**

Dr. Raj Rajkumar, Director

***INSTRUCTIONS:*** *Please use this form to submit your UTC proposal. Fill-in complete answers for all questions. Proposals are limited to 4 pages, excluding deployment partner support letters. Submit complete proposals along with your completed UTC Cost Proposal Form (see below)* ***no later than November 7, 2014.***

**1. Project Title:**

Proving Autonomous Vehicle & Advanced Driver Assistance Systems Safety

Is this project a renewal or continuation of a previous UTC project *(check one)* yes

Identify the Thrust Area:

In-Vehicle Technologies

Connected Vehicle Technologies

Infrastructure-based Technologies

Vehicle Automation Technologies

Mobility Analytics

Policy

Other

If Other, please provide a brief description of the thrust area:

**2.** **CMU** **Research Team:**

|  |  |  |
| --- | --- | --- |
| **Principal Investigator(s)** | Affiliation | Email |
| André Platzer | CS, CMU | aplatzer@cs.cmu.edu |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **Co-Principal Investigator(s)** | Affiliation | Email |
| TBN, Postdoc | CS, CMU |  |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Graduate Student(s)** | Degree Program | Anticipated Completion | Curriculum/Department |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Undergraduate Student(s)** | Degree Program | Anticipated Completion | Curriculum/Department |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**3. Non-CMU Deployment Partners:**

|  |
| --- |
| **Deployment Partners** |
|  |
|  |
|  |

*Letters of support are required to be attached to this proposal from all participating deployment partners on company letterhead. Deployment partners that do not provide a support letter will not be counted during the proposal selection process.*

**4. Contact Information for Non-CMU Deployment Partners (*from #3 above*):**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title** | **Organization** | **Phone/Email** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**5. Executive Summary (Abstract) of Project:**

***(Limit of 300 words,******Executive Summary will be used for public dissemination if project is awarded)***

Smart transportation systems hold tremendous potential to make future transportation both safer and more efficient. As a consequence, we increasingly put control decisions into the hands of computers. Widely deployed examples in modern cars include adaptive cruise control, lane departure warning systems, and emergency braking systems or electronic traction control systems. Even fully autonomous cars are becoming increasingly possible. Safety of the interaction of autonomous cars with their environment is of prime importance. Examples of such safety features include obstacle and pedestrian avoidance, lane assistance, and safe lane change maneuvers. Without sufficiently strong guarantees about certain minimal baseline safety behavior, it is getting increasingly impossible to advance computer-assisted car safety technology in reliable ways. Such guarantees are crucial pieces of evidence for authorities and stakeholders to accept novel designs that are, for good reasons, getting further away from the historic safety arguments. This project studies the use of formal verification techniques with differential dynamic logic in the KeYmaera theorem prover and the modeling tool Sphinx to develop provably safe controls for car traffic situations that can be helpful for both driver assistance technology and autonomous driving.

**6. Description of the Project:**

Smart transportation systems hold tremendous potential to make future transportation both safer and more efficient. As a consequence, we increasingly put control decisions into the hands of computers. Widely deployed examples in modern cars include adaptive cruise control, lane departure warning systems, and emergency braking systems or electronic traction control systems. Even fully autonomous cars are becoming increasingly possible. Safety of the interaction of autonomous cars with their environment is of prime importance. Examples of such safety features include obstacle and pedestrian avoidance, lane assistance, and safe lane change maneuvers. Without sufficiently strong guarantees about certain minimal baseline safety behavior, it is getting increasingly impossible to advance computer-assisted car safety technology in reliable ways. Such guarantees are crucial pieces of evidence for authorities and stakeholders to accept novel designs that are, for good reasons, getting further away from the historic safety argument that the driver is always in charge and could override the system if it malfunctioned.

Formal verification methods help to exhaustively analyze autonomous cars and their control algorithms for correctness. Verification of such systems is challenging, because they not only execute discrete (control) algorithms, but also interact with the real world through sensors and actuators, which gives rise to infinitely many possible scenarios to consider. For verification purposes, we thus need to take into account discrete control algorithms and the continuous physical behavior of the car and the environment. Hybrid systems are a suitable mathematical model to describe systems with interacting discrete and continuous behavior. We focus on theorem proving for hybrid systems as verification method, and use differential dynamic logic [1] implemented in the KeYmaera theorem prover for hybrid systems [2] and the modeling tool Sphinx [3].

In a recent case study [4], we proved the correctness of an obstacle avoidance algorithm for autonomous ground robots operating in an unconfined two-dimensional space with dynamic obstacles. The resulting behavior is provably safe and useful for ground robots. The results transfer to cars but result in correct but conservative behavior for traffic situations. This project proposes to generalize these results to car traffic.

Unlike agents in unstructured environments that round robots face, road traffic follows very specific rules to ensure both safety and efficiency. By considering these rules in the formal verification process, the hope is to verify correctness without hampering efficiency. We propose to consider formal verification case studies of safety features of autonomous cars, specifically taking into account the spatial and temporal constraints found in car traffic.

For example, lanes on roads together with rules on changing lanes are designed so that lateral separation between vehicles can be small. Lanes are also directional, so that vehicles can maintain speed even when other vehicles approach on the opposite lane, which gives high relative velocities that would cause ground robots in unstructured environments to engage aggressive collision avoidance measures that are necessary for safety in unstructured environments but inefficient for road traffic. Likewise, vehicles are supposed to maintain a safe distance to the cars in front of them, but can disregard the cars to the back. Traffic rules partition responsibility for safety sensibly between vehicles, because no single vehicle can guarantee safety when the entire environment acts maliciously. The observation is that global safety emerges because vehicles locally ensure not to be blamed of violating a traffic rule [5].

The primary objective of this project is to develop a safe-by-design controller that allows efficient driving with respect to basic traffic rules and under the assumption of “reasonable” driving behaviors. The safety definition will vary from a conservative separation property where vehicles are expected to maintain a strictly positive distance to a more relaxed and realistic definition where the deriver is not to blame if hit from behind while moving forward (this is often referred to as passive safety). We want to stress that the safety property we will be considering is flexible and the concepts and methodologies we will be developing will not assume a fixed template for safety allowing a wider range of applications. The tasks of this project will concentrate on scenarios similar to the following examples.

.

1. **Stay in a straight lane.** Consider a scenario where a single car has to stay on a straight lane, while it is allowed to steer and thus drive non-straight trajectories within the lane boundaries. This is an essential feature for any car to participate in road traffic and a pre-requisite for further scenarios that assume lanes and allow steering. Existing safety proofs for cars traveling in lanes (e.g., [6]) assume that the motion of a car is perfectly straight, which is is not satisfied in practice.
2. **Obstacle avoidance on a single directional lane.** Consider a scenario where a leader car, an intermediate car, and a follower car are moving forward in the same straight lane. The objective is to design and prove safety of a controller that will equip the intermediate car so that it always stops before hitting the leader car, while it reacts to safety violations of the follower car gracefully to not hamper efficiency. Existing proofs of obstacle avoidance (e.g., [4]) are inefficient in that they require the intermediate car to engage the emergency brakes when the follower car violates the necessary safety distance. With safety notions based on “blame” using the driving direction, the objective is to let the intermediate car react to safety distance violations of the follower car gracefully (i.e., not engage emergency brakes).
3. **Obstacle avoidance on multiple lanes with (opposite) driving directions.** This scenario considers multiple lanes, where the intermediate car has to ensure safety w.r.t. a leader car on the same lane, while not acting conservative about cars on other lanes. This scenario is important to let controllers handle opposing traffic and drive in close proximity to other cars. The analysis could be extended to unreasonable behavior of the leader car (e.g., drive backwards), in which case the safety notion has to blame collisions on the leader.
4. **Lane change maneuver to neighboring lane.** We plan to consider multiple lanes where the equipped car is allowed to change its lane. This extension allows a car to overtake the follower car instead of being required to stop when the leader stops. In this scenario, the challenge is to prove safety during the transition.
5. **Stay in a curved lane.** Roads are often curved. This scenario is designed to study the behavior of controllers on curved paths. We will consider one curved lane, before extending to multiple non-crossing lanes.

The complexity of all scenarios can be varied along the interfaces between the controlled car and its environment. We first assume perfect, instantaneous sensing and actuation, and loss–free, instantaneous communication. Extensions to sensing and actuation uncertainty, as well as communication delays are further interesting advances.

Depending on our progress on our main objectives, we consider studying liveness properties. We want to ensure that the safe designed controller has a realizable implementation that allows the equipped car to progress, safely. The liveness tasks of this project will focus on scenarios similar to the following examples.

1. **Drive to a waypoint on an empty straight lane.** In this scenario, a car has to drive from its current position to a waypoint further up on its lane, without obstacles or other cars on the lane. The objective is to show that obstacle avoidance controllers (e.g., the safety controllers of (2) and (3) above) do not prevent useful behavior. Can be extended to allow other cars on the lane, assuming those are not stopped infinitely long.
2. **Cross an intersection.** This scenario considers a car having to travel straight across an intersection, while yielding to traffic on the crossing road. Can be extended to making a right turn or a left turn at the intersection. Start with traffic from one direction (e.g., from the left) and then extend to traffic from both directions.

This research activity will be based on prior research by the CMU group about uses and advances of its background in KeYmaera-based theorem proving for hybrid systems.

Literature

[1] André Platzer. Logics of Dynamical Systems. In LICS, pages 13–24. IEEE, 2012. doi: 10.1109/LICS.2012.13.

[2] André Platzer and Jan-David Quesel. KeYmaera: A Hybrid Theorem Prover for Hybrid Systems. In Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, IJCAR, volume 5195 of LNCS. Springer, 2008.

[3] Stefan Mitsch, Grant O. Passmore, and André Platzer. Collaborative Verification-Driven Engineering of Hybrid Systems. Math. in Comp. Sci., 2014. doi: 10.1007/s11786-014-0176-y.

[4] Stefan Mitsch, Khalil Ghorbal, and André Platzer. On Provably Safe Obstacle Avoidance for Autonomous Robotic Ground Vehicles. In Robotics: Science and Systems, 2013.

[5] Stefan Mitsch, Jan-David Quesel, André Platzer. From Safety to Guilty and from Liveness to Niceness. *In Formal Methods for Robotics and Automation 2014*.

[6] Sarah M. Loos, André Platzer and Ligia Nistor. Adaptive cruise control: Hybrid, distributed, and now formally verified. In Michael Butler and Wolfram Schulte, editors, *17th International Symposium on Formal Methods, FM, Limerick, Ireland, Proceedings*, volume 6664 of *LNCS*, pages 42-56. Springer, 2011.

**7. Timeline of the Project:**

We plan to spend 3 months for each objective stated above. Depending on the progress made, the remaining time will be used to explore liveness properties.

**8. Expected Accomplishments and Metrics:**

We plan to deliver hybrid models that are proven safe. The concepts and methodology used to design and prove those models will constitute a companion technical report or publication to those models.

**9. Deployment Plan:**

Results from previous projects have been disseminated with industrial partners, including partners starting a commercialization in the relevant scope of the application domain. This practice will be continued in this project.

**10. Budget:** Please use separate **UTC Cost Proposal Form** to submit this information.

The travel expenses for the upcoming year will be used as follows:

Conferences with the limit of two project personnel travel on two east coast conferences and one project personnel travel on one west coast conference. The conference should be of interest to this project without necessarily presenting a publication related to this particular project. The conference choice will be justified if the travelers will not present a project-related publication.