Systematic and Provably Safe Design Methodology for Connected and Autonomous Vehicles

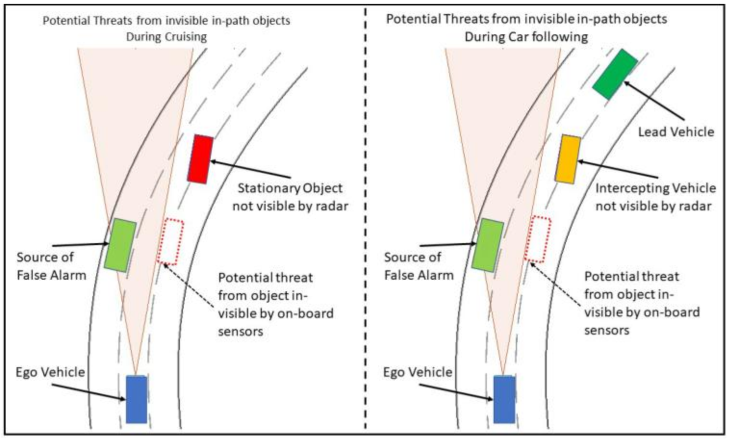
Petros Ioannou
Viterbi School of Engineering
ioannou@usc.edu

Project Objective

Design provable safe vehicle controllers that guarantee that all vehicle states stay inside safe sets while meeting the performance requirements of navigation and mobility. Use validated vehicle models and traffic simulations to demonstrate the effectiveness of the proposed methodology and evaluate the generated trade-offs between safety and mobility.

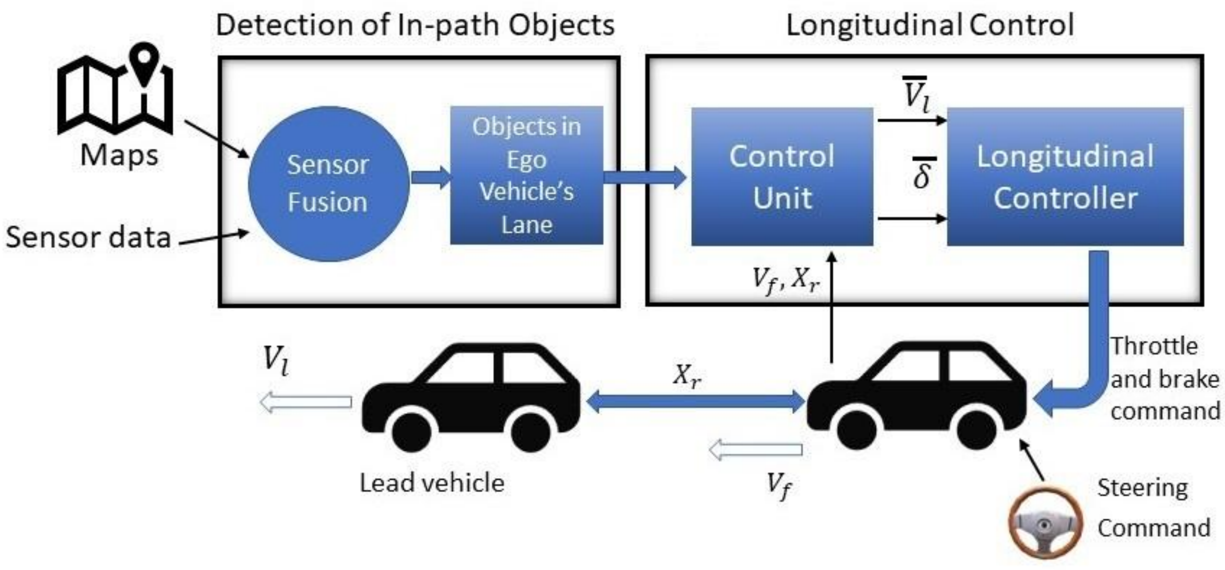
Problem Statement

Today's sensor technologies are not at the level of emulating human eyes with 100% accuracy. Recent accidents with autonomous vehicles where sensors failed to correctly identify the threat suggests that sensor possible inaccuracies or inability to identify upcoming obstacles due to environmental conditions, road geometry, unpredictable vehicle maneuvers and traffic conditions need to be considered in a more systematic way. The safety-critical nature of autonomous vehicles calls for systematic analysis and design procedures to ensure the safety of the passengers, pedestrians, and other actors on the road by considering sensor uncertainties, road geometry, weather and traffic conditions, etc. The following diagram shows an example of potential false alarms on a curved road where radar sensors may fail to identify the threat.



Research Methodology

A systematic control design methodology for provably safe autonomous vehicles for a wide range of driving conditions is developed in the presence or absence of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication which considers traffic rules, road geometry, sensor uncertainties and other environmental factor. The approach involves the development of safety constraints that define safety operational sets with vehicle controller designed to guarantee that the vehicle operates within these safety sets. Sensor uncertainties for example, lack of visibility around turns, bad weather, traffic lights, other vehicle maneuvers etc influence the size of these safety sets which are time varying and continuously adapting to driving conditions making sure that the vehicle is operating in a guaranteed for safety environment. The following diagram shows the configuration of the controller where the control unit contains all the safety sets that the longitudinal controller uses to generate the throttle and brake commands for the vehicle to remain inside these safety sets.



Sensor data may include any information available from on board sensors but also vehicle and roadside communications. For safety different sensors may provide measurements of same variables and these measurements need to be fused in order to reduce false alarms by rejecting erroneous data. If the state of the vehicle gets outside the safety set at a point in time due to a rapid change in traffic the proposed controller reacts automatically and brings the vehicle within the safety set. Example of such a rapid change includes vehicle cut-ins where the cut-in vehicle is too close to the ego vehicle creating an unsafe situation. The ego vehicle in this case decelerates immediately till the intervehicle spacing becomes safe i.e. gives enough time and space for the ego vehicle to stop without colliding. Another example is around curves where no sensor can see what is around the corner. Using map information to identify the curve the vehicle reduces its speed till what is behind the corner becomes visible. The reduction in speed depends on the geometry of the turn and is generated based on the ability of the vehicle to stop if there is a hidden from the sensors obstacle.

Results

Proposed a control design for autonomous vehicles which takes into account the uncertainties of sensors, road geometry, communication technologies, other vehicles and obstacles, traffic rules and traffic lights and external environmental conditions.

Demonstrated using computer simulations that the proposed control design for vehicle control keeps the vehicle within safety sets and therefore reduces the risk of accident and false alarms considerably.