U.S Senate Committee on Commerce, Science and Transportation

The Road Ahead: Advanced Vehicle Technology and Its Implications

Expert Testimony by

Peter F. Sweatman
University of Michigan Transportation Research Institute

Wednesday May 15, 2013

Good afternoon, Mr. Chairman, Ranking Member, and members of the Committee. I am honored to speak with you about key steps for creating a much safer and more efficient roadway transportation system through new and emerging vehicle technologies. My perspective is research, development and deployment, and how to maximize the benefits of new technologies for the citizens and economy of the United States, with world-wide application.

I shall talk about the most promising technological advances with the broadest scope for application, under the shortest time frames. My commentary will include current vehicle technologies and trends as well as the more transformational technologies on the horizon. I shall also talk about how we need to get the job done through coordinated technology development, purposeful deployment, and strong policy guidance. We have entered a transformational period, and need to plan for new technologies and their likely implications for public policy.

Our journey with advanced vehicle technology began when attention moved from systems that protect people involved in crashes to systems that help prevent crashes in the first place.

Such avoidance systems currently alert drivers and are beginning to assist drivers by indicating the appropriate avoidance action. But ultimately the driver is still totally responsible for taking action to avoid the crash. We need more incentives and standards for the performance of such systems, as well as independent data that quantifies the effectiveness of these “safety content” features already being used in the U.S. vehicle fleet.

At the same time as these very positive advances in vehicle safety content are being realized, we are seeing an even stronger move to infotainment and telematics in vehicles, particularly the ability to connect and use personal devices in vehicles. For example, we are seeing a mature level of usage of navigation and traffic information systems, and such systems are migrating from those installed by original equipment manufacturers to those available in smartphones. Telematics services also include personal communication (often with voice command), emergency assistance, and even smart insurance and energy management. Such services connect the vehicle with the cloud, increasing the range and power of available information being channeled to the vehicle.

We are seeing unprecedented attention to the human-machine interface in vehicles, in order to deal safely with the increased flow of information to the driver, and to minimize distraction. Increasingly, such interfaces may be customized by automakers, providing them with some control over the presentation of content entering the vehicle via personal devices, but not the content itself. Responsibility for the safety of these in-vehicle transactions with the driver is an interesting question. Because a range of manufacturers and service providers combine to produce telematics, a "chain of responsibility" approach is needed for safety.

While good design of physical interfaces can minimize distraction, distraction is primarily a human issue that extends beyond vehicle technology. The ultimate solution to distraction is to completely replace human control with elements of automation, although this will not happen for many more years. In the meantime, responsible design is essential. Responsible design includes smart interfaces that can limit access and interfaces that maintain eyes on the road and hands on the wheel.

As we move forward, the technology will increasingly draw attention to risky driving scenarios as they develop. This will apply whether we are talking about the manual driving of today or the automated driving of the future, where the driver will still need to take over in limited situations. There is no better technology for purposefully identifying risky driving scenarios than 5.9 GHz Dedicated Short Range Communication (DSRC) connected vehicles.

The University of Michigan Transportation Research Institute (UMTRI) is currently overseeing a model deployment of nearly 3,000 cars, trucks, transit buses, motorcycles and bicycles in Ann Arbor – these vehicles are equipped for standardized and licensed 5.9 GHz wireless communication enabling very promising crash avoidance systems. This work is sponsored by the U.S. DOT and is carried out in partnership with the automotive and intelligent transportation systems (ITS) industries, and their technology suppliers.

This connected vehicle technology has the potential to revolutionize our transportation system, by drawing drivers' attention to risks more immediately and reliably, providing protection in cases when driver attention is deficient, and giving drivers more time to react. Pervasively, this will help us all to avoid crashes and to utilize roadways and energy sources much more efficiently. **I know of no other technology that could have the same impact on safety, and potentially in a reasonably short time frame.**

And this technology will undoubtedly have very positive impacts on mobility, energy use, and environmental aspects of our transportation system, all of which will provide significant economic benefit to the United States. Our transportation system will not remain internationally competitive without it.

A golden era of automotive safety is within reach. The focus must be deploy the connected vehicle technology, while ensuring that it is reliable and secure, and bring about a rapid uptake by automotive consumers.

We need to fully utilize and deploy Dedicated Short Range Communication (DSRC) at 5.9 GHz for all classes of vehicle and at key infrastructure locations (for example, intersections, interchanges and curves). DSRC is equally effective for – and must be applied to – all modes of roadway transportation, and in fact all road users. A national ITS strategy is needed to guide the application of the 5.9 GHz platform to all vehicle classes and recommended infrastructure locations, benefiting all road users. Testing also needs to be done to understand how this spectrum can serve to protect vulnerable road users, including pedestrians and bicyclists. Furthermore, this is a technological advancement that is being realized and explored by vehicle manufacturers and governments around the world because of its great promise.

The current V2X platform, which has been developed mainly through vehicle-to-vehicle (V2V) R&D, needs to be deployed taking advantage of vehicle-to-infrastructure (V2I) connectivity. Infrastructure is a critical component of connected transportation. Consider the important category of roadway intersection safety. Intersection crash risks are more effectively recognized by combining the “fixed” viewpoint of the intersection with the “dynamic” viewpoint of the moving vehicle. We need a national strategy for vehicle-to-infrastructure communications.

The effectiveness of V2X relies on the shared use of data between vehicles, infrastructure, and devices. But inherently there is risk for any one manufacturer when the safety of their product is partially dependent on another manufacturers product. There will be a wariness to introduce these technologies in the United States due to our litigious climate. Other countries may very well benefit first from the technologies developed here. Because of this, it will be necessary to consider shared-liability regimes, including limiting the liability of automakers and other device makers.

The 5.9 GHz spectrum itself must be managed in such a way that V2V and V2I applications continue to function with full effectiveness, reliability and security, regardless of the burgeoning demand for spectrum for unlicensed uses. Safety trumps convenience. Sufficient bandwidth must be protected for exclusive use by vehicle and infrastructure, to ensure safe and secure communication. Any competing uses need to be sufficiently defined, and testing must be carried out to ensure that safety functionality is not diminished or impaired by any shared bands adjacent to the exclusive safety and security bands. Reliable and secure communication is non-negotiable.

The overall reliability of the V2X platform will depend critically on these exclusive 5.9 GHz bands, as well as the ability of the V2X platform to scale up to large numbers of vehicles in the vicinity. Further testing needs to be carried out to allow for the high traffic volumes and densities of the future, as well as longer-range DSRC deployments.

Nothing is more critical to the success of the V2X safety platform than cybersecurity. Further field testing of a new generation security system is needed to ensure that the platform remains secure, while maintaining the privacy of all users, under all conditions encountered in a full scale field test. And cybersecurity for vehicles in general is an area of growing awareness and concern, and a comprehensive strategy involving industry and government must be established and carried out.

In order to accelerate the uptake of the platform by automotive consumers, it is essential to provide infrastructure-based functionality that offers useful applications to users from day one. This needs to be part of the national ITS strategy. Equally importantly, attractive aftermarket devices, developed with the active support of the automotive manufacturers, are needed to expand access to safety and mobility benefits and increase the density of deployment of the platform. These devices will need to have the active support of automakers. Further field testing of aftermarket devices will also be needed.

Clearly, a further wave of technological development will occur in vehicle automation. Automated vehicles will develop partly from current experimental self-driving vehicles, and will also build upon a successfully-deployed connected vehicle and infrastructure platform. Automation will occur progressively and in stages of decoupling from the driver. Automation will also increasingly affect the layout and operation of the roadway infrastructure.

Automated vehicles will result from a convergence of current driver assistance technology, the connected vehicle and infrastructure platform, and self-driving vehicle technology, including advanced vehicle-based sensors. But automation will also be part of a larger transformation to a new 21st Century Mobility System. Other elements of this transformation are likely to include a new transportation service economy, multi-modal trips, shared vehicle use, alternative energy sources including electrification, data-intensive system management and more tailored vehicles built with new materials and manufacturing techniques.

The scale of the transformation is important. The United States has the opportunity to leap ahead in mobility technology supporting an improved way of life and new mobility industries. An industrial ecosystem will be created by the automotive and information technology industries and there will be many winners.

Our new mobility system will need to operate on, and make highly efficient use of, our existing roadway network. Automated cars will be capable of operating in narrower lanes, with much reduced headways, creating much more efficient use of roadway space. And they may park themselves without a driver.

As part of the need to reduce the cost of the infrastructure, the stresses placed on roadways and bridges by large freight trucks will need to be reduced substantially. A productive new system of less driver-intensive, modular, close-headway freight units will help lead the way in vehicle automation. Traffic system management will utilize extensive data generated through the connected vehicle and infrastructure platform.

The operation of the roadway infrastructure will change progressively as more automated vehicles are deployed and co-exist with conventional vehicles. Eventually, the usage of our infrastructure will change dramatically as cars and trucks are provided with more effective traffic lane configurations and conventional vehicles become the minority.

How do we prepare for, and sustain, this transformation?

The problems we have been working on are the right problems for the long haul. A critical requirement is for all vehicles, whether manual or automated, to be connected during a multi-decade transition. And connected vehicles provide the all-important connection with drivers. Connecting all elements of roadway transportation – vehicles, drivers and infrastructure – represents an historic step forward and a vital platform for innovation.

The need for **human-machine interface (HMI) technology** to focus the driver's attention is a core competency today, tomorrow and the day after. As we move forward, vigilant technology will draw attention to risky driving scenarios. And the driver will still need to take over in certain situations.

The United States must take the lead in **standards development** and decide where mandatory safety standards are needed and where open standards are needed for the nation's entrepreneurs.

Voluntary **performance standards** for vehicle safety systems are well advanced and need to be solidified for the connected vehicle platform, vehicle sensors and controls.

We need to start now with connected infrastructure. Changes in the operation of the **roadway infrastructure**, as more automated vehicles are deployed, will eventually be profound. These changes will be driven by timely and reliable operational data, driven by connected vehicle data sources. National policy positions are needed on **data ownership, access, and privacy**. Traffic system managers need guidance in order to exploit the extensive data generated through the connected vehicle and infrastructure platform.

What new risks do we face with a large-scale transformation of our ground transportation systems? The rewards are huge, but do bring new security risks.

We are on the threshold of a very large-scale transformation of our ground transportation systems. We are now moving towards a system that will achieve much more for our consumers and industries, and create a new mobility economy, with minimal safety and public health impacts, and sustainable energy use.

The huge rewards of the new mobility system will also entail new risks that must be dealt with. Automated, high-density movement at speed has the potential for large scale disruption and harm as a result of systems malfunction, cyberattack or human error. We will need to be willing to develop breakthrough capabilities in the testing and certification of automated systems, cybersecurity, and human machine interface design. Responsibility for safe operation will need to be shared by industrial partners in such a way that none bears an unreasonable level of liability.

National strategies, performance standards and testing requirements for the connected vehicle and infrastructure platform, vehicle sensors, levels of automation, and HMI will be required.

Attention in the form of policy or legislation will be needed to the assignment of responsibility for safe vehicle operation. This will transfer from the driver towards the vehicle manufacturer as levels of automation increase over time. The vehicle manufacturer will carry considerably more responsibility, under conditions of greater uncertainty, including shared data and decision making. It will be necessary to consider a "chain of responsibility" approach, to ensure that the risk is commensurate with the benefit for each party, and to limit the liability of several partners.

Cybersecurity is a new and difficult problem. It will be necessary for the government to convene thought leadership in transportation cybersecurity, develop a defined action plan, and lay out protocols for cybersecurity that address the required level of security, testing standards, updates, and responsibilities of all relevant parties.

In closing, I wish to emphasize that the mobility technologies of the future will emerge through a process built around connected vehicles and infrastructure. Successful new technologies, of national importance, must be accommodated by:

- **National testing, standards and certification for connected and automated vehicles;**
- **Progressive innovation within our infrastructure;**
- **Scientific solutions for engaging driver and machine;**
- **Limited transfer of responsibility for safety, from drivers to private companies; and**
- **A defined action plan and enduring set of protocols for transportation cybersecurity.**

I appreciate this opportunity very much and welcome your questions. Thank you for your attention.