NSF Transportation Cyber-Physical Systems Position Statement

Fault-Tolerant Vehicle 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

Recent developments by Google and most major automotive industry companies have raised the level of interest in road vehicle automation technology. Prior research and development work by PATH and others has already shown that most of the control system design problems for road vehicle automation 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 vehicle automation.

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 automated road vehicles, where there is very little tolerance for failures (which can easily kill or injure innocent members of the general public). While 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, including other transportation systems as well as medical equipment (which has already suffered disastrous examples of deaths caused by software bugs).

Research is also needed to develop the fundamental methods for designing provably safe vehicle automation systems and their fault management functions, refining the operational concepts for the target road vehicle automation application that can best implement comprehensive fault management and designing the experimental testbeds and test protocols that will be needed to prove the safety of the systems. 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 so that they can be used efficiently by researchers to evaluate alternative fault tolerant system designs and design methods.