Semester Project

Michael Dembinski

May 2, 2017

1 Introduction

In the year 2017 we are living in a time where the science fiction fantasies of old movies are becoming more and more plausible. We have access to massive amounts of information in our pockets, we are able to re-use rockets for space travel, and autonomous cars are on the horizon. Today, there are commercial vehicles that contain a range of autonomous driving features amounting to various levels of overall autonomy in modern day cars. On the horizon there is the potential for cars that require no driver, such as the Google self-driving car, or for some autonomous features to be common amongst all modern cars such as cruise control. With features like this being implemented in commercial vehicles, it is imperative that they are designed using formal methods to prove the safety of the system design. When designing each feature it is also important think of it in terms of its interaction with the driver and the other features, and not just as a stand alone feature.
This project will focus on the use of formal methods in the system design process of an autonomous vehicle. More specifically, this paper will detail the modeling, validation, and verification efforts for the system design of three autonomous features and their overall implementation. For this design the method of model checking with the assistance of Spin will be used. In order to maintain a tight scope on this project a certain set of assumptions were made at the outset.

- This is a semi-autonomous system that requires a driver.
- There are only three autonomous features on board.
  - Adaptive Cruise Control.
  - Lane Assist.
  - Collision Avoidance.
- Lower level operations work appropriately.

Throughout the rest of this paper, this design will be explored in more depth. Each model created will be described in more depth, along with each model's verification and results. Each model went through a very similar validation effort to ensure the model was modeling what was desired, this will be described in a

general fashion since it applied to each model in very similar ways. Since this project required a tight scope, some potential for future work to expand this design will also be discussed at the end of this paper.

2 Modeling

2.1 Adaptive Speed Control

In autonomous vehicles the main function of adaptive speed control is to maintain a specific follow distance of a certain time to maintain separation with the vehicle in front of it. This type of feature would only control the acceleration control of the vehicle. Essentially this system would need to be able to understand the current state of the vehicle in relation to forward traffic and make a decision based on this information to either do nothing, accelerate, or decelerate. To model this high level decision design, spin was used. The model included three processes running concurrently.

First there was a process to simulate the reading of a car ahead, it is made up of a loop that randomly picks whether a car is ahead or not. This essentially simulates the possibility for a sensor outcome to be true or false with regards to the presence of forward traffic.

The other two processes involved don't run unless there is a car ahead. If there is no car ahead the vehicle maintains chosen speed and neither accelerates nor decelerates. If there is a car ahead the second process acts as a distance monitor. It determines whether the follow distance is decreasing or increasing, and whether this distance is out of acceptable range one way or the other.

Depending on the results of process two, the third process will either accelerate, decelerate, or do nothing to correct the follow distance. It is important for the other two processes to run concurrently over this one so that it can simulate the possibility of a rapid change in the situation.

2.2 Lane Assist

This feature is very similar to adaptive speed control. Instead of using acceleration and deceleration to maintain a distance though, steering is used to maintain lane adherence. This system is similarly made up of three processes to simulate the decision process needed to determine if corrective action is needed to avoid leaving the lane unintentionally.

The first process is a reading process that determines whether or not lane lines can be seen by the sensors. This allows for the possibility of a road with no lane lines such as a back road in the country. It is also important for this one to run concurrently over the other two, to simulate the possibility of a rapid change from available lane lines to none. Second, there is a process to read the state of the situation. It determines whether a line has been breached or not, as well as whether the vehicle is to close to a line or not. This process will only run if there are usable lines as determined from process one. Lastly, using the output

of process two, the third process will make a control decision. In the case of a breach, a corrective steering measure will be used to veer the vehicle back into its lane. If the vehicle is close to the line but not breached however, there will only be a warning issued to the driver without any direct control being taken away from the user.

2.3 Collision Avoidance

This is arguably the most important feature included in this system. Collision avoidance is a feature that should be able to detect the potential for a collision and make an appropriate decision to avoid it if possible. Due to the nature of collisions an assumption was made to simplify the design, it was assumed that this event happens in a fairly short time frame. Because of this assumption we are able to design the three processes needed, to run in series and not concurrently. In Spin this series running is accomplished with a set of guards that make it possible for only one process to be active at any given time.
The first process acts simulates the system either detecting a potential collision or not. It would run constantly in the background of the overall system until it detected a potential collision.
Once this occurred the second process would be called to conduct a risk assessment. This model simulates a risk assessment by randomly assigning each potential corrective maneuver (veer right, veer left, speed up, slow down) with a risk rating between 0 and 3. It also automatically ranks the direction of the potential collision with a risk rating of 4, thus guaranteeing a max risk rating for that direction. 0 risk signifies the potential for a maneuver that results in no collision or off road result.
This risk assessment is important because it allows for the potential of an inevitable collision, but still leads to a ranking of the maneuvers. How this risk and ranking is done is in some ways a question of morality and ultimately not explored as part of this paper.
Process three is called after process two completes. This process is the process that decides which action to take in order to avoid the collision. In many cases it is possible to achieve an equal risk rating for multiple maneuvers. When a case like this happens, the system will favor veering right actions, and braking actions. Braking is prioritized because it will reduce energy in the system, except for the case of rear ending, however in this case it would be the maximum risk and thus wouldn't match the risk rating of any other maneuver. Swerving right is prioritized because in the US, if you swerve right you will not end up swerving into oncoming traffic lanes.

2.4 Overall System

This is the model of the overall system of the vehicle that determines which system is allowed control for speed and steering at any given time. This ended up being the simplest system to model because of an assumption made while modeling. This assumption is that the adaptive speed control has been acti-

vated since the start of the drive.
It is only made up of two processes that run concurrently. The first process runs as a detection process, monitoring the various feature monitors. The second process is the distribution process. Depending on which features are requesting control at any given time, this process will resolve requests in a particular order. If there is only one request for control it will warn the driver and relinquish control. However if there are multiple requests, it will favor the collision avoidance feature above all others due to the safety critical nature of this feature.

3 Model Validation

Now that the systems have been modeled it is necessary to now validate this model before the verification step. Validation is a means to ensure that what you have modeled accurately depicts your system. For each model a similar process was used to validate them. First while writing the model in Spin, an automaton was drawn and updated as a base to create the model from. After the model was written three things were done.
First the code was reviewed line by line to ensure proper syntax, logic, and intent. If any bugs were found at this step, the code was updated and then the review started over.
Next the model was simulated and reviewed using random initial seed values, this generally didn't produce any unwanted results. Once this was accomplished the simulation was run interactively allowing me to chose the next state of the system at each step. This allowed me to check for any unwanted results and ensure the potential for other uncommon results.
Lastly some simple validation specifications were written in temporal logic to check the system against. These were used to generate counter example traces that verified the possibility of certain outcomes. For example it allowed for the proof that a collision is possible in the collision avoidance model, which should be a potential outcome for that model.
This process was used for all four models, so this will be the extent of the discussion regarding model validation. Each specific discussion for particular model validation would be near identical with only a handful of details and results being different.

4 Verification

Verification is the step necessary to check that the model satisfies certain specifications such as liveness and safety properties. Liveness is an important property for semi-autonomous vehicles, in that most features should eventually give control back to the human driver. Each of these specifications is written using linear temporal logic and checked against the model using the Spin model checker. To ensure that all of these specifications are neither universally valid or invalid, they were each checked against a global model for each model. During this

check it seen that both the negative of the specification and the specification itself produce counterexamples.
The particular specifications used for verification of each model are listed below.

- Adaptive Speed Control
  - Safety/Liveness $\square\lozenge\neg tooClose$
- Lane Assist
  - Safety/Liveness $\square\lozenge\neg laneRbreach$
  - Safety/Liveness $\square\lozenge\neg laneLbreach$
- Collision Avoidance
  - Liveness $\square\lozenge(\neg maneuvering \vee collided)$
  - Safety $\square(maneuver_direction \implies minimum_risk_direction)$
- Overall System
  - Liveness $\square\lozenge HumanControlSteering$

5 Conclusion

This project has been an exercise in the formal methods design process. Instead of prototyping and testing designs to find problems and redesigning, this design loop is capable of recognizing design problems long before building and testing. All of the models detailed in this report underwent multiple iterations informed by the results of various steps in the model checking process.
This realization in a way makes the true results of this project, the models. All of the work on this project has been towards designing and improving upon the design of various models used to define a system of this type. This has all been done at a fairly high level of abstraction, but a similar process could be used to design lower level portions of the same system.
Because of this, there is a lot future work that can be done on this project by exploring lower levels of abstraction. That alone would greatly increase the scope of this project, but another option for future work would be to add additional features. To take this idea to the extreme would be to design a fully autonomous car that doesn't need a driver.

References

[1] Shigeharu Miyata, Takashi Nakagami, Sei Kobayashi, Tomoji Izumi, Hisayoshi Naito, Akira Yanou, Hitomi Nakamura, Shin Takehara *Improvement of Adaptive Cruise Control Performance* 2010: Hindawi Publishing Corporation.

[2] Jochen Pohl, Jonas Ekmark *A Lane Keeping Assist System For Passenger Cars*: Volvo Car Corporation.

[3] Adi Lang, Deepa Jonnagalda, Alex Atahua, Andy Hammond *Automobile Collision Avoidance System.*