Connected Cars: How to Accelerate Mainstream Adoption

Steve Tengler

Every so often, the media tells us about an automotive manufacturer on the cusp of delivering wireless, cooperative systems. The reader immediately thinks of *Knight Rider*, and wanders through a fantasy of connected car heaven.

However, this type of news is often miles from accurate; connected car offerings in the near-to-distant future are a different reality. This article examines the delays behind that “nearly done” automotive technology, and analyzes the value of our research dollars.

In 2005, several automakers introduced cooperative, wireless systems at the Intelligent Transportation Society World Congress in the parking lot of the San Francisco Giants’s then SBC Park. Messages were sent vehicle-to-vehicle and vehicle-to-infrastructure via dedicated short-range communications (DSRC) or, as it would later be renamed, “IEEE 802.11p (5.9 GHz).”

Most of the applications were safety-related systems that offered a seemingly futuristic understanding of position, speed and road conditions. But that was six long years ago – so, what has changed? Apart from the Giants stadium name-change, not much. Technology is no closer to the marketplace. Let’s explore why.

The “Co” in Cooperation

If you’ve heard the saying “the second mouse gets the cheese,” then you understand the fate of the first mouse — *snap*! Similarly, no company has succumbed to the lure of the first-to-market-cheese since each has foreseen the trap: producing a cooperative system with no cooperation.

Let’s imagine you are a leading automotive manufacturer that holds 20% of the U.S. market. That market is projected to reach 14 million vehicles in 2012. Considering there are over 250 million vehicles on the road, you could potentially communicate with 1.1% of the vehicles after just one year, assuming you installed the $200-$300 worth of equipment on all of your vehicles.

The first customer to purchase a wireless device creates the equivalent of a tree falling in an unoccupied forest. How satisfied will he or she be? If there’s no one else with whom to communicate, then not very satisfied at all. And how differentiating will that system be when all other automotive companies introduce systems that communicate the same information as your breakthrough device? Again, not at all. The moral to this story? In this case, being first has few rewards.

The Technology Hurdles

There are still four hiccups in the technology that, surprisingly, don’t make it to the media all that often.

- **Security**: If someone hacks into the system, there needs to be a means of crime identification and removal (e.g. law enforcement, disabling hardware, ignoring false broadcasts, etc.). Otherwise, Joe Hacker could ease his commute by diverting traffic or creating city-wide chaos. However, this level of security management requires a backhaul system to a centralized certificate authority (someone who manages the system). At one point, the government considered making this a series of installed roadside or intersection locations, but that was too expensive and fraught with state-to-state complications. The individual OEMs could seek an embedded or accommodated cellular connection (e.g. OnStar or SYNC), but those require cuts in penetration, depending on the actions of the customer, who could cancel his OnStar subscription, forget to connect, or turn on a Bluetooth cellphone. So, right now there’s no easy one-size-fits-all solution to security.
- **Positioning**: Any semi-autonomous system currently provides lane positioning by white-line monitoring (i.e. lane markers), but according to AASHTO, the likelihood of a lane departure fatality is twice as high in rural areas, where lane markings are less common and also tend to have inferior lighting and snow removal. To overcome that challenge, the vehicle must have highly accurate, autonomous positioning. This can only be achieved with one of several expensive solutions.
- **Packet Collisions**: Imagine being on the floor of the stock market — lots of people screaming, no one can effectively hear everyone all at once. During the initial phases of cooperative research on platooning done by the automotive manufacturers, this is exactly what the investigations determined. In congested multi-lane highway situations, each vehicle would be trying to broadcast its location, but no one would be able to “hear” it. Therefore, platooning would not be successfully (or safely) achieved.
- **Intelligence**: As artfully described by Hotchkiss in “Understanding the Human Part of the User Experience,” we humans are unbelievably adept decision-makers. Replacing us for even simple, predictable tasks like chess has taken decades and serious processing power. Driving is a complex task that requires thousands of decisions and reactions every mile. Implementing humans’ complex, dynamic decisions and observations to create an

autonomous system is an enormous task.

The Business Case

How does the automotive manufacturer make a profit on these cooperative, non-differentiating systems? How can an automotive manufacturer easily charge for the hardware? If infrastructure must be supplied, how is it governed?

The question of collective business was mentioned by The National Highway Traffic Safety Administration (NHTSA) at the 2011 Transportation Research Board's annual meeting, despite nearly a decade of investigations into cooperative technology. Until a means of making money is clearly delineated, no companies will be lining up to platoon, regardless of the societal benefits.

The solution occasionally proposed is that Wi-Fi could provide the accident avoidance systems, along with non-safety Internet connectivity at intersections. This plan is fraught with technological issues (the latency to join the intersection group — known as association timing — is too great) as well as business issues. Who pays to install Wi-Fi at millions of intersections? If the government gets that bill, how does it avoid competing with the private sector? Regardless of public or private, how does today's car count on the infrastructure 10 years from today? Who co-pays for maintenance? Maybe Google will provide free Wi-Fi, or maybe it will fizzle like some of the company's other beta releases.

Some Potential Solutions

Now, we're not expecting a *Jetsons*-type car, but a few key companies could help realize basic wireless functionality. The solutions, though, require the following strategic elements.

- **Creative User Experience**: To differentiate from the cooperative systems competition, the user experience (UX) must be unique in some fashion. For safety systems such as intersection collision avoidance and platooning, it is actually undesirable to have non-standard interfaces, since a common warning is more likely to elicit a common reaction. To differentiate, the OEM must create non-safety applications with unique UXs that provide value using the same technology. Be it a local chat room, an automated license plate game, or a quasi-classified information exchange, the human-machine

interface that provides the unique customer experience in a safe manner will justify or subsidize the costs.

- **Sleeping with the Enemy**: Entering the market via only one OEM is insufficient, but co-launching the system with one or two other vehicle manufacturers could easily result in 50-60% market penetration. This would require a coordinated launch, which is difficult enough with one OEM across multiple vehicle platforms, but is especially challenging between competitors. As crazy as it sounds, GM and Toyota have already discussed the opportunity, but reportedly struck no deal for co-distribution. Some OEMs are awaiting a mandate from the U.S. government that requires companies to install DSRC equipment, but that's the best way to arrive last to the party with little to no differentiation.
- **The Alpha and the Omega**: To launch the system, the vehicle and the infrastructure must exist first. The only ways for an automaker to ensure this is to either use something existing or provide the enabler on its own. Be it an embedded cellular system (e.g. Lexus Enform, GM OnStar) or an integration solution (e.g. Ford SYNC), the backhaul must attach to a privately-run security system. Otherwise, the design is fraught with risks that no manufacturer will accept, unless mandated by the U.S. Department of Transportation. If embedded, though, the UX must provide a flexible interface that will allow additional safety and non-safety applications to be added and removed as risks are determined.
- **Customer Reaction**: Research notes that 57% of people consider themselves better than average drivers. Human behavior studies have proven that people are only willing to trust an autonomous system in hazardous situations if it is familiar, and has a proven history of reliability. To launch anything successfully requires a commitment to marketing and usability demonstrations so that the public becomes comfortable with the new features.

Last, but not least, I want to leave you — the reader, the taxpayer, the automotive buyer — with this thought: Consider a technology investment no different than any other investment: value vs. cost. The government believes wireless systems could address 81% of all light-vehicle target crashes, but that's on paper, with no mitigating circumstances. What's the real number?

As for the cost, various government programs, like IntelliDrive, have spent over $100 million. A study by the Vehicle-Infrastructure Integration (VII) program estimates a piece cost of $50 per vehicle, with infrastructure deployment costs of $3.2 billion, and operating costs of just under $200 million per year. What is the acceptable prevention-to-investment ratio? Does money matter when it's *your* spouse or child saved? Will the slick UX of non-safety apps offset that cost? Whatever your thoughts, these decisions are being made nationally. Try to understand the reality of the situation before the industry takes off.

www.mashable.com [1]

Posted by Janine E. Mooney, Editor

February 9, 2012

Links:
[1] http://www.mashable.com