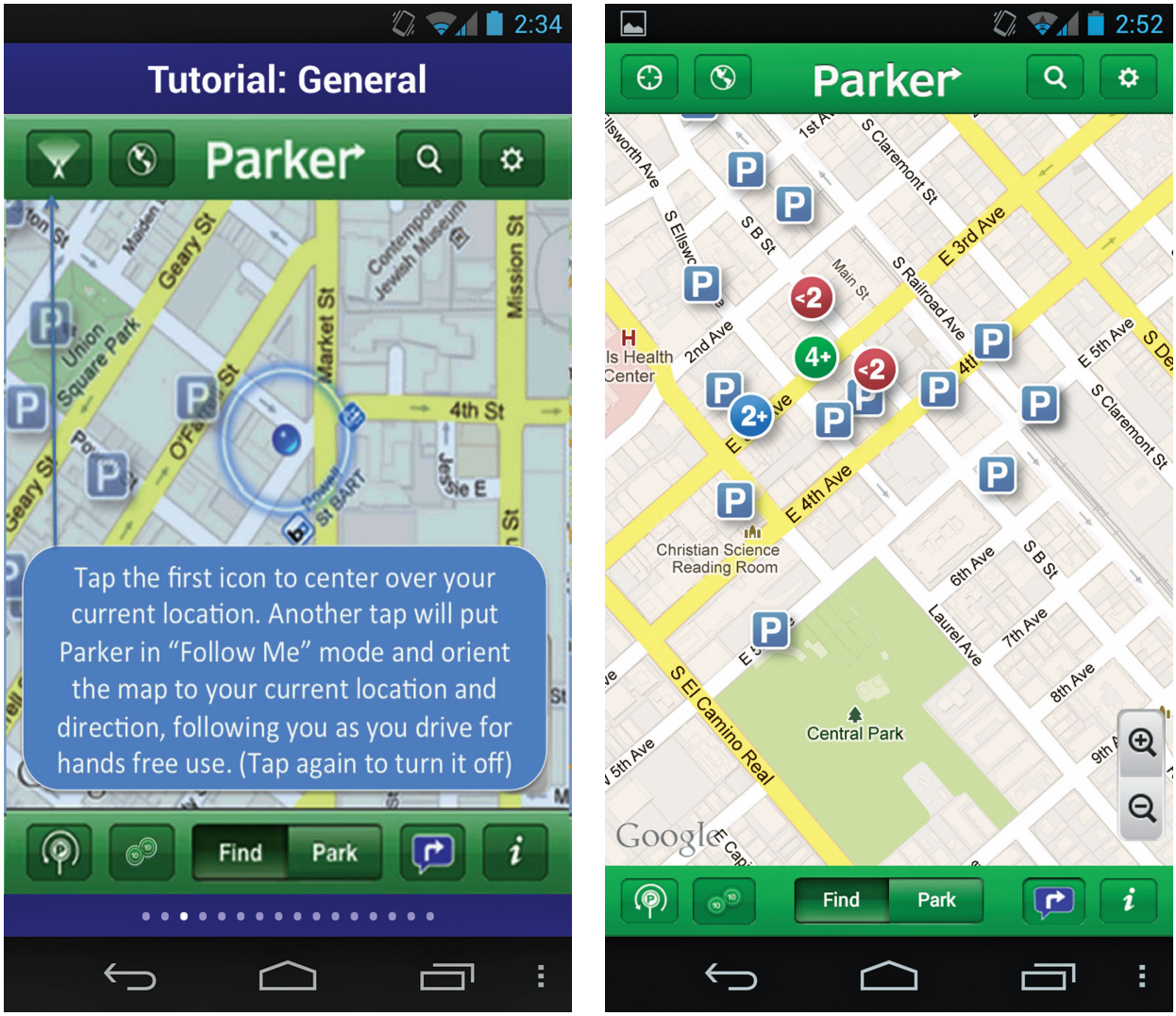
Examples extend from the stranger one picks up at the park-and-ride to make up a carpool to regular carpool members and to the kids going to the museum on the school trip or heading back from the soccer game. In such cases, the driver wants to give passengers who have their own devices controlled access to the vehicle's connectivity.

That means "identity management" for everyone in the vehicle. Guests in the car wouldn't necessarily have access to the same kind of information or the same level of bandwidth as the driver. Or perhaps if the driver is a real-estate agent showing a client an expensive new home, the system needs to be able to say, "This new device belongs to a red-carpet guest. Provide all-out service."

These decisions shouldn't necessarily be made in the car. This part of system design ties into security and policy management. It's a complex interchange of policy handshaking that ideally needs to happen in the cloud whenever the in-car system detects new devices, allowing a more sophisticated approach to providing access.

Taking that a step further, if the new device wants access to parts of the system that are vulnerable to malware, the in-car gateway could direct it first to a malware-cleaning site. That would never be a total solution, but it would provide a level of security. "That kind of thing is possible once you're able to have that end-to-end security, coupled with the ability to manage even the vehicle's ECUs (electronic control units) from the cloud," Devlin said.

OEMs are very interested in over-the-air updates to their ECUs. It's an economics and liability issue. Automotive OEMs



2. Streetline is working with many cities to demonstrate a mobile service that directs automobile drivers to open parking spaces (left). When drivers use the Parker app, a selection of open parking spaces appears on their phone (right).

in particular don't want ECU updates to be a cause for a major vehicle recall, nor do they want to rely on car owners to make appointments to have the work done at a dealer. "It's the ability to 'securely' provide that update to a unit and let it subsequently propagate to sub-tending ECUs that constitutes a huge money saver for OEMs," Devlin said. "But it has to be secure. It has to be reliable. It has to be scalable."

And if the data transfer drops for some reason before the update is complete despite all of its speed, security, and reliability, the system must be able to pick up where it left off once it reconnects. Inevitably, however, there are privacy and control issues that are connected to providing the potential for so much connectivity.

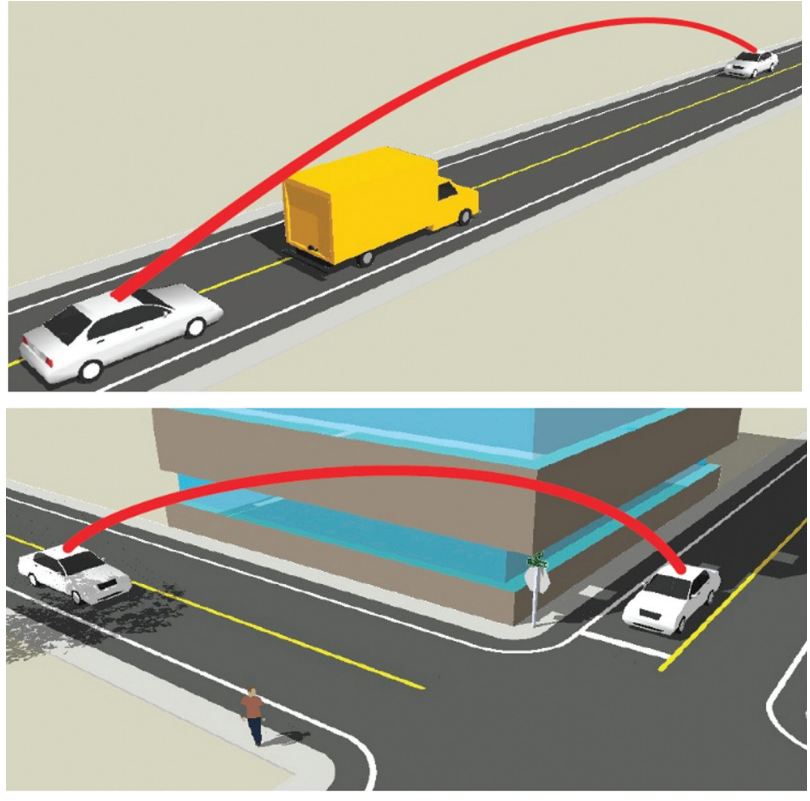
If your ECU can "phone home" for a factory update if its diagnostics indicate a flaw, can a built-in Breathalyzer call the cops (or less intrusively, a designated driver) if you are too drunk to drive? Could you limit the places your kids are allowed to go (known as geo-fencing) or demand a graphic display of speed and location when they come home?

UPGRADING AUTOMOTIVE BUSES

Looking ahead, each vehicle could support its own local network. Would an IP-based (Internet protocol) combination of RF and fiber replace some hardwired buses in the car? Would that be bulletproof enough? Cisco has been involved in a number of discussions on that front.

"There is a huge interest on the part of automotive manufacturers looking at this mesh that I like to think of as an instance of organic networking," Devlin said, though it isn't going to evolve in some predictable way.

"You are looking at a landscape that is being defined as we speak and there are multiple paths in which things can take shape. So we're actually placing bets on multiple fronts, through proof of concepts and experimenting with different ideas with different partners and customers," she said. "We don't have a definitive 'A is going to come before B before C,' but we do see A, B, C, D, E, F. We see the possibilities and we're placing bets among all those possibilities."



3. The Cohda Wireless DSRC (802.11p) radios employ patented techniques in the receiver to increase data throughput and extend range. This pays off in earlier warnings about road dangers about oncoming traffic just beyond that slow-moving semi you want to pass on a hill (top) or a speeding car just around the corner at a blind intersection (bottom).

SMART PARKING TECHNOLOGY

Your car is already part of the IoT if you park it around the intersection of 3rd Avenue and B Street in the business section of San Mateo, Calif., while shopping or dining. Something similar is true for 64 other cities, and the depth of coverage is growing.

Since last winter, San Mateo has been one of several sites for wireless sensor demonstrations in which drivers use their smart phones to find open parking spots. Another demonstration that allows drivers to find spaces in city lots is taking place in nearby San Carlos, Calif. The demos are a joint effort of Cisco and a company called Streetline. As the experiments feed back data to the cities, Streetline expects to increase penetration and turn the demos into revenue generators.

The technology uses buried sensors at each parking space—essentially, each parking space is an Internet "thing" with its own IP address—and a free consumer app called Parker from Streetline along with the intelligent networking technology platform from Cisco *(Fig. 2)*.

Sensors embedded in the pavement of the selected parking spaces detect when a space is available. Cisco's smart routers communicate with Streetline sensors to aggregate sensor data and, at the same time, communicate with the Streetline cloud center to deliver the availability of the parking spots. The intelligent network platform captures the data and publishes it into Parker, which displays real-time availability of these on-street spaces as well as locations of off-street parking garages and lots along with other information such as pricing and enforcement hours.

The Parker app's hands-free voice navigation system guides drivers to parking facilities using an audible cue when available parking is nearby. It also can toggle between availability and price, including real-time updates as prices are changed or updated. In fact, with the cooperation of the municipality, it's possible to access rates, hours, and time limits before leaving home.

Drivers can even tell the app where they want to go and be guided to the nearest open parking spaces. Friendliest of all, the app can guide drivers back to their cars after dinner or the show. The Parker app on my phone lists coverage in 65 cities. It runs on iOS and Android.

AUGMENTING AWARENESS

Cohda Wireless has investment and technical support from Cisco and NXP. Its hardware supports cooperative intelligent transport systems (CITS) that use vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications to enable cooperation between vehicles and road infrastructure to improve safety, mobility, and the environment.

Both the United States and Europe have released 5.9-GHz spectrum for CITS. Major trials are underway around the world. Foundation standards for CITS are the same in both the U.S. and Europe, and they have already been published. Cohda has a unique hardware solution for 802.11p receivers, which it says has advantages over radios from other CITS suppliers that rely on commercial off-the-shelf hardware.

Generally, CITS provides each vehicle with 360° awareness of all other vehicles on the road. If a threat is identified, the driver is immediately warned and can take steps to avoid an accident. Cohda Wireless says its technology extends this 360° awareness beyond buildings and around trucks that block the driver's view, enabling drivers to be aware of all threats, literally around corners.

The company has performed multiple demonstrations at transportation safety events. Typically, the trunks of two cars are fitted with identical DSRC demonstration systems, and antennas are mounted at the rear of the roof.

In the trunks of the demo cars, the Cohda Wireless radio interfaces with an STMicroelectronics STA2062 Cartesio Application processor for portable navigation, in-vehicle navigation, and telematics, which integrates a 32-bit ARM core with a 32-channel GPS subsystem and an array of ports for peripherals, including CAN, USB, and SPI.

The STMicroelectronics platform GPS receiver provides data about current location and time. This information is used to build SAE J2735 basic safety messages, which are then broadcast via the Cohda radio in one of the vehicles at a rate of 10 messages per second. The other Cohda radio receives those messages and forwards them to the processor, which extracts time-stamped positions. Combining knowledge of the local area and remote vehicles, the processor then geometrically assesses potential danger and issues warnings as appropriate.

At several international automotive shows, Cohda has conducted on-the-road comparisons between its products with the patented receiver modifications and competing hardware built using standard Wi-Fi chips. It says that by actual measurement in live conditions, Cohda devices can allow 10 to 15 times more data to be exchanged between vehicles and/or infrastructure and that the useful range is extended from around 20 meters to 200 meters.

Regardless of the type of transmitter in the DSRC radio in the other car, Cohda's system can provide a driver with a "do not pass" warning about oncoming traffic in the opposite lane when the closing time is on the order of 20 seconds, versus 3 seconds, if both radios use standard radios *(Fig. 3)*. When the potential collision involves a vehicle around a blind corner, rather than in a situation passing a big rig, warnings are available when there is still 6 seconds or more to react of time, compared to less than 2 seconds. ed

REFERENCE

1. Dedicated Short Range Communications (DSRC) Service, http://wireless.fcc.gov/services/index.htm?job=service_home&id=dedicated_src