2014 National Workshop on Transportation Cyber-Physical Systems
Selected Key Research Areas for Transportation CPS

Dave LeBlanc, André Weimerskirch, Jim Sayer
University of Michigan Transportation Research Institute

Transportation in the coming decades will be impacted by major trends, including:

- Toward highly connected and cyber-centered – not only within the transportation system, but also in interaction with other public and private institutions and their users
- Accelerating use of telematics in vehicles, with the need to provide cyber-security
- Increasingly sensitive to constraints of propulsion energy availability and emissions impacts,
- Increasingly influential on the safety, efficiency, and livability of ever-growing urban areas

There will be rapid growth in the demand for improvements in transportation performance and the pressure to respond will be both economic and social. The responses will be enabled by science and technology and collaboration between these fields. Motorized highway vehicles will continue to play a major role for the next half century, but the information content and the intelligence of both vehicle and infrastructure systems will expand dramatically in order to provide improved performance while *maintaining or increasing safety*. The intelligence is necessary to assist and/or replace the human driver and to provide system resilience.

Current developments in connected vehicles at UMTRI

UMTRI and its partners within the University of Michigan (UM) have been leaders in the system-level issues of vehicle safety technology and human-system interaction for decades. Currently UMTRI is hosting the largest-ever field study of connected vehicles using 5.9 GHz dedicated short-range communications. Over 2800 vehicles are currently in the field and each and every 10-Hz message broadcast from these vehicles is being loaded into a database. These messages include GPS data and other relevant information (especially signals relevant to crash avoidance). Over 30 roadside transceivers and receivers are also active in this study. This is the most recent field study but several previous UMTRI studies using vehicle-based driver assistance systems have been conducted as well. All told, these tests yield databases with over 2000 driving years of data, including over 140 driving years with continuous video, radar, GPS, and other information. These data allow rich explorations of driver behavior and performance, communication performance, vehicle-roadway interactions, and more.

UMTRI is also a major partner of the new UM Mobility Transformation Center (MTC), in partnership with the College of Engineering and other university units. The MTC involves university, private, and public investment in a broad effort to re-imagine transportation and help to stimulate key innovations toward that future. The MTC will provide an important platform and resource for transportation research, including cyber-physical systems, in part by a new test facility on 30 acres that will provide the ability to research and test connected and automated vehicles in a physical setting designed to provide a diverse set of roadway and roadside features that mimic common urban challenges to vehicle systems and vehicle-infrastructure systems.

Two research areas that are enablers for pushing transportation CPS forward are cyber-security and design and evaluation methods for reliable intelligent systems. These areas are discussed below in the context of highway vehicles although the underlying principles are often applicable to a wider domain.

Effective and efficient approaches to cyber-security and privacy

It is expected that by the date of this workshop the US Department of Transportation (USDOT) made an announcement whether it plans to seek a mandate for vehicle-to-vehicle (V2V) communications equipment to be included in all new build vehicles after a particular date. Cyber-security and privacy are major technological concerns on the way to deployment. This technology is foreseen as the first step to increasingly automated vehicles, and still research questions are open before actual deployment. In particular, the reliable detection and removal of misbehaving vehicles requires more research, and so does the determination of an optimized privacy mechanism in the vehicle against 3rd party (non-insider) attackers. It seems obvious that automotive cyber security concerns will become even more important with cars that will implement features of automated cars, such as control applications.

Parallel to this safety technology, consumers are increasingly demanding infotainment features in their cars that match home entertainment and smartphone technology. The combination of connected vehicles, complex vehicle electronics, and a variety of wireless interfaces leads to a heavily increased requirement for automotive cyber-security and privacy since such cars can be accessed remotely and hacked as every other connected computer system. The implications are manifold and the threat of compromised functional safety due to hacker attacks is a major concern. However, denial-of-service attacks (e.g. deactivating the engine), attacks for financial gain (e.g. modifying the mileage counter), and privacy violations (e.g. extracting the history of driven routes) also need to be considered.

It is unreasonable to believe that automotive software can be implemented without security weaknesses. In order to reliably separate wireless interfaces, infotainment applications, and functional safety components, a bullet proof firewall and intrusion detection system will be required in all future cars. One approach to be considered is based on separation of microcontrollers (or cores) to separate functions and the use of strict policies based on physical limitations or, if more flexibility is required, based on white lists that can only be updated using trustworthy mechanisms. It can be foreseen that with an increased level of vehicle communication (e.g. for V2V safety applications and automated cars), approaches addressing only in-vehicle cybersecurity will not be sufficient. Infrastructure support will be required to detect malicious nodes, to react to attacks (e.g. by warning of malicious cars), and to fix security weaknesses (e.g. by updating software over-the-air) without violating privacy rights. While security and privacy requirements for individual areas are available (e.g. EVITA for in-vehicle communication and CAMP VSC3 for V2V safety communications), a comprehensive list of such requirements including infrastructure and in-vehicle electronics has not been considered yet. Addressing the combination of systems in an integrated manner is a critical need, and this topic should be considered in developing a research agenda.

Improving reliability of automated vehicles

Future cyber-physical systems will make inferences from streams of real-time and historical data, and those decisions will impact lives and the performance of the overall CPS. This decision-making must become more reliable as automation and integration accelerates. As an example, most automated vehicle prototypes use a combination of real-time sensor data and databases to both "recognize" its current static environment and detect any deviations from the expected, as well as to sense other dynamic elements such as other vehicles, pedestrians, or changes in the environment. This assessment relies on models and heuristics to draw inferences, such as detecting a shift of lane marker position in a work zone by considering GPS and matching historic and real-time LIDAR data. Such intelligent approaches mark a major accomplishment in intelligent vehicles, however, the systems can be expected to encounter rare coincidences that had not been considered or tested, and negative performance consequences may result. To detect these rare cases, exhaustive testing is not sufficient – on the order of 10 billion miles are driven in the US per day and the number of circumstances is staggering. While exhaustive simulation can uncover gaps in code or algorithm holes, a critical and fundamental step in these systems is *drawing conclusions from the large and complex data streams that are based on remote sensors and/or empirical data sets*.

A common approach is to build a data library from challenging situations for playback during design, but the library is finite in size and diversity of circumstances. A new approach is to use selected events in this library as seed events that can be perturbed in simulation to produce a wider set of challenging circumstances. This requires inverting sensor data to determine the actual environment, adding perturbations (e.g., shifted lane lines), generating simulated sensor data, and then exposing the system to this simulated situation. Furthermore, UMTRI has recently used database techniques to speed up simulations of crash conflicts by almost two orders of magnitude when compared to procedural techniques. Combining the "seed event" approach with this faster simulation would provide a capability for addressing the challenge of reliability of the sensor processing of automated vehicles.

Authors

Dr. David LeBlanc is an Associate Research Scientist at UMTRI and Head of Engineering Systems at UMTRI He has published widely in vehicle dynamics and control, driver assistance system requirements and evaluation, and impacts of vehicle technology on driving performance in real-world conditions.

Dr. André Weimerskirch is joining UMTRI in January 2014 as an Associate Research Scientist. Before joining UMTRI, he cofounded the automotive cyber security company ESCRYPT (sold to Bosch in 2012. André is a main author of the V2V safety communications security protocol considered for deployment in the US and of the security concept in UMTRI-led Safety Pilot Model Deployment.

Dr. James Sayer is the head of Human Factors Systems at UMTRI. He is serving as the principal investigator of the Safety Pilot Model Deployment, is leading the development of the MTC test facility, and is pursuing advanced ITS demonstrations and deployments.