# Monitoring for Safety in Transportation CPS

A. Prasad Sistla and Miloš Žefran
University of Illinois at Chicago, Chicago, IL
{sistla,mzefran}@uic.edu

Transportation has been witnessing dramatic technology developments in recent years. At the core of these developments has been the interaction between computing and traditional mechanical/electrical components. Despite extensive testing and validation, these systems are still likely to exhibit erroneous behaviors due to their complexity. As a consequence, an additional level of security and safety, that can be provided by real-time monitors, is highly desirable.

Uncertainties in design, sensing and execution environment make monitoring of such CPS particularly challenging. We have been developing a methodology for real-time monitoring of stochastic CPS, providing conditions when such monitoring is feasible and computationally effective. Below we describe several new research directions that could have a significant impact on the safety of future transportation CPS.

1. Driver assist systems are fast being integrated into production vehicles. These systems take on ever increasing proportion of the low-level operation of the vehicle. However, their correct operation depends on the predictable behavior of the driver. Deviations from such expected behavior can lead to a system breakdown. To protect against such failures we propose to learn possible driver models, compute a probability distribution over these models based on the observed driver actions and then estimate the future behavior of the vehicle and monitor it for possible safety violations.

2. Vehicular networks are promising to dramatically change the nature of vehicular traffic. Of particular interest are advanced algorithms for route planning, congestion management and accident prevention. The dynamics of such networks critically depends on the physical environment as well as individual driver behavior. However, while the physical environment is relatively easy to sense, driver behavior is exceedingly difficult to model and measure. We propose techniques to learn the models of the environment and combine them with driver behaviors mentioned above. Using sampling techniques, these combined behaviors can be employed to propagate the belief of the overall state of the system. This belief can in turn be used for monitoring and prediction of system failures/accidents.

3. Current monitoring techniques are based on estimating the belief state of the system and directly employing it for the monitoring. We propose alternate methodologies that formulate monitoring as a Partially Observable Markov Decision Process (POMDP) through a suitable reward structure. The resulting POMDP can be efficiently solved using Partially Observable Monte Carlo Planning (POMCP), resulting in monitors that can be easily adapted to task at hand by appropriately modifying the reward structure.

4. Transportation CPS involve many components that operate autonomously and interact with each other. Model checking for verification of concurrent software and hardware systems offers many techniques that can be adapted for monitoring of such systems. Examples include symbolic techniques (such as BDDS SAT solvers) and symmetry reduction techniques. To make these techniques computationally efficient, they will be combined with particle filters used for state estimation.