NSF Cyber-Physical Systems Workshop Position Paper

An Automated Highway System as the Platform for Defining Fault-Tolerant Automotive Architectures and Design Methods

Steven E. Shladover, Sc.D.
California PATH Program
Institute of Transportation Studies
University of California, Berkeley
(510) 665-3514
steve@path.berkeley.edu

Background

Automated highway systems (AHS) have intrigued both the public and the technical community since the 1930s, but they have yet to advance beyond the test track into public service. Research and development work has advanced in fits and starts, beginning with GM/RCA industrial research in the 1950s, then academic research at The Ohio State University in the 1970s, and the PATH and National Automated Highway Systems Consortium (NAHSC) research from 1988 to 1998. PATH and several other research groups have continued related research since 1998, but at a significantly lower level of effort and with less ambitious horizons.

When I refer to an automated highway system, I do not mean an "autonomous vehicle", but rather an integrated system of coordinated and cooperating, fully automated vehicles. The coordination and cooperation among vehicles and between vehicles and the roadway infrastructure provide faster, richer information to the vehicle control system than an autonomous vehicle's sensors can provide, and they enable the vehicles to negotiate maneuvers and inform each other about problems such as failures and environmental disturbances. Combining these cooperative capabilities with the isolation of the automated vehicles from non-automated vehicles by operating them on dedicated, protected highway lanes makes it possible for the AHS to provide public benefits that greatly exceed the benefits of autonomous vehicles in terms of highway capacity increases, congestion relief, energy and emissions savings and safety. The cooperation and protection also simplify the design of the automation system by reducing uncertainties, excluding many uncontrollable hazards, and facilitating the implementation of fault recovery strategies. The design of the AHS is by no means a simple problem, but it at least stands a reasonable chance of being solvable within the next few decades.

When the NAHSC program was terminated prematurely in 1998 there was widespread doubt about the technical and economic feasibility of many of the needed enabling technologies. In the thirteen years since then, automotive technology has advanced significantly. The advent of hybrid electric vehicles has accelerated the use of all-electronic actuation of vehicle control actions (engine, steering and braking) and collision warning and control assistance systems have accelerated the use of ranging sensors to detect nearby vehicles. A major national initiative on cooperative vehicle systems has supported the development of a DSRC wireless communication technology that meets all the needs of an AHS (and may even lead to a government mandate that it be installed on all new vehicles by the end of this decade to support collision avoidance systems).

Technical Challenges and Possible Solutions

Despite concerns about the large number of highway deaths and injuries, the road transportation system is already remarkably safe. In the U.S., the mean time between fatal crashes is about 2 million vehicle hours and the mean time between injury crashes is over 50,000 vehicle hours. For an automated vehicle or an AHS to be acceptable to our society, it will need to be proven substantially safer than the current system. This is no mean feat, when we consider that it is a consumer product that needs to be affordable to the general public, that needs to operate for the life of a motor vehicle (at least ten years) with a minimum of maintenance, and that is confronted with a highly stochastic operating environment, with hazards that need to be identified and mitigated in a fraction of a second. The extensive design redundancy and intensive preventive maintenance regimes that have made commercial aviation safe are not economically viable in the automotive sector. Furthermore, drivers are not highly trained professionals like airline pilots and hazardous situations must be dealt with much more quickly on the road than in the air because of the close proximity among vehicles.

Prior research and development work by PATH and others has already shown that most of the control system design problems for AHS operating under “normal” conditions are solved or readily solvable. Automatic steering, speed and vehicle spacing control have been demonstrated to be achievable with high accuracy and smooth ride quality, even at very short gaps, and complicated cooperative maneuvers have been implemented at test sites. The major remaining technical challenges are associated with detecting, identifying and managing the responses to internal vehicle system faults and adverse situations in the external driving environment. This is where the Cyber-Physical Systems initiative can have a major impact in accelerating progress toward AHS deployment.

We do not yet have efficient and systematic methods for verifying the completeness and correctness of the control and fault management systems for automated road vehicles, which will incorporate many software modules of varying provenance. The combinatorial explosion of possible software paths makes exhaustive enumeration infeasible, and brute-force testing of the complete system would require multiple millions of vehicle hours of test track exposure to be able to demonstrate achievement of the required MTBF values. Even deliberate fault-injection testing to accelerate exposure to hazardous conditions cannot efficiently replicate the full range of conditions that the eventual public fleet of millions of interacting vehicles will encounter.

Research is needed to support development of efficient methods for designing and proving software-intensive safety-critical systems like the AHS, where there is very little tolerance for failures (which can easily kill or injure innocent members of the general public). While the automated vehicles could be a highly visible testbed to capture public imagination and gain support for an ambitious research program, the fundamental knowledge could be applied in other domains as well, such as medical equipment (which has already suffered disastrous examples of deaths caused by software bugs).

Milestones for the next 5, 10 and 20 years

The next five years are needed to develop the fundamental methods for designing the provably safe automation systems and their fault management functions, refining the operational concepts for the target highway automation application and designing the experimental testbed and test protocols that will be needed to prove the safety of the systems. The first prototype test vehicles need to be developed, equipped with sensors, actuators, controllers and data acquisition systems, in a flexible development environment that facilitates software updates.

Within the subsequent five years, a closed test track needs to be retrofitted, acquired or developed to serve as the automated highway testbed environment. A large fleet of test vehicles needs to be equipped with the target automation systems and data acquisition and experimental control systems, and then they need to be driven under automatic control on the test track to acquire mileage under a full range of environmental and traffic conditions. After the systems have been refined to the point that they appear to be able to operate for an extended time without unmanaged failures, a program of deliberate fault injection testing should be initiated to determine how well the systems can respond to a wide variety of faults and combinations of faults (including both system failures and environmental disturbances).

During the subsequent ten years, the refinements and extensions needed to commercialize the safe automotive system design approach need to be developed and proven in practice. The procedure used to verify the system safety design for one vehicle needs to be demonstrated to be transferable to other vehicles, which could have very different characteristics, with a manageable investment of engineering effort.

Biography

Dr. Steven Shladover has been researching vehicle automation systems for close to 40 years, beginning with his masters and doctoral research at MIT. His expertise is in vehicle dynamics and control and transportation systems, and he has published extensively in both fields. He was one of the founders of the California PATH Program at U.C. Berkeley and of the U.S. national program in Intelligent Transportation Systems. He led PATH's participation in the National Automated Highway Systems Consortium, including the high-profile 1997 demonstration of a fully automated platoon of eight vehicles, which carried nearly a thousand riders on an eight-mile demonstration drive in San Diego. Dr. Shladover was an Associate Editor of the Journal of Dynamic Systems, Measurement and Control and chaired the ASME Dynamic Systems and Control Division, which awarded him its Charles Stark Draper Award for Innovative Practice in 2008 "for fundamental contributions to the development of intelligent vehicle and highway systems". He also chaired the Transportation Research Board's Committee on Intelligent Transportation Systems for six years, and has led the U.S. delegation to ISO TC204/WG14, which is responsible for international standards on Vehicle-Roadway Warning and Control Systems, since 1994.