Received: 15 September 2021 | Revised: 14 December 2021 | Accepted: 3 January 2022

IET Intelligent Transport Systems

DOI: 10.1049/itr2.12162

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH PAPER

A verification framework for behavioral safety of self-driving cars

Huihui Wu[1,2] | **Deyun Lyu**[3] | **Yanan Zhang**[4] | **Gang Hou**[1,2] | **Masahiko Watanabe**[5] | **Jie Wang**[1,2] | **Weiqiang Kong**[1,2]

[1] School of Software Technology, Dalian University of Technology, Dalian, China

[2] Key Laboratory for Ubiquitous Network and Service Software of Liaoning Province, Dalian, China

[3] Graduate School of Information Science and Electrical Engineering, Kyushu University, Fukuoka, Japan

[4] Automotive Data of China (Tianjin) Co., Ltd, Tianjin, China

[5] NTT DATA Automobiligence Research Center, Yokohama, Japan

Correspondence
Weiqiang Kong, Dalian University of Technology, No. 321, Tuqiang Street, Dalian Economic and Technological Development Zone, Dalian, China.
Email: wqkong@dlut.edu.cn

Funding information
National Key Research and Development Project (Key Technologies and Applications of Security and Trusted Industrial Control System), Grant/Award Number: 2020YFB2009500; Fundamental Research Funds for the Central Universities, Grant/Award Number: DUT20TD107; NTT DATA Automobiligence Research Center

Abstract

While self-driving cars have already been widely investigated and achieved spectacular progress, a major obstacle in applications is the great difficulty in providing formal guarantees about their behaviors. Since the environment of the self-driving is usually not known beforehand and highly uncertain, classical verification approaches cannot be applied to guarantee safety. To cope with any traffic situation, a novel online verification framework is presented for verifying behavioral safety of self-driving cars. The framework is based on the proposed five safety considerations: new longitudinal and lateral safe distances, lane changes, overtaking and how to face new traffic participants. Different from the previous verification considerations, this verification framework allows actual behaviors of self-driving cars to be temporarily inconsistent with the popular strict safe distance. As long as the self-driving car respects the minimum safe distance calculated by our technique and executes improvement behaviors to restore the safe distance, it is still believed that the predictive behavior is safe. The framework can easily be integrated to existing self-driving systems and evaluate different indicators involving the steering angle, acceleration and braking. The benefits of the framework in different urban scenarios of the CARLA simulator and real traffic data provided by the NGSIM project are demonstrated. Results show that the technology can successfully detect unsafe behaviors and provide effective measures to avoid potential collisions.

1 | INTRODUCTION

Self-driving cars have emerged as a widespread technology for creating more efficient transportation. Several major vehicle manufacturers including Tesla, GM, Ford, BMW, Baidu, and Waymo/Google are actively trying to put self-driving cars into society to test and improve systems, and this trend is likely to continue and intensify. However, it has been reported that self-driving cars lead to dangerous consequences like a fatal collision [1–3]. These unexpected behaviors of self-driving cars result in unsafe systems, and restrict the application of self-driving cars. Hence, there is an urgent need for a well-studied method that can provide formal guarantees for the self-driving car's behavior. Unfortunately, to provide guarantees for self-driving cars by test is difficult in terms of an impractical amount of scenario requirements and long test time. A recent study has revealed that self-driving cars need to be tested for 440 million km to demonstrate that they have a better performance than humans with a 95% confidence level [4]. This translates to 12.5 years of test driving with a fleet of 100 vehicles continuously driving 24 h a day [5]. Automatic verification techniques are thus sorely needed.

Verifying self-driving cars is a difficult task. Self-driving cars are very sensitive to the driving environment, which is usually not known beforehand and highly uncertain. Even in simple scenarios, safety-critical situations can be created at any time due to the sudden cut-in from other traffic participants. Classical verification approaches perform the safety

assessment offline before the vehicle is deployed, but they cannot adjust to the changing environments and timing-constraints of the vehicle in guaranteeing safety. Novel online verification approaches are needed to cope with any traffic situation of the self-driving vehicle during its operation. Moreover, some verification approaches that are sensitive to real-time data and interact with the environment, such as calculations involving the safe distance, can only be verified online.

One approach to guarantee safety is collision avoidance. Specific methods include reachability analysis [6–8], inevitable collision state (ICS) [9–11], and passive safety [12]. Reachability analysis calculates reachable sets of the self-driving car and other obstacles, and then checks for intersections, which represent unsafe regions where collisions may occur. It is safe when any feasible future motion of the self-driving car does not intersect with the reachable set of each obstacle. However, the disadvantage of the set-based technology is that unsafe regions may grow rapidly in a long planning horizon, eventually blocking the entire drivable area [5]. Similar to reachability analysis, ICS also calculates the state of collision. When the self-driving car is in ICS, no matter which path is selected, a collision will eventually occur. Motion plans are called passive safe, if the vehicle is at standstill at the time of collision, which is ensured by pre-computed braking trajectories in [12]. However, these two approaches are computationally expensive, and most works can only deal with a single trajectory prediction of traffic participants for online calculation.

Another potential approach is logical reasoning. Different logic applications can guarantee safety, such as higher-order logic in [13], multi-lane spatial logic in [14], and quantified differential dynamic logic in [15]. However, these logical expressions for the verification may become more complicated with the complexity of systems, which increases the difficulty of verification. Moreover, it cannot provide sufficient guarantees in facing new scenarios. Therefore, although collision avoidance and logical reasoning are often used to check the performance of self-driving systems, they are difficult to implement verification.

In this work, we propose a novel online verification framework to verify behavioral safety of self-driving cars. We reconsider the safety of lane changes and overtaking based on new safe distances we have already proposed in [16]. New safe distances of self-driving vehicles focus on neglected aspects, inflexible settings and overly idealistic assumption to supplement existing works by considering the safe distances of each stage in detail and modeling close to real traffic situations. Moreover, the following vehicle's response during lane changes is an important but overlooked issue. Thus, we consider this issue and propose feasible solutions to avoid or mitigate a potential collision. Misbehavior of new traffic participants is crucial to the current traffic situation, not only affecting motion planning of self-driving cars, but also bringing safety hazards. We propose a verification framework for new traffic participants, which can track new traffic participants with different safe distances and provide an early warning to avoid potential collisions when the current conditions unsatisfy the minimum safe distance. Finally, an online verification framework is formed by five behavioral safety considerations, which includes the longitudinal and lateral safe distances, safe lane changes, safe overtaking and how to face new traffic participants.

In existing works, as long as the current safety conditions are not satisfied, the predicted behavior of self-driving cars is directly judged as unsafe. However, in our framework, before the self-driving car reaches the limit of safety conditions (the most stringent safety conditions), we will continue to track it. If the self-driving car takes some measures to mitigate the current situation until safety conditions are finally satisfied, we believe that the predicted behavior is still safe. Therefore, our approach is slack. During our online verification, we mark those cases that unsatisfy safety requirements. These marks are reflected by pre-setting 5 parameters (the rationality of planned trajectories, the accuracy of the prediction model, the implementability, the resilience and the sensitivity). These parameters can be used to evaluate the performance of the self-driving system, and may be used to guide planning trajectories or evaluate the accuracy of behavior prediction in the future.

Our contributions can be summarized as follows. We (i) propose an online verification framework to verify the behavioral safety of self-driving systems, which allows effortless integration in vehicles and reduces costs for certification; (ii) reconsider the safety of lane changes and overtaking based on new safe distances; (iii) discuss implementation measures about the response of the following vehicle during lane changes; (iv) implement continuous tracking to quickly identify whether a new traffic participant interferes with the predicted behavior of the ego vehicle; (v) show the performance of self-driving system by predetermined parameters; (vi) conduct a safety evaluation on the CARLA's self-driving system, demonstrating the feasibility of our framework and finding safety hazards in the self-driving system.

The rest of the paper is organized as follows. We begin with some background on safe distances between vehicles in Section 2. We then describe some verification conditions in the safety framework in Section 3, followed by a safety framework for self-driving cars in Section 4. Experimental results are described in Section 5. Related work is discussed in Section 6, and we conclude in Section 7.

2 | BACKGROUND

In various verification approaches for self-driving cars, a key component is the safe distance definitions between two vehicles, which we denote as d_{safe}. Current safety considerations related to safe distances undertaken in many works are based on the safe distance definitions of Responsibility Sensitive Safety (RSS) [17] and Rizaldi et al. [18]. If there are no new traffic participants in the current scenarios, the safety of a lane change depends on four adjacent vehicles (the leading and following vehicle in both the current and the target lane). In consensus with Pek et al. [19], the ego vehicle must respect the safe distance to the leader in at least one of the lanes at every point in time. When the ego vehicle approaches the gap and prepares the lane change, it is necessary to respect the safe distance to

the leader in the source lane. Once the ego vehicle completely enters the source lane, the follower in the source lane is expected to respect the safe distance to the ego vehicle.

2.1 | Safe distance

To determine whether a self-driving car is in a safe state or even if a planned maneuver can be safely executed, Vienna Convention on Road Traffic [20] adopted by 74 countries is introduced. The Vienna Convention defines the safe distance between two vehicles as a "sufficient distance to avoid a collision if the vehicle in front should suddenly slow down or stop". It means that the safe distance d_{safe} to a leading vehicle B_l must be large enough for the ego vehicle to stop behind it if B_l, at worst, performs an maximum emergency brake. According to the natural language description of the safe distance in the Vienna Road Traffic Convention, two different safe distance definitions mathematically defined are proposed in [17] and [18].

The indices l and f denote the leading or following vehicle of the ego vehicle inside a lane. t is the time, and we assume that the initial time is $t_0 = 0$. We use v to denote the velocity. a and b denote the deceleration and acceleration, respectively, of a vehicle. The future position of a vehicle for a point in time $t \geq 0$ is expressed by the following motion equation:

$$d(t) = d_0 + vt + \frac{1}{2}at^2, \tag{1}$$

where d_0 denotes the position of the vehicle at t_0.

In [18], Rizaldi *et al.* proposed the longitudinal safe distance definitions, which takes reaction times $\delta \geq 0$ into account. The leading vehicle performs an emergency brake with maximum deceleration $a_{max,l} < 0$. After $\delta > 0$ seconds of reaction time, the ego vehicle also performs an emergency brake with maximum deceleration $a_{max,ego}$. The braking movement of the leading vehicle mathematically is defined as follows:

$$d_l(t) = \begin{cases} d_{0,l} + v_l t + \frac{1}{2}a_{max,l}t^2 & 0 \leq t \leq t_{stop,l} \\ d_{0,l} - \frac{v_l^2}{2a_{max,l}} & t_{t_{stop,l}} \leq t \end{cases}, \tag{2}$$

where $t_{stop,l} = v_l / |a_{max,l}|$ is the stopping time of the leading vehicle. They model that the ego vehicle maintains its current speed for δ s before performing an emergency brake. The braking movement of the leading vehicle mathematically is defined as follows:

$$d_{ego}(t) = \begin{cases} d_{0,ego} + v_{ego}t & 0 \leq t \leq \delta \\ d_{0,ego} + v_{ego}t + \frac{1}{2}a_{max,ego}(t-\delta)^2 & \delta \leq t \leq t_{stop,ego} + \delta \\ d_{0,ego} + v_{ego}^2\delta - \frac{v_{ego}^2}{2a_{max,ego}} & t_{t_{stop,l}} - \delta \leq t \end{cases}, \tag{3}$$

where $t_{stop,ego} = v_{ego} / |a_{max,ego}|$ is the stopping time of the ego vehicle. The ego vehicle collides with a leading vehicle B_l if their positions are equal for some $t \geq 0$:

$$\exists t \geq 0 : d_l(t) - d_{ego}(t) = 0. \tag{4}$$

If $d_l(t) - d_{ego}(t)$ is regarded as a quadratic function, a collision means that the equation has at least one zero solution. The condition that the function has zero solution by mathematical deduction is described as:

$$d_l(\delta) \leq u_{stop,ego} \wedge |a_{max,l}| < |a_{max,ego}| \wedge v_l^* < v_{ego} \wedge t_{stop,ego} < t_l^*, \tag{5}$$

where $u_{stop,ego}$ is the stopping distance of the ego vehicle including the reaction time δ, v_l^* is the velocity of B_l at time δ after starting emergency braking, and $t_l^* = v_l^* / |a_{max,l}|$ is the stopping time of the leading vehicle. We refer interested reader to [18] for the deduction details of arithmetic manipulations and reasoning. According to that, the minimum required safe distance between the two vehicle is described by the following motion equation:

$$d_{safe,1} = \frac{(v_l + a_{max,l}\delta - v_{ego})^2}{2(a_{max,l} - a_{ego})} - v_l\delta - \frac{1}{2}a_{max,l}\delta^2 + v_{ego}\delta. \tag{6}$$

This situation describes the situation where the two vehicles have the same speed before the two vehicles have stopped. However, if the two vehicles do not have the same speed during their whole movement, the minimum safe distance required is described by the following motion equation:

$$d_{safe,2} = \frac{v_l^2}{2a_{max,l}} + v_{ego}\delta - \frac{v_{ego}^2}{2a_{ego}}. \tag{7}$$

If the ego vehicle stops after $d_l(\delta)$, that is, the position of the leading vehicle at time $t = \delta$, we denote $d_l(\delta) \leq u_{stop,ego}$. According to [18], they check whether the distance is larger than $d_{safe,1}$ in (6) when $|a_{max,l}| < |a_{max,ego}| \wedge v_l^* < v_{ego} \wedge t_{stop,ego} < t_l^*$ is true. Otherwise, they check the distance against $d_{safe,2}$ because theory in [18] suggests that there will be no collision. After introducing the relative distance $d_{rel} = d_l - d_{ego}$, we can conclude that the ego vehicle respects the safe distance to the leading vehicle B_l if the condition

$$((d_{rel} > d_{safe,1} \wedge (5)) \vee (d_{rel} > d_{safe,2} \wedge \neg(5))), \tag{8}$$

holds.

In [17], Shalev-Shwart et al. proposed the other definition of longitudinal safe distance, which is based on the ego vehicle using emergency braking with the minimum deceleration $a_{min,ego}$ after the reaction time δ. The safe distance is defined as:

$$d_{safe,3} = \frac{v_l^2}{2a_{max,l}} + \left[v_{ego}\delta + \frac{1}{2}b_{max,ego}\delta^2\right] - \frac{(v_{ego} + b_{max,ego}\delta)^2}{2a_{min,ego}}. \tag{9}$$

We use B_j to denote the vehicle at the side of the ego vehicle. Furthermore, they also proposed the minimal lateral safe distance:

$$d^{lat}_{safe,1} = \mu + \frac{2v_l + b^{lat}_{max,l}\delta}{2}\delta + \frac{(v_l + b^{lat}_{max,l}\delta)^2}{2a^{lat}_{min,l}} - \left[\frac{2v_{ego} + a^{lat}_{max,ego}\delta}{2}\delta - \frac{(v_l + a^{lat}_{max,l}\delta)^2}{2a^{lat}_{min,ego}}\right], \quad (10)$$

where μ is the minimum distance parameter, v_l and v_{ego} are lateral velocities, b^{lat}_{max} and a^{lat}_{min} are the maximum lateral acceleration within the reaction time δ and the minimum lateral deceleration after the reaction time δ, respectively. The minimum lateral distance is at least μ [17].

3 | SAFETY CONDITIONS IN THE SAFETY FRAMEWORK

3.1 | New longitudinal and lateral safe distances

Safe distance definitions of Responsibility Sensitive Safety (RSS) [17] and Rizaldi et al. [18] based on formalized traffic rules in Section 2 are efficient means for verifying the behavioral safety of self-driving vehicles. However, existing definitions of the longitudinal safe distance are not comprehensive in the sense that, for example, they ignore the possibility of a collision that may happen in between two vehicles start to decelerate and stop. Moreover, the longitudinal safe distance between the ego vehicle and the following vehicle lacks flexibility in setting, and the lateral safe distance is considered too ideal. Therefore, we presented new longitudinal and lateral safe distance in our previous work [16], which focus on neglected aspects, inflexible settings and overly idealistic assumption to supplement the existing work by considering the safe distances of each stage in detail and modeling close to real traffic situations. In this paper, we extend new longitudinal and lateral safe distances to verify behavioral safety of lane changes, overtaking and how to face new traffic participants. Thus, we review, in this subsection, the main notions and results of new safe distances. We refer interested readers to [16] for more details.

During calculating the longitudinal safe distance between the ego vehicle and the leading vehicle B_l, B_l performs an emergency brake with the maximum deceleration $a_{max,l}$, and then performs a uniform deceleration motion. The longitudinal current position of the leading vehicle B_l is described by the motion equation:

$$d_l(t) = d_{0,l} + v_l t + \frac{1}{2}a_{max,l}t^2, \quad (11)$$

where v_l is the velocity of the leading vehicle B_l. Motion curves of the ego vehicle and the leading vehicle B_l as shown in Figure 1. After the leading vehicle B_l performs an emergency brake, the current motion of the ego vehicle is divided into two stages. During the reaction time δ, the ego vehicle performs a uniform acceleration motion with the maximum acceleration $b_{max,ego}$. The longitudinal current position of the ego vehicle for any $t \leq \delta$ is described by the motion equation:

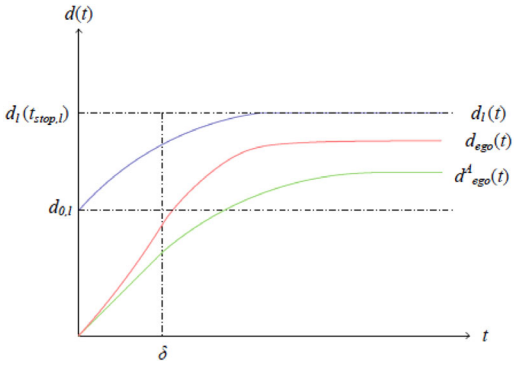


FIGURE 1 Motion curves of the ego vehicle and the leading vehicle B_l. The blue curve represents the motion curve of the leading vehicle B_l. The motion curve of the ego vehicle is shown as the red curve. The green curve represents the motion curve of the ego vehicle considered in [18] (i.e. the uniform motion performed by the ego vehicle during the reaction time δ)

$$d_{ego}(t) = v_{ego}t + \frac{1}{2}b_{max,ego}t^2, \quad (12)$$

where v_{ego} is the velocity of the ego vehicle. And after the reaction time, it performs a uniform deceleration motion with the deceleration a_{ego}. The longitudinal current position of the ego vehicle for $t > \delta$ is described by the motion equation:

$$d_{ego}(t) = v_{ego}\delta + \frac{1}{2}b_{max,ego}\delta^2 + (v_{ego} + b_{max,ego}\delta)(t-\delta) + \frac{1}{2}a_{ego}(t-\delta)^2. \quad (13)$$

When the motion considered in the reaction time becomes an acceleration motion, the speed of the ego vehicle changes quickly, and the required safe distance is greater than that in [18]. As Figure 1 shows, we can deduce that if the ego vehicle is moving at a uniform acceleration during the reaction time δ and the leading vehicle B_l performs an emergency brake with $a_{max,l}$, a collision will occur according to the original safe distance calculation.

We denote $t_{stop,ego} = \delta - (v_{ego} + b_{max,ego}\delta)/a_{ego}$ and $t_{stop,l} = -v_l/a_{max,l}$ as the stopping times of the vehicles. The maximum and minimum value of $t_{stop,ego}$ and $t_{stop,l}$ are denoted $t_{stop,max}$ and $t_{stop,min}$. The distance function between the leading vehicle B_l and the ego vehicle is defined as:

$$f(t) = d_l(t) - d_{ego}(t). \quad (14)$$

As long as it is guaranteed that at any time $t \in [0, t_{stop,max}]$, the condition $f(t) > 0$ always holds, and it can be ensured that the ego vehicle will not collide with the leading vehicle B_l.

According to the stopping time $t_{stop,l}$ of the leading vehicle B_l, we divide the motion into two situations. The first situation is the case of $\delta \geq t_{stop,l}$, which describes the situation where the ego vehicle fails to respond in reaction time δ after the leading vehicle B_l performs an emergency brake with the maximum deceleration $a_{max,l}$. We use δ^* to denote this longer reaction time (i.e., $\delta^* > \delta$). The distance function $f(t)$ is divided into the following four cases:

- If $t_{stop,l} \geq t \geq 0$, then

$$f(t) = d_{0,l} + v_l t + \frac{1}{2} a_{max,l} t^2 - \left(v_{ego} t + \frac{1}{2} b_{max,ego} t^2 \right). \quad (15)$$

- If $\delta^* \geq t \geq t_{stop,l}$, then

$$f(t) = d_{0,l} + \frac{v_l^2}{2a_{max,l}} - \left(v_{ego} t + \frac{1}{2} b_{max,ego} t^2 \right). \quad (16)$$

- If $t_{stop,ego} \geq t \geq \delta^*$, then

$$f(t) = d_{0,l} + \frac{v_l^2}{2a_{max,l}} - \left[v_{ego} t + b_{max,ego} \delta^* \left(t - \frac{\delta^*}{2} \right) + \frac{1}{2} a_{ego} (t - \delta^*)^2 \right]. \quad (17)$$

- If $t \geq t_{stop,ego}$, then

$$f(t) = d_{0,l} + \frac{v_l^2}{2a_{max,l}} - \left[v_{ego} \delta^* + \frac{1}{2} b_{max,ego} (\delta^*)^2 \right] + \frac{(v_{ego} + b_{max,ego} \delta^*)^2}{2a_{ego}}. \quad (18)$$

After solving $f(t) > 0$, we get two longitudinal safe distances. The first safe distance for $t_{stop,l} \geq t \geq 0$ is as follows:

$$d_{safe,1} = \frac{v_l^2}{2a_{max,l}} + v_{ego} t_{stop,l} + \frac{1}{2} b_{max,ego} t_{stop,l}^2. \quad (19)$$

The second safe distance for $t \geq t_{stop,l}$ is as follows:

$$d_{safe,2} = \frac{v_l^2}{2a_{max,l}} + \left[v_{ego} \delta^* + \frac{1}{2} b_{max,ego} (\delta^*)^2 \right] - \frac{(v_{ego} + b_{max,ego} \delta^*)^2}{2a_{ego}}. \quad (20)$$

The second situation is the case of $\delta < t_{stop,l}$. This situation describes that after the leading vehicle B_l performs an emergency brake with the maximum deceleration $a_{max,l}$, the ego vehicle performs an emergency brake with the deceleration a_{ego} after the reaction time δ. This is also a generally accepted view during calculating the longitudinal safe distance.

The distance function $f(t)$ is divided into the following five cases:

- If $\delta \geq t \geq 0$, then the distance function $f(t)$ is the same as (15).
- If $t_{stop,min} > t > \delta$, then

$$f(t) = d_{0,l} + v_l t + \frac{1}{2} a_{max,l} t^2 - \left[v_{ego} t + b_{max,ego} \delta \left(t - \frac{\delta}{2} \right) + \frac{1}{2} a_{ego} (t - \delta)^2 \right]. \quad (21)$$

- If $t_{stop,ego} > t \geq t_{stop,l}$, then the distance function $f(t)$ is the same as (17) except that δ^* in (17) is replaced by δ.
- If $t_{stop,l} > t \geq t_{stop,ego}$, then

$$f(t) = d_{0,l} + v_l t + \frac{1}{2} a_{max,l} t^2 - \left(v_{ego} \delta + \frac{1}{2} b_{max,ego} \delta^2 \right) + \frac{(v_{ego} + b_{max,ego} \delta)^2}{2a_{ego}}. \quad (22)$$

- If $t \geq t_{stop,max}$, then the distance function $f(t)$ is the same as (18) except that δ^* in (18) is replaced by δ.

After solving $f(t) > 0$, we get some longitudinal safe distances. To simplify, we denote $c_1 = (v_l - v_{ego})/(b_{max,ego} - a_{max,l})$, $c_2 = (v_l + a_{ego}\delta - v_{ego} - b_{max,ego}\delta)/(a_{ego} - a_{max,l})$, and $c_3 = (v_l + a_{ego}\delta - v_{ego} - b_{max,ego}\delta)$.

- If $\delta \geq t \geq 0$, there are two cases. If $c_1 \geq \frac{\delta}{2}$, then the collision will not happen. If $c_1 < \frac{\delta}{2}$, then

$$d_{safe,1} = (v_{ego} - v_l)\delta - \frac{1}{2}(a_{max,l} - b_{max,ego})\delta^2. \quad (23)$$

- If $t_{stop,min} > t > \delta$ and $a_{max,l} < a_{ego}$, there are two cases. If $c_2 \leq (\delta + t_{stop,min})/2$, then

$$d_{safe,2} = \frac{1}{2}(a_{ego} - b_{max,ego})\delta^2 - (v_l + a_{ego}\delta - v_{ego} - b_{max,ego}\delta) t_{stop,min} - \frac{1}{2}(a_{max,l} - a_{ego}) t_{stop,min}^2. \quad (24)$$

If $c_2 > (\delta + t_{stop,min})/2$, then the safe distance is the same as (23).

- If $t_{stop,min} > t > \delta$ and $a_{max,l} > a_{ego}$, there are three cases. If $c_2 \in [\delta, t_{stop,min}]$, then

$$d_{safe,3} = \frac{(v_l + a_l\delta - v_{ego} - b_{max,ego}\delta)^2}{2(a_{max,l} - a_{ego})} - v_l\delta - \frac{1}{2} a_{max,l}\delta^2 + v_{ego}\delta + \frac{1}{2} b_{max,ego}\delta^2. \quad (25)$$

TABLE 1 Longitudinal safe distance between the ego vehicle and the leading vehicle

Condition	Safe distance
$\delta \geq t \geq 0 \wedge c_1 \geq \frac{\delta}{2}$	0
$t_{stop,min} > t > \delta \wedge a_{max,l} = a_{ego} \wedge c_3 \geq 0$	
$\delta \geq t \geq 0 \wedge c_1 < \frac{\delta}{2}$	$d_{safe,1}$
$t_{stop,min} > t > \delta \wedge a_{max,l} < a_{ego} \wedge c_2 > (\delta + t_{stop,min})/2$	
$t_{stop,min} > t > \delta \wedge a_{max,l} > a_{ego} \wedge c_2 < \delta$	
$t_{stop,min} > t > \delta \wedge a_{max,l} < a_{ego} \wedge c_2 \leq (\delta + t_{stop,min})/2$	$d_{safe,2}$
$t_{stop,min} > t > \delta \wedge a_{max,l} > a_{ego} \wedge c_2 > t_{stop,min}$	
$t_{stop,min} > t > \delta \wedge a_{max,l} = a_{ego} \wedge c_3 < 0$	
$t_{stop,min} > t > \delta \wedge a_{max,l} > a_{ego} \wedge c_2 \in [\delta, t_{stop,min}]$	$d_{safe,3}$
$t \geq t_{stop,min}$	$d_{safe,4}$

If $c_2 < \delta$, then the safe distance is the same as (23). If $c_2 > t_{stop,min}$, then the safe distance is the same as (24).

- If $t_{stop,min} > t > \delta$ and $a_{max,l} = a_{ego}$, there are two cases. If $c_3 \geq 0$, then the collision will not happen. If $c_3 < 0$, then the safe distance is the same as (24).
- If $t \geq t_{stop,min}$, then the safe distance $d_{safe,4}$ is the same as (20) except that δ^* in (20) is replaced by δ.

We summarizes these safe distances and corresponding conditions mentioned above into Table 1.

During calculating the longitudinal safe distance between the ego vehicle and the following vehicle B_f, B_f performs an emergency brake with the maximum deceleration $a_{max,f}$, and then performs a uniform deceleration motion. The longitudinal current position of the following vehicle B_f is described by the motion equation:

$$d_f(t) = v_f t + \frac{1}{2} a_{max,f} t^2, \tag{26}$$

where v_f is the velocity of the following vehicle B_f. Motion curves of the ego vehicle and the following vehicle B_f as shown in Figure 2.

If a collision occurs and the ego vehicle has respected the traffic rules at all times, considering the question of liability, a view in [21] is that another traffic participant must have violated the rules and thus caused the collision. Therefore, in the previous work, the planner of the system for self-driving cars directly set the safe distance between the ego vehicle and the following vehicle B_f to be the same as the distance between the ego vehicle and the leading vehicle B_l. However, on real road traffic, if there is no vehicle in front of the ego vehicle, there will be a more optimized and flexible design of the safe distance. If the following vehicle B_f cannot respect the longitudinal safe distance to the ego vehicle, the ego vehicle can accelerate to the maximum velocity. If there is a leading vehicle in the source lane, a lane change becomes a better choice when the traffic conditions in multiple lane support lane change.

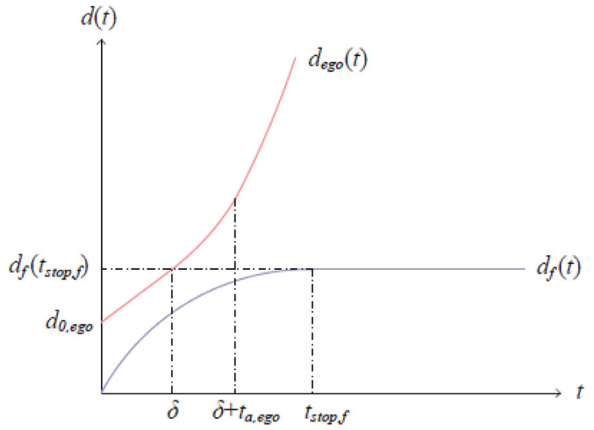


FIGURE 2 Motion curves of the ego vehicle and the following vehicle B_f when there is no leading vehicle B_l of the ego vehicle. The blue curve represents the motion curve of the following vehicle B_f. The motion curve of the ego vehicle is shown as the red curve

In the traffic rules and the existing autonomous driving research, the safe distance between the ego vehicle and the following vehicle is mainly maintained by the following vehicle. Once the following vehicle cannot respect a safe distance to the ego vehicle, it means that a collision will definitely occur if the ego vehicle performs emergency braking. We consider that it is possible for the ego vehicle to actively escape the collision hazard in this situation. For example, the ego vehicle can accelerate in a situation where there is no leading vehicle, increasing the safe distance from the following vehicle to avoid or reduce the collision. The following vehicle still respects the safe distance to the ego vehicle, and setting this new safe distance actually adds a layer of protection to the ego vehicle's own safety and enhances its ability to resist uncertain behaviors of the following vehicle. This approach will not conflict with the application of the original safe distance.

When there is no leading vehicle B_l in front of the ego vehicle, we introduce new longitudinal safe distance and the dangerous distance (i.e., when the distance between the two vehicles is less than the dangerous distance, a collision must occur.) between the ego vehicle and the following vehicle B_f. After the following vehicle B_f performs an emergency brake, the current motion of the ego vehicle is divided into three stages. During the reaction time δ, the ego vehicle performs a uniform motion. The longitudinal current position of the ego vehicle for any $t \leq \delta$ is described by the motion equation:

$$d_{ego}(t) = d_{0,ego} + v_{ego} t. \tag{27}$$

After the reaction time δ, it performs a uniform acceleration motion with the maximum acceleration $b_{max,ego}$. The time for the ego vehicle to accelerate from the current velocity v_{ego} to the maximum velocity $v_{max,ego}$ with the maximum acceleration $b_{max,ego}$ is denoted as $t_{a,ego} = (v_{max,ego} - v_{ego})/b_{max,ego}$. The longitudinal current position of the ego vehicle for $\delta + t_{a,ego} > t > \delta$ is described by the motion

equation:

$$d_{ego}(t) = d_{0,ego} + v_{ego}t + \frac{1}{2}b_{max,ego}(t-\delta)^2. \tag{28}$$

Once the ego vehicle accelerates to the maximum velocity $v_{max,ego}$, it will perform a uniform motion. The longitudinal current position of the ego vehicle for $\delta + t_{a,ego} > t > \delta$ is described by the motion equation:

$$d_{ego}(t) = d_{0,ego} + v_{ego}(\delta + t_{a,ego}) + \frac{1}{2}b_{max,ego}t_{a,ego}^2 + v_{max,ego}(t - \delta - t_{a,ego}). \tag{29}$$

We use $t_{stop,f} = \frac{v_f}{a_{max,f}}$ to denote the stopping time of the following vehicle B_f. The distance function between the following vehicle B_f and the ego vehicle is defined as:

$$g(t) = d_{ego}(t) - d_f(t). \tag{30}$$

As long as it is guaranteed that at any time $t \in [0, t_{stop,f}]$, the condition $g(t) > 0$ always holds, and it can be ensured that the ego vehicle will not collide with the following vehicle B_f. Therefore, $d_{0,ego}$ such that $g(t) > 0$ is the minimal longitudinal safe distance d_{safe}. The distance function $f(t)$ is divided into the following five cases:

- If $\delta \geq t_{stop,f} > t \geq 0$ or $t_{stop,f} > \delta \geq t \geq 0$, then

$$g(t) = d_{0,ego} + v_{ego}t - \left(v_f t + \frac{1}{2}a_{max,f}t^2\right). \tag{31}$$

- If $\delta \geq t \geq t_{stop,f} \geq 0$, then

$$g(t) = d_{0,ego} + v_{ego}t + \frac{v_f^2}{2a_{max,f}}. \tag{32}$$

- If $\delta + t_{a,ego} \geq t_{stop,f} > t > \delta$ or $t_{stop,f} > \delta + t_{a,ego} \geq t > \delta$, then

$$g(t) = d_{0,ego} + v_{ego}t + \frac{1}{2}b_{max,ego}(t-\delta)^2 - \left(v_f t + \frac{1}{2}a_{max,f}t^2\right). \tag{33}$$

- If $\delta + t_{a,ego} > t \geq t_{stop,f} > \delta$, then

$$g(t) = d_{0,ego} + v_{ego}t + \frac{1}{2}b_{max,ego}(t-\delta)^2 + \frac{v_f^2}{2a_{max,f}}. \tag{34}$$

- If $t_{stop,f} \geq t \geq \delta + t_{a,ego}$, then

$$g(t) = d_{0,ego} + v_{ego}(\delta + t_{a,ego}) + \frac{1}{2}b_{max,ego}t_{a,ego}^2 + v_{max,ego}(t - \delta - t_{a,ego}) - \left(v_f t + \frac{1}{2}a_{max,f}t^2\right). \tag{35}$$

After solving $g(t) > 0$, we get some longitudinal safe distances between the following vehicle B_f and the ego vehicle. To simplify, we denote $z_1 = (v_{ego} - v_f)/a_{max,f}$, $z_2 = (v_f + a_{max,f}\delta - v_{ego})/(b_{max,ego} - a_{max,f})$ and $z_3 = (v_{max,ego} - v_f)/a_{max,f}$.

- If $\delta \geq t_{stop,f} > t \geq 0$, there are three cases. If $v_{ego} \geq v_f$, then the collision will not happen. If $v_{ego} < v_f$ and $z_1 \geq t_{stop,f}$, then

$$d_{safe,1} = -\frac{v_f^2}{2a_{max,f}} - v_{ego}t_{stop,f}. \tag{36}$$

If $v_{ego} < v_f$ and $z_1 < t_{stop,f}$, then

$$d_{safe,2} = -\frac{(v_{ego} - v_f)^2}{2a_{max,f}}. \tag{37}$$

- If $t_{stop,f} > \delta \geq t \geq 0$, there are three cases. If $v_{ego} \geq v_f$, then the collision will not happen. If $v_{ego} < v_f$ and $z_1 \geq \delta$, then

$$d_{safe,3} = (v_f - v_{ego})\delta + \frac{1}{2}a_{max,f}\delta^2. \tag{38}$$

If $v_{ego} < v_f$ and $z_1 < t_{stop,f}$, then the safe distance is the same as (37).

- If $\delta \geq t \geq t_{stop,f} \geq 0$, then the safe distance is the same as (36).
- If $\delta + t_{a,ego} \geq t_{stop,f} > t > \delta$, then there are three cases. If $z_2 \leq \delta$, then the safe distance $d_{safe,4}$ is the same as (38). If $t_{stop,f} > z_2 > \delta$, then

$$d_{safe,4} = \frac{(v_f + b_{max,ego}\delta - v_{ego})^2}{2(b_{max,ego} - a_{max,f})} - \frac{1}{2}b_{max,ego}\delta^2. \tag{39}$$

If $z_2 \geq t_{stop,f}$, then

$$d_{safe,5} = -v_{ego}t_{stop,f} - \frac{1}{2}b_{max,ego}(t_{stop,f} - \delta)^2 - \frac{v_f^2}{2a_{max,f}}. \tag{40}$$

- If $\delta + t_{a,ego} > t \geq t_{stop,f} > \delta$, then the safe distance is the same as (40).
- If $t_{stop,f} > \delta + t_{a,ego} \geq t > \delta$, then there are three cases. If $z_2 \leq \delta$, then the safe distance is the same as (38). If $\delta + t_{a,ego} > z_2 > \delta$, then the safe distance is the same as (39). If $z_2 \geq \delta + t_{a,ego}$, then

$$d_{safe,6} = (v_f - v_{ego})(\delta + t_{a,ego}) - \frac{1}{2}b_{max,ego}t_{a,ego}^2 + \frac{1}{2}a_{max,f}(\delta + t_{a,ego})^2. \tag{41}$$

- If $t_{stop,f} \geq t \geq \delta + t_{a,ego}$, then there are three cases. If $z_3 < \delta + t_{a,ego}$, then the safe distance is the same as (41). If

TABLE 2 Longitudinal safe distance between the ego vehicle and the following vehicle

Condition	Safe distance
$\delta \geq t_{stop,f} > t \geq 0 \wedge v_{ego} \geq v_f$	0
$t_{stop,ego} > \delta \geq t \geq 0 \wedge v_{ego} \geq v_f$	
$\delta \geq t_{stop,f} > t \geq 0 \wedge v_{ego} < v_f \wedge z_1 \geq t_{stop,f}$	$d_{safe,1}$
$\delta \geq t \geq t_{stop,f} \geq 0$	
$\delta \geq t_{stop,f} > t \geq 0 \wedge v_{ego} < v_f \wedge z_1 < t_{stop,f}$	$d_{safe,2}$
$t_{stop,f} > \delta \geq t \geq 0 \wedge v_{ego} < v_f \wedge z_1 < t_{stop,f}$	
$t_{stop,f} > \delta \geq t \geq 0 \wedge v_{ego} < v_f \wedge z_1 \geq \delta$	$d_{safe,3}$
$\delta + t_{a,ego} \geq t_{stop,f} > t > \delta \wedge z_2 \leq \delta$	
$t_{stop,f} > \delta + t_{a,ego} \geq t > \delta \wedge z_2 \leq \delta$	
$\delta + t_{a,ego} \geq t_{stop,f} > t > \delta \wedge t_{stop,f} > z_2 > \delta$	$d_{safe,4}$
$t_{stop,f} > \delta + t_{a,ego} \geq t > \delta \wedge \delta + t_{a,ego} > z_2 > \delta$	
$\delta + t_{a,ego} \geq t_{stop,f} > t > \delta \wedge z_2 \geq t_{stop,f}$	$d_{safe,5}$
$\delta + t_{a,ego} > t \geq t_{stop,f} > \delta$	
$t_{stop,f} > \delta + t_{a,ego} \geq t > \delta \wedge z_2 \geq \delta + t_{a,ego}$	$d_{safe,6}$
$t_{stop,f} \geq t \geq \delta + t_{a,ego} \wedge z_3 < \delta + t_{a,ego}$	
$t_{stop,f} \geq t \geq \delta + t_{a,ego} \wedge t_{stop,f} > z_3 > \delta + t_{a,ego}$	$d_{safe,7}$
$t_{stop,f} \geq t \geq \delta + t_{a,ego} \wedge z_3 \geq t_{stop,f}$	$d_{safe,8}$

$t_{stop,f} > z_3 > \delta + t_{a,ego}$, then

$$d_{safe,7} = -\frac{(v_{max,ego} - v_f)^2}{2a_{max,f}} - v_{ego}\delta - \frac{1}{2}(v_{ego} + v_{max,ego})t_{a,ego} + v_{max,ego}(\delta + t_{a,ego}). \tag{42}$$

If $z_3 \geq t_{stop,f}$, then

$$d_{safe,8} = -v_{ego}\delta - \frac{1}{2}(v_{ego} + v_{max,ego})t_{a,ego} - v_{max,ego}(t_{stop,f} - \delta - t_{a,ego}) - \frac{v_f^2}{2a_{max,f}}. \tag{43}$$

We summarizes these safe distances and corresponding conditions mentioned above into Table 2.

The ideal minimal lateral safe distance in Section 2 is that the ego vehicle and the vehicle B_j in adjacent lanes accelerate with the maximum lateral acceleration $b^{lat}_{max,ego}$ and $b^{lat}_{max,j}$ within the reaction time δ, and decelerate with the minimum lateral deceleration $a^{lat}_{min,ego}$ and $a^{lat}_{min,j}$ after the reaction time δ. However, due to the limitation of the human driver's viewing angle during the driving, the vehicle B_j may ignore dangerous situation and fail to slow down in time. The worst state is that the vehicle B_j has not take any measures to avoid or mitigate a potential collision (i.e. it still uses the maximum lateral acceleration $b^{lat}_{max,j}$ to approach the ego vehicle laterally). The lateral current position of the vehicle B_j is described by the motion equation:

$$d^{lat}_j(t) = d^{lat}_{0,j} - \left(v^{lat}_j t + \frac{1}{2}b^{lat}_{max,j}t^2\right), \tag{44}$$

where v^{lat}_j is the lateral velocity of the vehicle B_j. Motion curves of the ego vehicle and the adjacent vehicle B_j as shown in Figure 3. The ego vehicle decelerates with the maximum lateral deceleration $a^{lat}_{min,ego}$ after the reaction time δ. The lateral current position of the ego vehicle is described by the motion equation:

$$d^{lat}_{ego}(t) = v^{lat}_{ego}\delta + \frac{1}{2}b^{lat}_{max,ego}\delta^2 + \left(v^{lat}_{ego} + b^{lat}_{max,ego}\delta\right)(t-\delta) + \frac{1}{2}a^{lat}_{min,ego}(t-\delta)^2, \tag{45}$$

where v^{lat}_{ego} is the lateral velocity of the ego vehicle. The distance function between the vehicle B_j and the ego vehicle is defined as:

$$h(t) = d^{lat}_j(t) - d^{lat}_{ego}(t). \tag{46}$$

If $h(t) > \mu$, then the lateral safe distance between the vehicle B_j and the ego vehicle is satisfied. After solving$h(t) > \mu$, We obtain two lateral safe distances. To simplify, we denote $t^{lat}_{ego} = -(v^{lat}_{ego} + b^{lat}_{max,ego}\delta)/a^{lat}_{min,ego}$ and $w = -(v^{lat}_{ego} + b^{lat}_{max,ego}\delta - a^{lat}_{min,ego}\delta + v^{lat}_j)/(b^{lat}_{max,j} + a^{lat}_{min,ego})$. The first safe distance for $b^{lat}_{max,j} \leq -a^{lat}_{min,ego}$ is as follows:

$$d^{lat}_{safe,1} = \mu + v^{lat}_j t^{lat}_{ego} + \frac{1}{2}b^{lat}_{max,j}\left(t^{lat}_{ego}\right)^2 + d^{lat}_{ego}\left(t^{lat}_{ego}\right). \tag{47}$$

The second safe distance for $b^{lat}_{max,j} > -a^{lat}_{min,ego}$ have two cases. If $w > t^{lat}_{ego}$, then the safe distance d^{lat}_{safe} is the same as (47). If

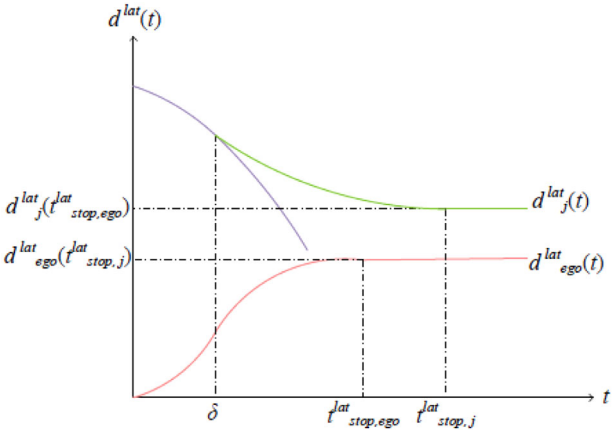


FIGURE 3 Motion curves of the ego vehicle and the vehicle B_j. The blue curve and the green curve represent the motion curve of the adjacent vehicle B_j we consider and that of the adjacent vehicle B_j considered in [18], respectively. The motion curve of the ego vehicle is shown as the red curve

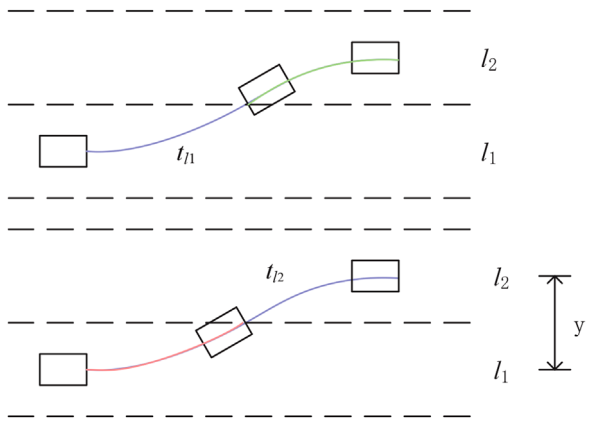


FIGURE 4 Lane change maneuvers

$w \leq t^{lat}_{ego}$, then

$$d^{lat}_{safe,2} = \mu - \frac{\left(v^{lat}_{j} + v^{lat}_{ego} + b^{lat}_{max,ego}\delta - a^{lat}_{min,ego}\delta\right)^2}{2\left(b^{lat}_{max,j} + b^{lat}_{max,ego}\right)} + \frac{1}{2}a^{lat}_{min,ego}\delta^2 - \frac{1}{2}b^{lat}_{max,ego}\delta^2. \tag{48}$$

3.2 | Lane change maneuvers and overtaking

Safe overtaking is based on safe lane changes, which can be regarded as two continuous lane changes and one acceleration motion. We divide the types of continuous lane changes into the same direction (change the lane to the left lane twice) and the different directions (change the lane to the left lane and then to the right lane). Here, overtaking are two continuous lane changes in different directions. Therefore, we can verify the safe overtaking by considering the safety of lane change maneuvers of self-driving cars.

Let y is the lateral distance between the center of current lane l_1 and the center of target lane l_2, where y is the distance needed to change a lane. We denote δ_s as the reaction time needed to execute steering. We divide the required time t_s to perform a steering maneuver into two parts. We introduce t_{l_1} and t_{l_2} as the time intervals during which the occupancy of the ego vehicle is located in lane l_1 and l_2, respectively. As shown in Figure 4, we take the time to determine the overtaking as the starting time of t_{l_1}, the steering angle starts to change after the reaction time δ_s, and the time when the center position of the rear of the ego vehicle reaches the center line is used as the end time of t_{l_1}. As shown in the blue line in Figure 4, we take the time that the center position of the front of the ego vehicle reaches the center line as the starting time of t_{l_2}, and the time when the steering angle returns to the front is the end time of t_{l_2}.

In the previous work, in order to guarantee safety of lane change maneuvers, the ego vehicle always respects a safe distance to the leading and following vehicles during the planned trajectory. The safe free space S^t of the ego vehicle for a point in time $t \geq 0$ is defined as

$$S^t = \{d \in \mathbb{R} \mid d_f(t) + d_{safe,f}(t) < d < d_l(t) - d_{safe,l}(t)\}. \tag{49}$$

To verify the safety, the ego vehicle needs to be driven within the respective safe spaces, S^t_1 in l_1 and S^t_2 in l_2, at any time $t \leq t_s$ during the lane change, that is

$$\forall t \leq t_{l_1} : d_{ego}(t) \in S^t_{l_1} \wedge \forall t - t_{l_1} \leq t_{l_2} : d_{ego}(t) \in S^t_{l_2}. \tag{50}$$

If no new traffic participant appears and affects the planned trajectories during the lane change, the basic condition for the ego vehicle to change lanes is to respect the required safe distance to other vehicles in the l_1 and l_2 lanes. Furthermore, the leading vehicle B_l on l_1 or l_2 is preferably in a constant speed or accelerating state. Otherwise, if the leading vehicle B_l suddenly decelerates, there is a safety hazard. Similarly, the following vehicle B_f on l_1 or l_2 is preferably in a constant speed or decelerating state. Otherwise, if the following vehicle B_f suddenly accelerates, there is also a safety hazard.

For the situation where there is only the leading vehicle or only the following car in lanes l_1 and l_2, if the leading vehicle suddenly decelerates or the following car suddenly accelerates, the ego vehicle can adjust its speed to compensate for a sudden deceleration (even for emergency braking) or acceleration during the lane change. The most complicated situation is that there are both the leading and following vehicles in lane l_1 or l_2.

a) When there are the leading and following vehicles in the lane l_1, the ego vehicle must respect safe distances to the leading vehicle B_l and the following vehicle B_f before starting to change lanes. The speed v_{ego} is decomposed into the lateral speed $v_{ego,y}$ and the longitudinal speed $v_{ego,x}$ during the lane change. When $t \leq t_{l_1}$, $v_{ego,x}$ is decreasing, and the longitudinal distance $d_l - d_{ego}$ between the leading vehicle B_l and the ego vehicle becomes larger, the longitudinal distance $d_{ego} - d_f$ between the following vehicle B_f and the ego vehicle is reduced, which brings a risk of a collision with the following vehicle B_f. The ego vehicle need increase $d_{ego} - d_f$ by accelerating (increasing $v_{ego,x}$) in time to respect a safe distance to the following vehicle B_f. However, the longitudinal distance $d_{ego} - d_f$ cannot be too large, otherwise $d_l - d_{ego}$ will decrease, bringing a risk of a collision with the leading vehicle B_l. Therefore, when the ego vehicle is about to leave the boundary of lane l_1, $d_{ego} - d_f$ must satisfy the safe distance.
b) When there are the leading and following vehicles in the lane l_2, the ego vehicle must respect safe distances to the leading vehicle B_l and the following vehicle B_f before entering the boundary of the lane l_2. Similarly, the ego vehicle's speed v_{ego} is decomposed into the lateral speed $v_{ego,y}$ and the longitudinal speed $v_{ego,x}$ during the lane change. When $t - t_{l_1} \leq t_{l_2}$, $v_{ego,x}$ increases, the longitudinal distance $d_l - d_{ego}$ decreases, the longitudinal distance $d_{ego} - d_f$ increases, which brings a risk of a collision with the leading vehicle B_l. The ego vehicle need increase $d_l - d_{ego}$ by decelerating (reducing $v_{ego,x}$) in time to respect a safe distance to the following vehicle B_l.

However, the longitudinal distance $d_{ego} - d_f$ cannot be too large, otherwise $d_{ego} - d_f$ will decrease, which will bring a risk of a collision with the following vehicle B_f. When the ego vehicle just reaches the boundary of the lane l_2, $d_{ego} - d_f$ must satisfy the required safe distance, and when the lane change is completed, $d_l - d_{ego}$ must satisfy the required safe distance.

In the target lane l_2, if the leading vehicle B_l decelerates and the following vehicle B_f accelerates, the ego vehicle continues to track. Once the ego vehicle cannot respect safe distances to the leading vehicle B_l and the following vehicle B_f at the same time, it immediately abandons the lane change and returns to the original lane l_1 or changes the lane to the adjacent lane l_4 of lane l_2 (if there is a lane change opportunity in lane l_4). If new traffic participants appear, and the original lane l_1 and lane l_4 (if they exist) are occupied, the ego vehicle cannot change lanes and has to perform an emergency brake maneuver.

New traffic participants often appear in the driving of self-driving cars, and they may affect the predicted behavior and planned trajectory, as well as during lane change maneuvers.

a) When $t \leq t_{l_1}$, there are two cases. If there is a new traffic participant in lane l_1 and it breaks into the safe space $S^t_{l_1}$ of the ego vehicle, the ego vehicle can speed up the lane change or start emergency braking. If a new traffic participant enters lane l_2 first or is about to enter lane l_2, we check whether the safe distance is respected, if respected, the ego vehicle continues to change lanes, if not respected, the ego vehicle accelerates to become its leading vehicle or slow down to become its following vehicle, and finds other opportunities to change lanes.
b) When $t - t_{l_1} \leq t_{l_2}$, there are also two cases. If the lane change fails, the ego vehicle thus wants to return to the original lane l_1. But at this same time, there are new traffic participants in lane l_1, for example, the safe space $S^t_{l_1}$ of the ego vehicle is already occupied by other vehicle, or the current traffic situation is changed due to the insertion of a new vehicle. The ego vehicle can accelerate to become its leading vehicle and then change lanes or change lanes to the adjacent lane l_4 of lane l_2. If the lane change is impossible, the emergency brake will be activated. If there is a new traffic participant in lane l_2, the current traffic situation is changed. The ego vehicle can decelerate or accelerate to respect the safe distance to it, or changes lanes if the safe distance cannot be respect, or performs an emergency brake maneuver if there is no opportunity for the lane change maneuver.

If the ego vehicle fails to change lanes, how to safely return to the original lane l_1 becomes a crucial issue. When $t \leq t_{l_1}$, the ego vehicle can straighten the steering angle and continue to drive on lane l_1. If $t - t_{l_1} \leq t_{l_2}$, the self-driving system first checks whether there is a chance to change lanes. If there is an opportunity, the ego vehicle will immediately start the lane change. If the safe space in the original lane l_1 is occupied by other vehicles, the ego vehicle can turn on the turn signal to convey the lane change intention to the following vehicle in lane l_1. We can track whether the following vehicle will give way politely. If the following vehicle refuses to coordinate, the ego vehicle can create an opportunity to change lanes by accelerating or decelerating. If the lane change is impossible all the time, the ego vehicle only slows down and try to restore a safe distance with the leading vehicle, otherwise it has to start emergency brake.

How the following vehicle should react to the leading vehicle is also an important problem, but it was ignored in previous work. In order to solve this problem, we propose some safety strategies.

a) For the ego vehicle and the leading vehicle B_l in lane l_1, there are two cases. When the ego vehicle receives the lane change instruction from B_l, if the self-driving system detects that B_l has turned on the turn signal to convey its lane change intention, the ego vehicle should cooperate; if the ego vehicle has started to change lanes, B_l starts to change lanes again and occupies the safe space $S^t_{l_2}$ of the ego vehicle, which belongs a misbehavior of B_l.
b) For the ego vehicle and the leading vehicle B_l in lane l_4, there are also three cases. If the leading vehicle B_l has entered lane l_2 before the ego vehicle, we consider the safe distance, if it can be respected, continue to change lanes, if not, give up this lane change. If the ego vehicle and B_l enter l_2 at the same time, we check whether the safe distance is respected, if it is respected, the ego vehicle continues to change lanes, if not respected, the ego vehicle tries to decelerate to restore the safe distance, and if it still fails to recover, the ego vehicle has to give up this lane change. If the ego vehicle has completely entered l_2 and B_l is still close to l_2, which belongs a misbehavior of B_l, and the treatment is the same as the second case.

The above process reflects the rationality of the ego vehicle's trajectory planning and the accuracy of the prediction model. When the safe distance is unsatisfied, we keep the tracking to observe whether the ego vehicle implements feasible solutions to avoid or mitigate a potential collision in time. It can reflect the sensitivity, implementability and resilience of the self-driving system. Therefore, a safe self-driving system should ensure that the ego vehicle responds sensitively to the deceleration of B_l and the acceleration of B_f during the lane change, and avoids the risk of collision. An overtaking behavior of the ego vehicle can be regarded as two consecutive lane changes and an acceleration process. As long as it is ensured that the safety requirements are satisfied during the two consecutive lane changes, it can be determined that the overtaking behavior of the ego vehicle is safe.

3.3 | New traffic participants

A safe lane change guarantees that no collision occurs according to traffic rules and RSS concept [17], while a single vehicle cannot ensure that it will never be involved in a collision [22]. In fact, self-driving cars often encounter some disturbance objects, which suddenly appear in traffic scenarios. The new

traffic participant refers to the new physical object that is sensed by the sensors of the self-driving vehicle, which can be a vehicle, a pedestrian or an animal. When new traffic participants appear, the current traffic environment of the ego vehicle may be changed, which may cause a potential collision, such as a corrected steering angle incident of Didi's self-driving car. When the interviewer was riding in a Didi self-driving car, there was a takeover. The Didi's takeover occurred at an intersection when a laterally approaching vehicle suddenly drove into the lane. The security officer carried out a dynamic takeover due to safety considerations. The dynamic takeover (vehicle from moving to stationary) means that there are potential collision risks in the driving process of the self-driving car, and the safety officer will immediately take over the ego vehicle. In this incident, due to a cut-in of a new traffic participant, the vehicle B_{new}, the lateral safe distance between the ego vehicle ego and the vehicle B_{new} is not respected. If the ego vehicle cannot take measures in time, a collision may occur, which will eventually trigger the security officer's human intervention.

In the above case, the ego vehicle should detect other vehicles within a certain range that do not respect the lateral safe requirements, and take feasible measures in time to increase the lateral safe distance and eliminate the risk of collision. Within a certain range here, from the traffic laws and the perspective of human driving, when considering the lateral safe distance, the vehicle should be at the same level and in front. It also inspired by the longitudinal safe distance, the safe distance mainly depends on the following vehicle B_f. If each following vehicle pays attention to keeping a safe distance from its leading vehicle, then the following vehicle B_f will be responsible for the collision. Therefore, a successful system for self-driving cars should have the ability to respond in time, when new traffic participants appear and interfere with the predicted behavior of the ego vehicle.

The safe distance of the ego vehicle with respect to the new traffic participant is flexibly set according to the type of the specific participant. Our safety framework for new traffic participant here mainly takes vehicles as an example, so the safe distance mentioned here is the new longitudinal and lateral safe distance mentioned in Section 3.1. For pedestrians, the corresponding safe distance can be set in combination with the pedestrian behavior prediction model, which is also our future work.

An incident of correcting the steering angle of Didi's self-driving car is also a sudden incident about new traffic participants not being "passed", which inspired us to face the challenge. In order to solve this problem, we propose the following strategy.

a) When a vehicle B_{new} as the new vehicle participant operates accidentally (brakes too late and cannot reverse), it may trigger a collision. The ego vehicle should evade in time to protect itself, adjust the (lateral or longitudinal) distance with the vehicle B_{new} to maintain a safe distance. Because the vehicle B_{new} cannot reverse at this time, it can only be supplemented by the ego vehicle.
b) If the roles are reversed and the ego vehicle is in the position of the vehicle B_{new}, first keep the lateral safe distance, and then keep the longitudinal safe distance. Note that when the ego vehicle merges into the target lane after turning, the required safe distance d_{safe} between the ego vehicle and the following car B_f in the target lane must be respect.

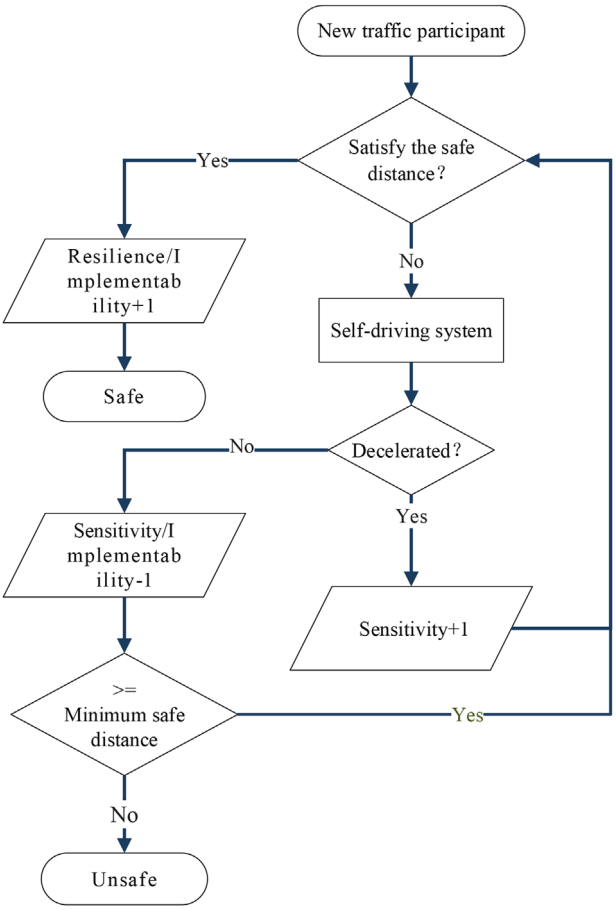


FIGURE 5 A verification framework for new traffic participant

In actual traffic, these traffic participants may be children playing on the side of the road, pedestrians or animals who want to cross the road, or goods scattered from the leading vehicle. These various traffic participants who are difficult to predict their activity trajectories bring difficulties to safety verification. To overcome these difficulties, we propose a verification framework for new traffic participants (shown in Figure 5), which can track new traffic participants with different safe distances and issue an early warning to avoid potential collisions when the current conditions cannot satisfy the minimum safe distance. For our own verification, we assume that if the maneuver is proven formally safe w.r.t. our safety conditions and a collision has occurred nonetheless, another vehicle must be liable. For a new traffic participant, the safe distance between it and the ego vehicle is first checked whether it is satisfied. For unsatisfactory situations, the framework continues to track whether the self-driving system takes feasible measures to restore the safe distance. If the safe distance between the two vehicles is restored successfully, we still believe that the behavior of the system is safe. However, if it cannot be restored and exceeds the

minimum safe distance, we consider the behavior of the system to be unsafe and issue an early warning to avoid potential collisions. Different from general verification methods that only focuses on collision avoidance, we investigate the sensitivity, resilience and implementability of handling dangerous situations according to the reaction time and the measures of the self-driving system in the verification. These assessments can better reflect deficiencies of the self-driving system, and can provide guidance for subsequent improvements to this system in the future.

4 | SAFETY FRAMEWORK

The system for self-driving car outputs the steering angle, acceleration and braking. We consider correct behavior safety for prediction outputs. In Section 3, we discuss the five aspects of the longitudinal safe distance, the lateral safe distance, lane change maneuvers, overtaking and how to face new traffic participants for self-driving car in detail. We set the safety requirements involved in those five aspects as safety conditions, and then apply these safety conditions to the verification framework we proposed as shown in Figure 6.

Our safety verification framework starts from prediction outputs of the self-driving vehicle and detects whether the current state of the ego vehicle satisfies safety conditions. If safety conditions are satisfied, the current behavior is considered to be temporarily safe. For unsatisfied situations, the framework further checks whether the ego vehicle takes feasible measures (such as decelerating) for satisfying the safety conditions. If safety conditions are satisfied by taking effective measures during the follow-up tracking, the current behavior of the ego vehicle is considered to be temporarily safe. However, if the safety conditions are unsatisfied after measures are taken all the time, once the ego vehicle no longer takes any feasible measures, the framework checks whether its current state satisfies the minimum safe distance. When the minimum safe distance is unsatisfied, the current behavior is considered unsafe. When it is satisfied, the framework detects whether the ego vehicle performs emergency braking. If emergency braking is not performed, the behavior is considered unsafe. If emergency braking is performed and the collision is avoided, the behavior is still considered safe. If a collision occurs after the emergency braking is performed, further safety analysis is required to determine who is responsible. If the ego vehicle respects all traffic rules, it will not be responsible for the collision. If it is the responsibility of the ego vehicle, the behavior is considered unsafe. The judgment of liability here is mainly based on traffic rules. For example, the following vehicle or a vehicle that is suddenly inserted laterally collides with the host vehicle, which is the responsibility of other vehicles.

In the existing work, as long as the self-driving car dissatisfies current safety conditions, its predicted behavior is directly judged as unsafe. However, in our framework, we will continue to track the self-driving car until it reaches the limit of safety condition (the strictest safety condition). If the self-driving car take some measures to alleviate the current situation until safety conditions are finally satisfied, we believe that the predicted behavior is still safe. Therefore, compared with existing methods, our framework is slack. In addition, in our online verification process, we set 5 parameters (the rationality of the planned trajectory, the accuracy of the prediction model, the implementability, the resilience and the sensitivity), which can mark these different responses of the self-driving car and non-compliance with safety requirements. These parameters can be used to evaluate the performance of self-driving systems, and can be used to guide trajectory planning or evaluate the accuracy of behavior predictions in the future.

Our framework applies formal verification methods to prove the correctness of the vehicles' behavior. However, it does not mean that if a vehicle unsatisfies the safety conditions in our framework, a collision is bound to occur. Our safety conditions describe whether the ego vehicle is at risk of collision. For example, if the ego vehicle unsatisfies the safety conditions with the leading vehicle, the behavior of the vehicle at this time is unsafe. Since once the leading vehicle brakes urgently and the ego vehicle cannot change lanes, a collision will definitely occur. However, if the preceding vehicle does not brake but keeps moving, the ego vehicle will not collide with the leading vehicle.

Moreover, the ability to cooperate with other vehicles is reflected in whether the ego vehicle interferes with other vehicles' execution of the scheduled planned route. For example, when the leading vehicle B_l performs a lane change, whether the ego vehicle decelerates and respects a safe distance to the leading vehicle B_l (at least not accelerate until the leading vehicle B_l completely passes the lane line); or when the vehicle B_j in the adjacent lane has transferred a lane change command, whether the ego vehicle respects a safe distance by deceleration or becomes the leading vehicle of B_j by acceleration to support this lane change.

5 | EXPERIMENTAL RESULTS

The presented longitudinal safe distance has been evaluated on a data-set of recorded traffic from the NGSIM project [23] to investigate the safety of human driven lane changes. The data-set contains the position, speed, acceleration, and respective lane of vehicles driving on US Highway 101. Data collection time was between 7:50 a.m. and 8:35 a.m. with a granularity of $\Delta t = 0.1$s. The study area is 640 m long and consists of five lanes.

We assumed a maximum absolute acceleration of $a_{max} = 8$ m/s^2 per vehicle and a maximum velocity of $v_{max} = 16.67$ m/s. Furthermore, we make use of the safe distance extension to take different reaction times into account, assuming $\delta_{human} = 1.0$ s for humans and $\delta_{machine} = 0.3$ s for self-driving cars [24]. The safety evaluation on the longitudinal safe distance of following and leading vehicles has been implemented using forward simulation of the vehicles' initial state.

NGSIM data not only includes the current vehicle's position, speed and acceleration, but also includes the lane and the IDs of the leading and following vehicles in the same lane. The speed, acceleration, and position of these vehicles can be easily

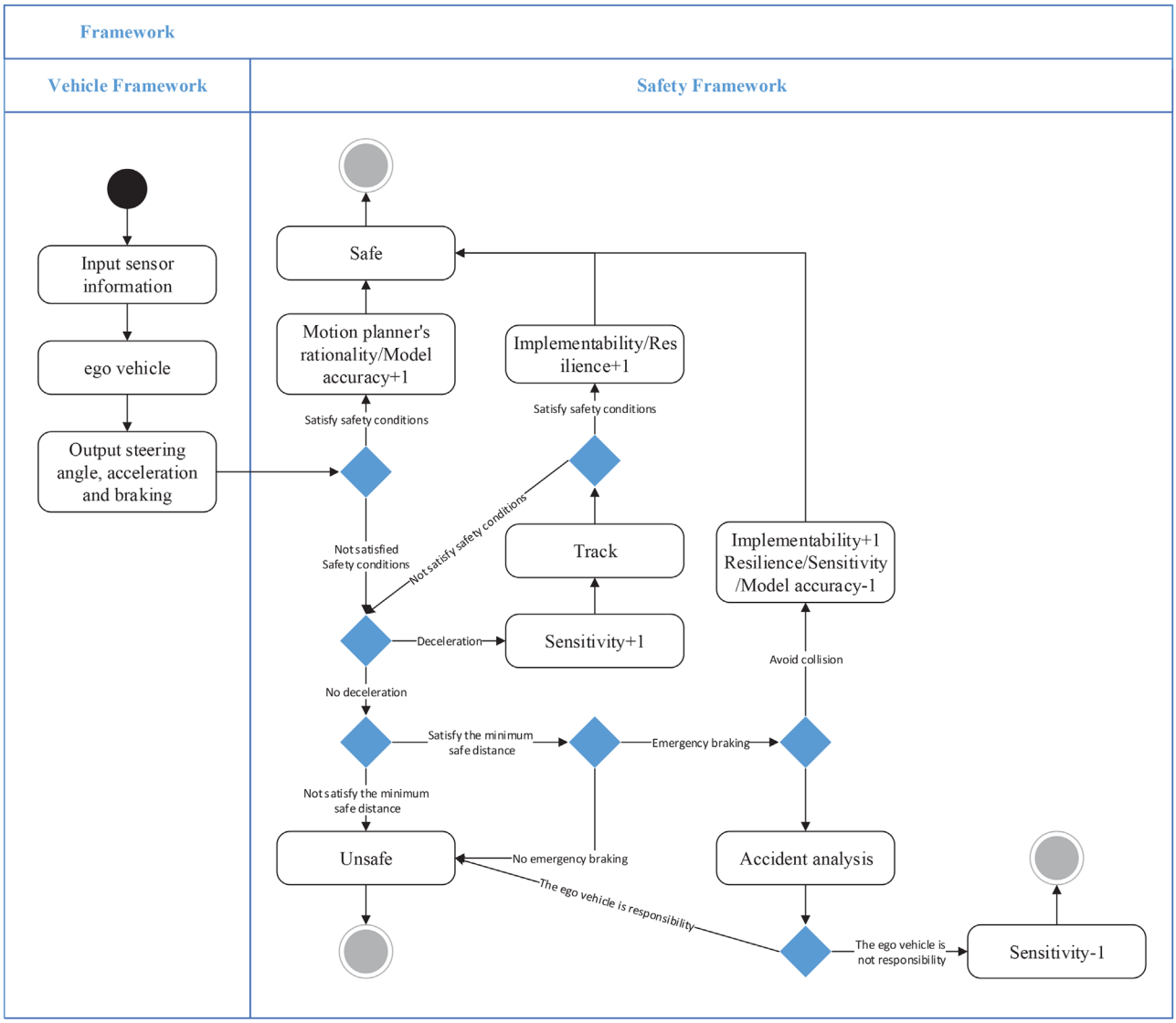


FIGURE 6 A verification framework for self-driving car

obtained from these vehicle IDs. First, the vehicle's IDs whose lane has changed are found by searching the NGSIM data. Then, the approximate lane change time is locked according to the position change of the vehicle and the corresponding time. During the lane change time, we track these information of the leading and following vehicles in the lane where the lane changing vehicle is located. Finally, these longitudinal safe distances of the leading and following vehicles are calculated to check whether these safe distances are satisfied. If the safe distance is not satisfied during the lane change, report it.

Table 3 highlights the evaluation results of $N = 1341$ total longitudinal safe distances for different reaction times. In terms of $\delta = 0.0$ s, an average of 85.39% of the lane changes are classified as safe. This number will decrease to 75.81% if $\delta_{machine}$ is used. Considering that the vehicles in the data-set are controlled by humans, only 54.15% of the lane changes are classified as safe.

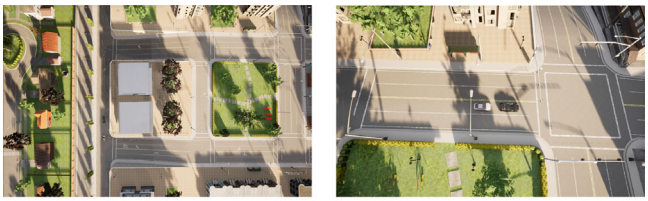
TABLE 3 Percentage of the longitudinal safe distances between the ego vehicle and the leading (or following) vehicle for various reaction times

Data-set	n	$\delta = 0.0s$	$\delta_{machine} = 0.3s$	$\delta_{human} = 1.0s$
7:50–8:05	531	86.25%	75.52%	62.52%
8:05–8:20	410	83.17%	73.41%	53.17%
8:20–8:35	400	86.75%	78.5%	52.75%

To evaluate the longitudinal safe distance between the ego vehicle and B_f under no leading vehicle B_l, we again analyzed the evaluation results of $N = 1341$ total safe distances between the ego vehicle and the following vehicle for different reaction times in Table 4. In terms of $\delta = 0.0$ s, an average of 69.76% of the lane changes are classified as safe. The percentage increases to 70.14% if $\delta_{machine}$ is used. Considering that the ego vehicle and its following vehicle in the data-set are controlled by humans,

TABLE 4 Percentage of the longitudinal safe distances between the ego vehicle and the following vehicle for various reaction times

Data-set	n	$\delta = 0.0$ s	$\delta_{machine} = 0.3$ s	$\delta_{human} = 1.0$ s
7:50–8:05	87	71.26%	72.41%	72.41%
8:05–8:20	17	76.47%	76.47%	76.47%
8:20–8:35	13	61.54%	61.54%	61.54%



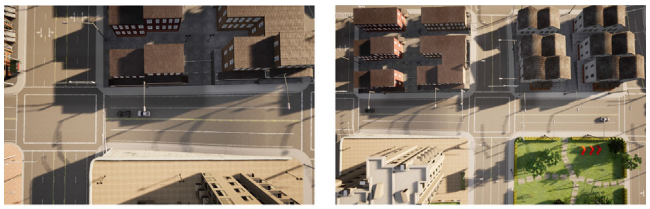
(a) Initial Scenario (b) Termination Scenario

FIGURE 7 The ego vehicle follows its leading vehicle B_l on the same lane (a). The leading vehicle B_l decelerates suddenly, and the ego vehicle respects a safe distance to the vehicle B_l by performing deceleration until B_l stops (b)

also 70.14% of the lane changes are classified as safe. We find that the average percentage for the response time for humans or self-driving cars is higher than the corresponding average percentages in Table 3. It shows that the safe distance without any leading vehicle is sometimes satisfied, but it has been mistakenly regarded as unsatisfied by the same safe distance requirement as the leading vehicle.

We used a proof-of-concept implementation of online verification to check behavioral safety of self-driving cars on the CARLA [25], which is an open-source simulator for self-driving research. Our framework is implemented partly in Python and runs on a computer with an Intel i7 3.2GHz processor and 32GB memory. We build seven urban scenarios by CARLA to demonstrate the benefits of our framework. It takes about 1–37 s for the framework to work on an urban scenario. Regarding the memory, the computer we use is 32G memory, and the memory usage at runtime is 13.9% (4.3G) - 14.2% (4.4G). To increase credibility, We repeated 100 times for each scenario. For seven scenarios, we set the maximum absolute acceleration and deceleration of vehicles to $|a_{max,l}|$=8 m/s^2 and $|a_{max,l}|$=7 m/s^2, respectively.

An urban scenario, in which the leading vehicle suddenly slows down until it stops, is shown in Figure 7. In this scenario, the ego vehicle remains safe by executing the calculation and inspection of the longitudinal safe distance in our verification framework. In fact, until both the leading vehicle and the ego vehicle stop, the safe distance between the two vehicles is maintained. It shows that the self-driving system can sensitively detect the deceleration of the leading vehicle and respect the safe distance. In fact, there is another optimization strategy, which lets the ego vehicle change to the adjacent shoulder lane to certainly avoid a collision. It shows that the self-driving system lacks the flexibility of motion planning. In the repeated experiment of this scenario, we found that the two vehicles stopped at other intersections as shown in Figure 8a



(a) New Termination Scenario 1 (b) New Termination Scenario 2

FIGURE 8 The ego vehicle and its leading vehicle B_l stopped at other intersections (a). the two vehicles were driving in different directions when they encountered a green light at the intersection (b)

and the two vehicles were driving in different directions when they encountered a green light at the intersection as shown in Figure 8b.

Figure 9a shows the initial urban scenario, in which the ego vehicle is leading vehicle. The initial distance between the ego vehicle and the following vehicle maintains the safe distance. The intended trajectory of the ego vehicle is planned by the CARLA's self-driving system, and the following vehicle B_f accelerates at a constant acceleration. However, the ego vehicle as the leading vehicle of the following vehicle B_f did not take any measure to avoid a potential collision, such as accelerating to respect a safe distance to the following vehicle B_f or changing lanes. Finally, the following vehicle B_f lead to a potential collision as shown in Figure 9c. It is a typical example showing that the CARLA's self-driving system predicts unsafe behavior for motion planning. If the ego vehicle respects our proposed new minimum safe distance to the following vehicle, it can completely maintain a safe distance by accelerating without changing lanes to avoid a collision. In the repeated experiment of this scenario, we found some new scenarios as shown in Figure 10 where some sensitive parameters changed. We analyzed that the difference in the speed of the following vehicle in the simulator caused the change in the parameters of the framework.

The lateral distance between the ego vehicle and the adjacent vehicle B_j is less than the minimum lateral safe distance as shown in Figure 11a. In this scenario, the current state of the ego vehicle is unsafe by executing our verification framework. To avoid a potential collision, the ego vehicle should take measures to restore a safe distance with the adjacent vehicle B_j. Figure 11b shows the planned trajectory, which lets the ego vehicle swerve to the adjacent shoulder lane to restore the lateral safe distance and certainly avoid a collision. From the final scene Figure 11c, the ego vehicle and B_j have recovered the lateral safe distance. It shows that the CARLA's self-driving system is still more sensitive to the lateral distance and responds quickly.

Finally, we focus on new traffic participants suddenly appeared that affect original motion plans of the ego vehicle. In an urban scenario as shown in Figure 12a, the ego vehicle drives on a predetermined planned route. However, at an intersection, a new vehicle appears suddenly and crosses the road. The ego vehicle decelerates to give way to the new traffic participant, which reflects the self-driving system's ability to cooperate with other vehicles. Finally, the ego vehicle smoothly becomes

(a) Initial Scenario (b) Halfway Scenario (c) Termination Scenario

FIGURE 9 The following vehicle B_f follows the ego vehicle on the same lane (a). The following vehicle B_f suddenly accelerates and the distance between two vehicles gradually decreases, but the ego vehicle did not accelerate according to the original prediction (b). Eventually, the following vehicle B_f collides with the ego vehicle (c)

(a) New Scenario 1 (b) New Scenario 2 (c) New Scenario 3

FIGURE 10 The sensitivity parameter is 0 (a). The sensitivity parameter is 2 (b). The sensitivity parameter is 4 (c)

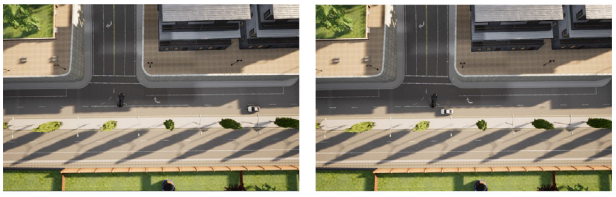
(a) Initial Scenario (b) Halfway Scenario (c) Termination Scenario

FIGURE 11 The ego vehicle is adjacent to the adjacent vehicle B_j (a). The ego vehicle swerve to the adjacent shoulder lane to certainly avoid a collision (b). The ego vehicle recovers the lateral safe distance with the adjacent vehicle B_j by executing the predicted trajectory of CARLA's self-driving system (c)

(a) Initial Scenario (b) Halfway Scenario 1

(c) Halfway Scenario 2 (d) Termination Scenario

FIGURE 12 The ego vehicle intends to continue across the intersection (a). However, the new vehicle suddenly crosses the target lane of the ego vehicle (b). The ego vehicle decelerates to give way to the new traffic participant (c). The ego vehicle smoothly becomes the following vehicle of the new vehicle (d)

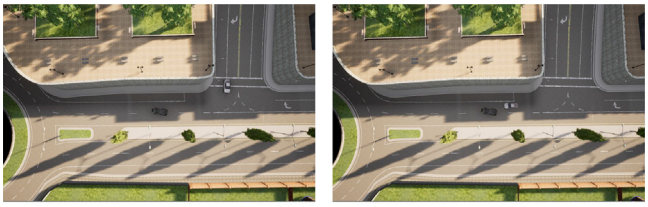


(a) Initial Scenario (b) Termination Scenario

FIGURE 13 There is a faulty vehicle parked at an intersection, in front of the ego vehicle. (a). The ego vehicle respects a safe distance to the faulty vehicle by performing braking (b)

the following vehicle of the new vehicle and respects a safe distance to it (see Figure 12d).

Figure 13a shows the initial urban scenario, in which the ego vehicle drives on a predetermined planned route. Another faulty vehicle stopped at the intersection ahead, and the rear of the vehicle went beyond the lane line where its own lane was located, but it would not affect the driving of other vehicles. The ego vehicle finally regards the faulty vehicle as the leading vehicle and brakes as shown in Figure 13b. It shows that



(a) Initial Scenario (b) Termination Scenario

FIGURE 14 The ego vehicle performs a right turn (a). The ego vehicle respects a safe distance to the faulty vehicle by performing braking (b)

(a) Initial Scenario (b) Termination Scenario

FIGURE 15 There is a faulty vehicle in front of the ego vehicle parked at an intersection, and the ego vehicle was driving on the right-turn lane (a). The ego vehicle respects a safe distance to the faulty vehicle by performing braking (b)

the CARLA's self-driving system is still sensitive to the longitudinal distance and responds quickly. The scene is similar to the corrected steering angle incident of Didi's self-driving vehicle. Unfortunately, The Carla's self-driving system did not adopt a steering method to increase the lateral safe distance to complete overtaking.

The ego vehicle may not be able to detect the new traffic participant in time because of its visual field as shown in Figure 14a. In this urban scenario, after the ego vehicle is turning, it encounters another vehicle that failed during the lane change and was stuck in the middle of two lanes. The ego vehicle may not be able to detect the new traffic participant in time because of its visual field before turning, but it finally regards the new traffic participant as the leading vehicle and performs braking from Figure 14b.

Figure 15a shows the initial urban scenario, in which the location of the faulty vehicle is the same as that of the urban scenario Figure 13, except that the ego vehicle is in the lane turning right. The ego vehicle finally regards the faulty vehicle as the leading vehicle and brakes. However, based on the driving experience of the human driver from the location of the faulty vehicle, the ego vehicle has a chance to complete the turn by re-steering. It reflects the lack of flexibility of the system in motion planning.

To reflect the performance of self-driving cars on prediction behaviors in different scenarios, five parameters (the rationality of the planned trajectory, the accuracy of the prediction model, the implementability, the resilience and the sensitivity) are set in our verification framework. These parameters are used to identify the different reactions of self-driving cars in common driving scenarios and to detect non-compliance cases with safety requirements. These parameters obtained in the above seven scenarios are shown in Table 5. We repeated 100 times for each of seven scenarios conducted with CARLA. Each evaluation parameter is averaged. From Table 5, it can be seen that the Carla's self-driving system is more sensitive to the leading car, the adjacent car, and the car suddenly appearing at the fork in the simulation environment, but there are defects in the interaction with the following car. These parameters can be used to evaluate the performance of self-driving systems, and can be used to guide trajectory planning or evaluate the accuracy of behavior predictions in the future.

6 | RELATED WORK

The safety for self-driving cars is recognised an important problem [26]. Therefore, many safeguarding approaches for the domain of self-driving cars have been proposed. One approach to guarantee safety is to examine the system under test offline, before actual usage [27]. Model-checking or branches of modal logic are used to guarantee accordance with a specified behavior. However, frequent software updates and online machine learning methods cannot be properly handled by these approaches, since the system may change post-examination.

Another approach is to monitor the system online to enhance the level of safety [28]. One group of approaches uses probabilistic metrics [29–31] to determine a collision probability or empirical performance indicators [32] resulting in a safety rating for the vehicle under test. However, a sufficient safety assurance cannot be provided based on these metrics. Furthermore, some of the trained models might extend to complex realizations, that cannot be approved themselves [33]. By contrast, methods relying on formal and deterministic fundamentals can provide guarantees based on imposed requirements. Among them are reachable sets [5, 34, 35], runtime verification [36], and metric-based approaches [37], including the RSS model [17]. However, some of these approaches tailored to a specific software lack flexibility and cannot be bundled with other software components or approaches. Furthermore, all of these approaches have in common, that they focus on selected safety aspects (e.g. dynamic collision detection) and do not strive for a holistic online verification with the goal of safety approval [33].

There are methods relied on switching among several operating modes. In [38], the authors proposed an integrated control strategy for adaptive cruise control with auto-steering for highway driving. An appropriate logic-based control strategy is used to create synergies and safe interaction between longitudinal and lateral controllers to obtain both lateral stability and advanced adaptive cruise control functionalities. However, methodical integration of longitudinal adaptive cruise control strategies and of lateral control strategies is to a large extent missing, as well as validation in real-time computing environment of the safety and performance of longitudinal and lateral integrated solutions. Therefore, in [39], the authors proposed a real-time validation of an integrated vehicle dynamic control strategy, designed to create safe interaction between longitudinal and lateral controllers: the integrated system is designed, implemented and tested through Dynacar, a real-time

TABLE 5 Parameters used to evaluate self-driving cars in seven scenarios

Scenario	Plan rationality	Model accuracy	Sensitivity	Implementability	Resilience
1	1	1	0	0	0
2	0	−1	1.3	0	−1
3	1	1	0	0	0
4	1	1	0	0	0
5	2	2	0	0	0
6	2	2	0	0	0
7	2	2	0	0	0

simulation environment for the development and validation of vehicle embedded functionalities.

The authors of [5] propose a safety framework to verify the safety of each planned trajectory on-the-fly, using formal methods to handle uncertain measurements and future behaviors of traffic participants and disturbances acting on the ego vehicle, among others. The framework is composed of modules for set-based prediction, fail-safe trajectory generation, and online verification. In case of any malfunction, where new trajectories cannot be obtained during run-time, the self-driving car remains safe, since it can just execute the previously verified fail-safe trajectory which is stored on a redundant memory.

In a recent paper [40], the authors propose an autonomous driving system (ADS) verification framework, which can efficiently support cost-effective simulation by means of the functional mock-up interface (or the data distribution service) and cloud computing. By testing whether the verification of the ADS in the simulation environment is accurate and whether the distributed simulation is interworked, it can compare the difference between the ADS made for the experiment and the ideal ADS, and confirm that the interworking test is also accurate.

7 | CONCLUSION AND FUTURE WORK

We presented a novel framework for verifying behavioral safety of self-driving cars online. The technique is based on our proposed five safety considerations: new longitudinal and lateral safe distances, lane changes, overtaking and how to face new traffic participants. Different from the previous verification considerations, our verification framework allows predicted behaviors (i.e., prediction outputs) of self-driving cars to be temporarily inconsistent with the popular strict safe distance. As long as the self-driving car respects the minimum safe distance calculated by our technique and executes improvement behaviors to restore the safe distance, we still believe that the predictive behavior is safe. To evaluate the self-driving system, when we detect whether the predicted behavior satisfies safety standards and take effective measures under unsafe conditions, we introduce five weighted indicators, which may be used to improve this system in the future. Our success in verifying properties of some urban scenarios in CARLA indicates that the technique has great potential in verifying behavioral safety of real-world self-driving cars. Since our framework is independent of the utilized planning framework, it can easily be integrated in existing vehicle frameworks.

In a next step, we plan to increase the technique's scalability. Specifically, we will explore the combination of our framework and pedestrian's behavior prediction model or vehicle-following model. Apart from improving the safety conditions applied in our framework, we plan to explore better strategies for the optimization of self-driving cars according to the weight in the framework.

ACKNOWLEDGMENTS

This work was supported by National Key Research and Development Project (Key Technologies and Applications of Security and Trusted Industrial Control System NO. 2020YFB2009500), the Fundamental Research Funds for the Central Universities (DUT20TD107), and NTT DATA Automobiligence Research Center.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

CONFLICT OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ORCID

Huihui Wu https://orcid.org/0000-0001-7254-3379

REFERENCES

1. Google's self-driving car caused its first crash (2016)
2. Fatal car crash involving a self-driving uber shows there are major flaws in the software, hardware, and testing procedures involving autonomous vehicles (2018)
3. Tesla says vehicle in deadly crash was on autopilot (2018)
4. Kalra, N., Paddock, S.M.: Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability? Transport. Res. Part A: Policy Pract. 94, 182–193 (2016)
5. Pek, C., Koschi, M., Althoff, M.: An online verification framework for motion planning of self-driving vehicles with safety guarantees. In AAET-Automatisiertes und vernetztes Fahren (2019)
6. Althoff, M.: Reachability analysis of nonlinear systems using conservative polynomialization and non-convex sets. In: Proceedings of the 16th

International Conference on Hybrid Systems: Computation and Control, HSCC 2013, pp. 173–182. ACM, New York (2013)
7. Herbert, S.L., Chen, M., Han, S., Bansal, S., Fisac, J.F., Tomlin, C.J.: Fastrack: A modrk for fast and guaranteed safe motion planning. In: 56th IEEE Annual Conference on Decision and Control, CDC 2017, pp. 1517–1522. IEEE, Piscataway (2017)
8. Mitchell, I.M.: Comparing forward and backward reachability as tools for safety analysis. In: Proceedings of 10th International Workshop on Hybrid Systems: Computation and Control, HSCC 2007, pp. 428–443. ACM, New York (2007)
9. Althoff, D., Buss, M., Lawitzky, A., Werling, M., Wollherr, D.: On-line trajectory generation for safe and optimal vehicle motion planning. In: Autonomous Mobile Systems 2012-22, pp. 99–107. Springer, Berlin (2012)
10. Martinez-Gomez, L., Fraichard, T.: An efficient and generic 2d inevitable collision state-checker. In: 2008 IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 234–241. IEEE, Piscataway (2008)
11. Petti, S., Fraichard, T.: Safe motion planning in dynamic environments. In: 2005 IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 2210–2215. IEEE, Piscataway (2005)
12. Bouraine, S., Fraichard, T., Salhi, H.: Provably safe navigation for mobile robots with limited field-of-views in dynamic environments. Auton. Robots 32(3), 267–283 (2012)
13. Damm, W., Peter, H.-J., Rakow, J.-H., Westphal, B.: Can we build it: Formal synthesis of control strategies for cooperative driver assistance systems. Math. Struct. Comput. Sci. 23(4), 676–725 (2013)
14. Hilscher, M., Linker, S., Olderog, E.R.: Proving safety of traffic manoeuvres on country roads. In: Theories of Programming and Formal Methods - Essays Dedicated to Jifeng He on the Occasion of His 70th Birthday, pp. 196-212. Springer, Berlin Heidelberg (2013)
15. Loos, S.M., Platzer, A., Nistor, L.: Adaptive cruise control: Hybrid, distributed, and now formally verified. In: FM 2011: Formal Methods - 17th International Symposium on Formal Methods, pp. 42–56. Springer, Berlin (2011)
16. Wu, H., Lyu, D., Hou, G., Watanabe, M., Kong, W.: A new consideration of the longitudinal and lateral safe distance of self-driving vehicle. under submission.
17. Shalev-Shwartz, S., Shammah, S., Shashua, A.: On a formal model of safe and scalable self-driving cars. CoRR, abs/1708.06374 (2017)
18. Rizaldi, A., Keinholz, J., Huber, M., Feldle, J., Immler, F., Althoff, M., Hilgendorf, E., Nipkow, T.: Formalising and monitoring traffic rules for autonomous vehicles in isabelle/hol. In: 13th International Conference on Integrated Formal Methods, IFM 2017, pp. 50–66. Springer, Berlin Heidelberg (2017)
19. Pek, C., Zahn, P., Althoff, M.: Verifying the safety of lane change maneuvers of self-driving vehicles based on formalized traffic rules. In: 2017 IEEE Intelligent Vehicles Symposium (IV), pp. 1477-1483. IEEE, Piscataway (2017)
20. Economic Commission for Europe: Inland Transport Committee. Vienna Convention on Road Traffic (1968)
21. Rizaldi, A., Althoff, M.: Formalising traffic rules for accountability of autonomous vehicles. In: IEEE 18th International Conference on Intelligent Transportation Systems, ITSC 2015, pp. 1658–1665. IEEE, Piscataway (2015)
22. Naumann, M., Königshof, H., Stiller, C.: Provably safe and smooth lane changes in mixed traffic. In: 2019 IEEE Intelligent Transportation Systems Conference (ITSC), pp. 1832–1837. IEEE, Piscataway (2019)
23. Federal Highway Administration Research and Technology. US highway 101 dataset. (2007)
24. Johansson, G., Rumar, K.: Drivers brake reaction times. Human Factors 13(1), 23–27 (1971)
25. Dosovitskiy, A., Ros, G., Codevilla, F., López, A.M., Koltun, V.: CARLA: an open urban driving simulator. In: 1st Annual Conference on Robot Learning, CoRL 2017, pp. 1–16. Springer, Cham (2017)
26. Koopman, P., Wagner, M.: Challenges in autonomous vehicle testing and validation. SAE Int. J. Transport. Safety 4(1), 15–24 (2016)
27. Luckcuck, M., Farrell, M., Dennis, L.A., Dixon, C., Fisher, M.: Formal specification and verification of autonomous robotic systems: A survey. ACM Comput. Surv. 52(5), 100:1–100:41, (2019)
28. Lefèvre, S., Vasquez, D., Laugier, C.: A survey on motion prediction and risk assessment for intelligent vehicles. ROBOMECH J. 1(1), 1–14 (2014)
29. Kim, B., Park, K., Yi, K.: Probabilistic threat assessment with environment description and rule-based multi-traffic prediction for integrated risk management system. IEEE Intell. Transp. Syst. Mag. 9(3), 8–22 (2017)
30. Annell, S., Gratner, A., Svensson, L.: Probabilistic collision estimation system for autonomous vehicles. In: 19th IEEE International Conference on Intelligent Transportation Systems, ITSC 2016, pp. 473-478. IEEE, Piscataway (2016)
31. Lambert, A., Gruyer, D., Saint-Pierre, G., Ndjeng, A.N.: Collision probability assessment for speed control. In: 11th International IEEE Conference on Intelligent Transportation Systems, ITSC 2008, pp. 1043–1048. IEEE, Piscataway (2008)
32. Reschka, A., Böhmer, J.-R., Nothdurft, T., Hecker, P., Lichte, B., Maurer, M.: A surveillance and safety system based on performance criteria and functional degradation for an autonomous vehicle. In: 15th International IEEE Conference on Intelligent Transportation Systems, ITSC 2012, pp. 237–242. IEEE, Piscataway (2012)
33. Stahl, T., Eicher, M., Betz, J., Diermeyer, F.: Online verification concept for autonomous vehicles - illustrative study for a trajectory planning module. In: 23rd IEEE International Conference on Intelligent Transportation Systems, ITSC 2020, pp. 1–7. IEEE, Piscataway (2020)
34. Schürmann, B., Hess, D., Eilbrecht, J., Stursberg, O., Köster, F., Althoff, M.: Ensuring drivability of planned motions using formal methods. In: 20th IEEE International Conference on Intelligent Transportation Systems, ITSC 2017, pp. 1–8. IEEE, Piscataway (2017)
35. Althoff, M., Dolan, J.M.: Online verification of automated road vehicles using reachability analysis. IEEE Trans. Robotics 30(4), 903–918 (2014)
36. Kane, A., Chowdhury, O., Datta, A., Koopman, P.: A case study on runtime monitoring of an autonomous research vehicle (ARV) system. In: 6th International Conference on Runtime Verification, pp. 102–117. Springer, Berlin Heidelberg (2015)
37. Feth, P., Schneider, D., Adler, R.: A conceptual safety supervisor definition and evaluation framework for autonomous systems. In: 36th International Conference on Computer Safety, Reliability, and Security, SAFECOMP 2017, pp. 135–148. Springer, London (2017)
38. Idriz, A.F., Rachman, A., Baldi, S.: Integration of auto-steering with adaptive cruise control for improved cornering behaviour. IET Intel. Transport Syst. 11(10), 667–675 (2017)
39. Rachman, A., Idriz, A.F., Li, S., Baldi, S.: Real-time performance and safety validation of an integrated vehicle dynamic control strategy. IFAC-PapersOnLine 50(1), 13854–13859 (2017)
40. Cho, D.-S., Yun, S., Kim, H., Kwon, J., Kim, W.: Autonomous driving system verification framework with FMI co-simulation based on OMG DDS. In: 2020 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–6. IEEE, Piscataway (2020)

How to cite this article: Wu, H., Lyu, D., Zhang, Y., Hou, G., Watanabe, M., Wang, J., Kong, W.: A verification framework for behavioral safety of self-driving cars. IET Intell. Transp. Syst. 1–18 (2022). https://doi.org/10.1049/itr2.12162