Autonomous Vehicles Meet the Physical World: RSS, Variability, Uncertainty, and Proving Safety

Philip Koopman[1,2](✉), Beth Osyk[1,2], and Jack Weast[1,2]

[1] Edge Case Research, Pittsburgh, PA, USA
koopman@cmu.edu, bosyk@ecr.guru, jack.weast@intel.com
[2] Intel, Chandler, AZ, USA

Abstract. The Responsibility-Sensitive Safety (RSS) model offers provable safety for vehicle behaviors such as minimum safe following distance. However, handling worst-case variability and uncertainty may significantly lower vehicle permissiveness, and in some situations safety cannot be guaranteed. Digging deeper into Newtonian mechanics, we identify complications that result from considering vehicle status, road geometry and environmental parameters. An especially challenging situation occurs if these parameters change during the course of a collision avoidance maneuver such as hard braking. As part of our analysis, we expand the original RSS following distance equation to account for edge cases involving potential collisions mid-way through a braking process.

Keywords: Autonomous vehicle safety · RSS · Operational design domain

1 Introduction

The Responsibility-Sensitive Safety (RSS) model proposes a way to prove the safety of self-driving vehicles [12]. The RSS approach is currently deployed in Intel/Mobileye's test fleet of fully automated vehicles. Application areas of RSS include both fully autonomous vehicles and driver assistance systems. This paper reports results of an ongoing joint project to externally validate and further improve RSS.

A salient feature of RSS is the use of Newtonian mechanics to specify behavioral constraints such as determining safe following distance to avoid collisions even when other vehicles make extreme maneuvers such as hard braking. Employing RSS as safety checking logic requires not only knowledge of the physics of the situation, but also correct measurements to feed into the RSS equations.

We consider an example of applying RSS rules to a longitudinal following distance scenario involving the vehicle under consideration (often called the *ego vehicle*) as a follower behind a lead vehicle. To put RSS into practice, the ego vehicle requires at least some knowledge of the physical parameters fed into the physics equations, including ego vehicle and lead vehicle status, road geometry, and operational environment. However, proving guaranteed safety via that approach is complicated by variability and uncertainty.

© Springer Nature Switzerland AG 2019
A. Romanovsky et al. (Eds.): SAFECOMP 2019, LNCS 11698, pp. 245–253, 2019.
https://doi.org/10.1007/978-3-030-26601-1_17

This paper identifies the implications for these issues in applying RSS to real vehicles. Additionally, it proposes a new following distance equation to encompass edge cases that were out of scope for the original RSS analysis.

A significant finding is that variability and uncertainty in the operational conditions introduce significant challenges for ensuring safety while maintaining acceptable permissiveness. (The permissiveness of a system is how free it is to operate without violating safety constraints [6].) Variability is especially problematic because of the large potential dynamic range of driving conditions [9]. For example, the difference between safe following distance on an icy hill compared to flat dry pavement means that a one-size-fits-all worst case approach to safe following distance is unlikely to result in a vehicle people will actually want to use. This paper seeks to identify the issues that must be resolved to use the RSS equations in a way that provides provable safety to the maximum degree practicable. Designing approaches that can use this foundation to address the challenges of variability and uncertainty is left as future work.

2 Related Work

Advanced Driver Assistance Systems (ADAS) have made large strides in improving automotive safety, especially in mitigating the risk of rear end collisions. Autonomous Emergency Braking (AEB) can now fully stop a vehicle in many lower-speed situations [1]. Beyond AEB, vehicles may offer driver assistance technologies including a safe distance warning [1]. Technologies have differing availability depending on speed and manufacturer [7]. Test protocols generally select a few speed combinations representative of urban and highway driving [7] in controlled conditions. Moreover, it is typical for current ADAS systems to used fixed rules of thumb (e.g., the two-second following rule as used by [5]) for establishing operational safety envelopes that while potentially improving safety on average can either be to conservative or too optimistic. This paper takes a broader approach that considers the specifics of the vehicles involved and environmental conditions. We are not aware of other work that considers expanding physics-based safety analysis such as RSS to consider environmental conditions and vehicle performance characteristics.

Work on characterizing and dealing with perception uncertainty in the context of safety critical systems is still developing. [3] provides a model of factors that influence development and operational uncertainty.

Safe state analysis is a theme for autonomous vehicle path planning. Path planning algorithms may consider the safety of the current state and reachable states in order to plan a path, including making predictions about potentially occluded obstacles [10]. Such approaches tend to suffer from probabilistic limitations on their ability to provide deterministic safety, whereas the RSS approach to safety aspires to provide a deterministic model for safety.

We base our analysis on an initial RSS paper [12], and are aware of a follow up paper [13]. Interest in the performance aspect of RSS continues to grow, with a model and analysis of traffic throughput presented in [Mattas19] comparing RSS to human drivers under various values for the RSS parameters. We are not aware of other published analyses of RSS equations for correctness and completeness.

3 RSS Overview

3.1 The RSS Following Distance Equation

In an RSS leader/follower scenario, the follower vehicle is presumed to be responsible for ensuring a safe longitudinal distance, so we assume that the ego vehicle is the follower. For this situation, RSS uses a safety principle of: “keep a safe distance from the car in front of you, so that if it will brake abruptly you will be able to stop in time.” [12] Fig. 1 shows a notional vehicle geometry:

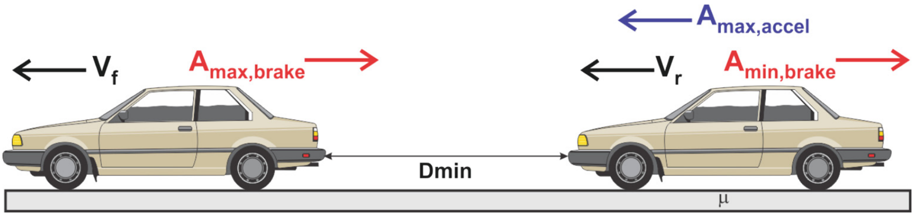

Fig. 1. Reference vehicle geometry for leader/follower.

This yields a minimum following distance (id., Lemma 2):

$$d'_{min} = MAX\left\{0, \left(v_r\rho + \frac{1}{2}a_{max,accel}\rho^2 + \frac{\left(v_r + \rho a_{max,accel}\right)^2}{2a_{min,brake}} - \frac{v_f^2}{2a_{max,brake}}\right)\right\} \qquad (1)$$

Where in our case the ego vehicle is the following (“rear”) vehicle, and:

- d'_{min} is the minimum following distance between the two vehicles for RSS
- v_f is the longitudinal velocity of the lead (“front”) vehicle
- v_r is the longitudinal velocity of the following (“rear”) vehicle
- ρ is the response time delay before the ego (rear) vehicle starts braking
- $a_{max,brake}$ is the maximum braking capability of the front vehicle
- $a_{max,accel}$ is the maximum acceleration of the ego (rear) vehicle
- $a_{min,brake}$ is the minimum braking capability of the ego (rear) vehicle

The d'_{min} equation considers a leading vehicle, going at initial speed v_f, which executes a panic stop at maximum possible braking force $a_{max,brake}$. The ego following vehicle traveling at v_r is initially no closer than distance d'_{min}. In the worst case, the ego vehicle is accelerating at $a_{max,accel}$ when the lead vehicle starts braking. There is a response time ρ during which the ego vehicle is still accelerating. Then the ego vehicle detects the lead vehicle braking and reacts by panic braking with deceleration of at least $a_{min,brake}$. RSS considers the worst case scenario to be a highly capable lead vehicle with high $a_{max,brake}$ followed by an ego vehicle that brakes at an initially lower braking capability of at least $a_{min,brake}$. A poorly braking follower requires additional distance to accommodate its inability to stop quickly.

While a derivation based on comparative stopping distances confirmed the equation, analysis using Ptolemy II [11] revealed edge cases beyond the scope of the analysis in [12]. (Additional RSS braking profile information is provided by [13].) Specifically, Eq. 1 does not detect situations in which the two vehicle positions overlap in space during – but not at the end of – the braking response scenario.

As a thought experiment, consider an ego vehicle with good brakes that has matched speeds with a leader of significantly worse braking ability. Equation 1 is derived assuming the minimum vehicle separation occurs at the final rest positions. If the rear vehicle has superior braking, it could mathematically be "ahead" of the lead vehicle at some time during braking, yet still have a final rest position "behind" the lead vehicle due to shorter stopping distance. In reality, this is a crash. Thus, an additional constraint is that the rear vehicle must remain behind the lead vehicle at all points in time.

A related scenario is a rear vehicle approaching with high relative velocity and superior braking. The rear vehicle might collide during the interval in which both vehicles are braking, while still having a computed stopping point behind the lead vehicle.

To address these situations, we break the analysis up into two parts based on the situation at the time of a collision if following distance is violated: (1) impact during response time ρ and (2) impact after ρ but before or simultaneous with the rear vehicle stopping. (Impact is no longer possible after the rear vehicle stops for this scenario.)

Accounting for situation (1) requires computing the distance change during the response time ρ. There are two cases. The first is when the front vehicle stops before ρ, and the second is when the front vehicle stops at or after ρ.

Situation (2) has two parts. First, compute the distance change during ρ:

$$d''_{min} = (v_r - v_f)\rho + \frac{(a_{max,accel} + a_{max,brake})\rho^2}{2} \tag{2}$$

Next, solve for the distance between the two vehicles after ρ as a function of time:

$$\begin{aligned} d'''_{min} = & \left(v_r + a_{max,accel}\rho\right)t_r - \frac{a_{min,brake}t_r^2}{2} \\ & - \left(\left(v_f - a_{max,brake}\rho\right)t_f - \frac{a_{max,brake}t_f^2}{2}\right) \end{aligned} \tag{3}$$

This is a parametric equation involving the time after the response time for both vehicles: t_r ant t_f. The minimum distance will occur at time $t_r = t_f = t$ when both vehicles have equal speed (with the value of t then substituted into Eq. 3 for evaluation):

$$t = \frac{(v_{r0} - v_{f0}) + \left(a_{max,accel} + a_{max,brake}\right)\rho}{\left(a_{min,brake} - a_{max,brake}\right)} \tag{4}$$

The special case minimum following distance is the sum of d'_{min} and d''_{min}, and only holds when the rear vehicle is faster than the front vehicle at the end of the response time *and* the rear vehicle can brake better than the front vehicle:

$$d_{min} = \begin{cases} MAX\left[d'_{min}, \left(d''_{min} + d'''_{min}\right)\right]; special\,case \\ d'_{min} \qquad\qquad\qquad ; otherwise(Original\,RSS) \end{cases} \tag{5}$$

Because $a_{max,accel}$ is likely to be of secondary importance for small ρ, we focus the balance of our discussion on braking. However, similar issues apply to acceleration.

3.2 Coefficient of Friction

Implicit in the RSS equations is that the maximum frictional force exerted by the vehicle on the ground limits braking ability ([14] pg. 119):

$$F_{friction} = \mu * F_{normal} \tag{6}$$

where:

- $F_{friction}$ is the force of friction exerted by the tires against the roadway
- μ is the coefficient of friction, which can vary for each tire
- F_{normal} is the force with which the vehicle presses itself onto the road surface

The friction coefficient is a property of both the tires and the road surface. It is important to note that μ can be above 1.0 for some materials ([14] pg. 119), so a rigorous proof cannot assume limited μ without placing constraints upon installed tires.

3.3 The Normal Force and Road Slope

The normal force on each tire is a property of the vehicle weight, weight distribution, the effects of suspension, the slope of the road, and so on. The normal force is the weight of the vehicle multiplied by the cosine of the road slope, shown by Fig. 2:

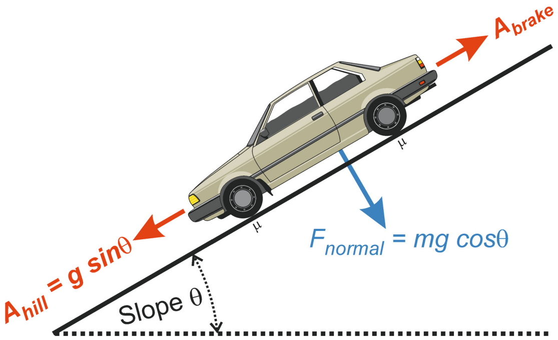

Fig. 2. Vehicle forces on an inclined roadway.

In this situation, braking ability is potentially limited by the reduced normal force. Moreover, gravity is pulling the vehicle down the hill, acting against and further reducing the net braking force ([14] pg. 102). If μ is low, the net force can result in the vehicle sliding down the hill (either forwards or backwards) if the brakes cannot overcome the gravitational downhill force vector. Transverse road slope (camber) can similarly reduce F_{normal}, but at least does not affect vehicle speed directly.

3.4 Road Curvature

An additional limitation to braking capability is that the centripetal force exerted by a vehicle to make turns must be provided by $F_{friction}$ ([14] pg. 128). The net vehicle acceleration (both radial and linear) is a result of a force vector applied by the tire contact patches to the road surface. It follows that any force used to curve the vehicle trajectory steals available force from the ability to stop the vehicle by requiring a force vector that is at off-axis from the vehicle's direction of travel. That means that if the ego vehicle is in a tight turn it will have trouble braking effectively. Lane positioning and racing line techniques [8] add additional complexity.

A banked curve complicates analysis even further, involving potential increases or decreases to F_{normal} depending upon whether the bank (superelevation) is tilted toward or away from the center of the curve.

4 Uncertainty and Variability

While Newtonian Mechanics provides us the tools to determine following distance in principle, even a simplified equation setup for a vehicle's maximum stopping distance on a downhill corkscrew turn is worthy of a college Physics final exam. But in the real world we don't actually know the precise values of all the variables in the equations.

An important issue with proving safety in a cyber-physical system is that there is inherent uncertainty in sensor measurements. That uncertainty includes both issues of accuracy (how close the measurement is to the actual value being measured) and precision (what the distribution of errors in the measurement is across multiple measurements). Uncertainty can additionally be characterized as aleatory uncertainty (e.g., sensor noise that causes non-zero precision), and epistemic uncertainty (e.g., inaccurate measurements and incorrect modeling of the environment) [2]. Both types of uncertainty impair the ability to formally prove safety for a real-world system.

The mere existence of a probability distribution for aleatory uncertainty impairs the ability to create a perfect proof. In principle any series of data points might, with some probability, be wildly inaccurate. Data filtering and statistical techniques might improve the situation, but in the end there is always some non-zero (if infinitesimal) probability that a string of outlier data samples will cause a mishap. Over-sampling to drive that uncertainty below life-critical confidence thresholds (e.g., failure rate of 10^{-9}/hr) could be impracticable due to the fast time constants required for vehicle control.

For epistemic uncertainty, a significant problem is providing a completely accurate model of the environment and the vehicle. Moreover, even if limitations on sensors and potential correlated sensor failures are mitigated through the use of high-definition maps, variability of operational environments is a significant issue.

Uncertainty cannot be completely eliminated in the real world, so the question is how to account for it within the RSS model while keeping the system practical and affordable. In support of that, we consider sources of uncertainty and variability.

4.1 Other Vehicle Parameters

Ensuring that the ego vehicle avoids colliding with other vehicles requires understanding the state of those other vehicles. Knowing where they are and where they are going requires other vehicle pose and kinematic information: {position, orientation, speed, acceleration, curvature} in addition to a prediction of how that information is going to change in the near future (e.g., path plan). That information will be imperfect.

In the absence of perfect information, RSS simply assumes that distance is known and that the lead vehicle will immediately execute a panic braking maneuver at $a_{\mathrm{max,brake}}$. While in an ideal world all vehicles have a predetermined and consistent $a_{\mathrm{max,brake}}$, in the current world not all vehicles are thus equipped. However, even if new vehicles are standardized, braking capability can increase further due to factors such as after-market brake upgrades, after-market tire upgrades, low tire pressure, after-market aerodynamic modifications, and even driver leg strength. While a vehicle might be equipped with a feature that intentionally limits maximum deceleration, too strict a limit would extend stopping distance and increase collision rates in other situations such as single car crashes.

If the ego vehicle wants to optimize following distance based on the actual lead vehicle capabilities, it will need a way to determine what those are. Most vehicles are not designed to brake above 1 g, but it is likely this limit is not universal on public roads.

4.2 Ego Vehicle Parameters

While knowing the exact state of the lead vehicle is difficult, it is also important to appreciate that knowing the state of the ego vehicle is also difficult. Many of the parameters that affect the lead vehicle also affect the ego vehicle, although the concern in this case is more about unexpectedly reduced braking ability. Some factors that might reduce braking capability below expectations include:

- Transient equipment degradation: brake fade due to overheating, brake wetness (e.g., due to puddle splash), cold tire temperature, etc.
- Equipment condition: brake wear, brake actuator damage, low tire tread depth, high tire pressure, etc.
- System interactions: interactions between braking system and electronic stability control, effect of anti-lock braking features, etc.

4.3 Environmental Parameters

Successfully executing an aggressive braking maneuver involves not only the vehicle, but also the environment. While environmental conditions in a road segment might be reasonably well known via a local weather service (which becomes safety critical as soon as it is relied upon for this purpose), average values might differ substantially from the instantaneous environmental conditions relevant to a braking maneuver. After all, it is not the average road conditions over a kilometer of road that matter, but rather the specific road conditions that apply to paths of the set of tire contact patches of each vehicle during the course of a panic stop maneuver. Relevant factors that could result in a faster-than-expected lead vehicle braking maneuver combined with a slower-than-expected ego vehicle braking maneuver due to differences on the roadway include:

- Road surface friction: road surface, temperature, wetness, iciness, texture (e.g., milled ridges that increase traction; bumps that cause loss of tire contact), etc.
- Road geometry: slope, banking, camber, curvature as previously discussed
- Other conditions: hydroplaning, mudslides, flooding, high winds pushing against a high profile vehicle body, road debris, potholes, road buckling, etc.

While the two vehicles will traverse the same stretch of roadway for some braking time, their contact patches are not necessarily going to follow exactly the same paths. Localized tire track road conditions can result in different stopping ability even if we attempt to measure some average value of μ. Consider, for example, a lead vehicle that brakes hard in snowy weather on a cleared tire path while the following ego vehicle gets caught slightly laterally displaced from the tracks with its tires on ice.

4.4 Potential Assumption-Violating Actions

Even if we know the values for all the variables, there are assumptions made by the RSS longitudinal safety guarantees and stated scope limitations that might be violated by real world situations. Examples include:

- Lead vehicle does not violate the assumed maximum braking deceleration limit (e.g., due to impact with a large boulder that suddenly falls onto the road).
- Roadway μ does not unexpectedly change (e.g., flash ice-over).
- Ego vehicle does not fall below minimum expected braking capability (e.g., due to brake fade, puddle splashes onto brake rotor).
- There are no significant equipment failures (e.g., catastrophic brake failure of ego vehicle during a panic braking event).
- There are no unusual vehicle maneuvers (e.g., cut-in scenarios in which a vehicle suddenly appears too close; cut-out scenarios in which the lead vehicle swerves to reveal a much slower, too-close new lead vehicle [4]).

5 Conclusion

An examination of RSS has validated the following distance equation for common situations and augmented that formula to handle a class of edge cases for potential collisions that can happen during a braking event. A significant potential impediment to practical adoption of RSS is providing sufficient permissiveness while ensuring safety in extreme conditions such as icy roads and encountering clusters of outlier sensor data.

To arrive at a practicable balance between safety and permissiveness, further engagement with government and industry standards organizations is recommended.

Acknowledgment. This research was supported by Intel.

References

1. ADAC Vehicle Testing, Comparative Test of Advanced Emergency Braking Systems (2013)
2. Chen, D., Östberg, K., Becker, M., Sivencrona, H., Warg, F.: Design of a knowledge-base strategy for capability-aware treatment of uncertainties of automated driving systems. In: Gallina, B., Skavhaug, A., Schoitsch, E., Bitsch, F. (eds.) SAFECOMP 2018. LNCS, vol. 11094, pp. 446–457. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-99229-7_38
3. Czarnecki, K., Salay, R.: Towards a framework to manage perceptual uncertainty for safe automated driving. In: Gallina, B., Skavhaug, A., Schoitsch, E., Bitsch, F. (eds.) SAFECOMP 2018. LNCS, vol. 11094, pp. 439–445. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-99229-7_37
4. European New Car Assessment Programme (Euro NCAP), "Test Protocol – AEB Systems", Version 2.0, March 2017
5. Fairclough, S., May, A., Carter, C.: The effect of time headway feedback on following behaviour. Accid. Anal. Prev. **29**(3), 387–397 (1997)
6. Guiochet, J., Powell, D., Baudin, É., Blanquart, J.-P.: Online safety monitoring using safety modes. In: Workshop on Technical Challenges for Dependable Robots in Human Environments, PASADENA, United States, pp. 1–13, May 2008
7. Hulshof, W., Knight, I., Edwards, A., Avery, M., Grover, C.: Autonomous emergency braking test results. In: Proceedings of the 23rd International Technical Conference on the Enhanced Safety of Vehicles (ESV) (2013)
8. Kapania, N., Subosits, J., Gerdes, J.C.: A sequential two-step algorithm for fast generation of vehicle racing trajectories. J. Dyn. Syst. Meas. Control, V **138**, Paper 091005, September 2016
9. Koopman, P., Fratrik, F.: How many operational design domains, objects, and events? In: SafeAI 2019, AAAI, 27 January 2019
10. Orzechowski, P., Meyer, A., Lauer, M.: Tackling occlusions & limited sensor range with set-based safety verification. In: 2018 21st International Conference on Intelligent Transportation Systems (ITSC), November 2018. https://arxiv.org/abs/1506.06579
11. Ptolemy Project: heterogeneous modeling and design. https://ptolemy.berkeley.edu/ptolemyII/index.htm. Accessed 5 May 2019
12. Shalev-Shwartz, S., Shammah, S., Shashua, A.: On a formal model of safe and scalable self-driving cars. Mobileye 2017. https://arxiv.org/abs/1708.06374. v6 updated 27 Oct 2018
13. Shalev-Shwartz, S., Shammah, S., Shashua, A.: Vision zero: can roadway accidents be eliminated without compromising traffic throughput? In: Mobileye 2018. https://export.arxiv.org/abs/1901.05022
14. Walker: Halliday/Resnick: Fundamentals of Physics, 8th edn., vol. 1. Wiley (2008)