World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:10, No:02, 2016

VeriFy: A Solution to Implement Autonomy Safely and According to the Rules

Authors : Michael Naderhirn, Marco Pavone

Abstract : Problem statement, motivation, and aim of work: So far, the development of control algorithms was done by control engineers in a way that the controller would fit a specification by testing. When it comes to the certification of an autonomous car in highly complex scenarios, the challenge is much higher since such a controller must mathematically guarantee to implement the rules of the road while on the other side guarantee aspects like safety and real time executability. What if it becomes reality to solve this demanding problem by combining Formal Verification and System Theory? The aim of this work is to present a workflow to solve the above mentioned problem. Summary of the presented results / main outcomes: We show the usage of an English like language to transform the rules of the road into system specification for an autonomous car. The language based specifications are used to define system functions and interfaces. Based on that a formal model is developed which formally correctly models the specifications. On the other side, a mathematical model describing the systems dynamics is used to calculate the systems reachability set which is further used to determine the system input boundaries. Then a motion planning algorithm is applied inside the system boundaries to find an optimized trajectory in combination with the formal specification model while satisfying the specifications. The result is a control strategy which can be applied in real time independent of the scenario with a mathematical guarantee to satisfy a predefined specification. We demonstrate the applicability of the method in simulation driving scenarios and a potential certification. Originality, significance, and benefit: To the authors' best knowledge, it is the first time that it is possible to show an automated workflow which combines a specification in an English like language and a mathematical model in a mathematical formal verified way to synthesizes a controller for potential real time applications like autonomous driving.

Keywords : formal system verification, reachability, real time controller, hybrid system
Conference Title : ICRMV 2016 : International Conference on Robotics and Machine Vision
Conference Location : Melbourne, Australia
Conference Dates : February 04-05, 2016