Short Papers

Towards a Complete Safety Framework for Longitudinal Driving

Galina Sidorenko, Aleksei Fedorov, Johan Thunberg, and Alexey Vinel, *Senior Member, IEEE*

***Abstract*—Formal models for the safety validation of autonomous vehicles have become increasingly important. To this end, we present a safety framework for longitudinal automated driving. This framework allows calculating minimum safe inter-vehicular distances for arbitrary ego vehicle control policies. We use this framework to enhance the Responsibility-Sensitive Safety (RSS) model and models based on it, which fail to cover situations where the ego vehicle has a higher decelerating capacity than its preceding vehicle. For arbitrary ego vehicle control policies, we show how our framework can be applied by substituting real (possibly computationally intractable) controllers with upper bounding functions. This comprises a general approach for longitudinal safety, where safety guarantees for the upper-bounded system are equivalent to those for the original system but come at the expense of larger inter-vehicular distances.**

***Index Terms*—Automated driving, collision avoidance, safety validation, responsibility-sensitive safety, vehicle-to-vehicle communications.**

I. Introduction

Despite the tremendous progress in machine learning, computer vision, localization, vehicular communications, and other enablers for automated driving (AD), the adoption of autonomous vehicles (AVs) on public roads is still rather limited [1]. One of the aspects which becomes increasingly important for future market deployment of AVs is their *safety validation* [2], [3]. It is evident that statistical approaches based on, for example, on-road testing, do not scale well, which makes it important to design formal models for the safety analysis [4].

One of the well-known examples of such a model is Responsibility-Sensitive Safety (RSS) [5]. Particularly, it provides minimum inter-vehicle distances (IVDs), which are safe to keep, for given braking capabilities of the vehicles. For the case of connected vehicles, where braking relies on vehicle-to-vehicle (V2V) communications, safe IVDs are also dependent on the qualities of inter-vehicular radio links [6]. Recent related efforts in the context of the RSS model are in the direction of overcoming its assumptions on the longitudinal behavior by reachable set based worst-case predictions [7], finding its reasonable parameters based on real traffic data [8], [9] or providing methods to automatically explore the performance limits of AV safety models [10].

Limitations of the RSS model have been investigated and reported in [9], [11], [12], [13]. Specifically, due to improper choice of model parameters, the minimum distance provided by the RSS can become unnecessarily large, which has a negative effect on road efficiency [12]. In [12], an attempt to optimize the RSS model is made in order to achieve a trade-off between safety and efficiency. The proposed models are assessed by numerical simulations.

Our work not only proposes a theoretical approach to overcome the conservative results in RSS but also shows an explicit parameter interval where the RSS distance is insufficient to guarantee safety. Such a special case where safety cannot be guaranteed with the original RSS model has been previously reported in [4]. However, the domain for this special case was not completely described and lacked one condition. Without this condition, as we show by an example, the safe IVDs become unnecessarily large. In our work, compared to [4], this condition is present, and results are presented comprehensively and explicitly.

In this paper, we focus on longitudinal AD with short IVD, which is foreseen to be a common scenario for future AVs. An incentive for driving close comes both from better road utilization and also, in certain cases, from the fuel-saving effect [14]. Recently, we derived minimum safe distances for a special scenario where the follower vehicle uses an adaptive cruise control (ACC) [15]. To calculate those distances, we introduced and applied a novel *3-step methodology* [15] that allowed us to handle the considered safety analysis problem effectively. The three steps can be summarized as follows:

1) A so-called *minimum safe braking set* is specified. Upon reaching this set, the follower vehicle has to emergency brake immediately to avoid a rear-end collision.
2) Trajectories of the two considered vehicles are obtained on the time interval $[0; \tau]$, where τ is referred to as a *response time*. During the first τ seconds, the follower vehicle is unaware of the emergency braking situation ahead and continues to move forward according to its control law.

Manuscript received 9 July 2022; revised 25 August 2022 and 19 September 2022; accepted 23 September 2022. Date of publication 27 September 2022; date of current version 19 December 2022. *(Corresponding author: Galina Sidorenko.)*

Galina Sidorenko and Johan Thunberg are with Halmstad University, 301 18 Halmstad, Sweden (e-mail: galina.sidorenko@hh.se; johan.thunberg@hh.se).

Alexey Vinel is with the Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany, and also with Halmstad University, 301 18 Halmstad, Sweden (e-mail: alexey.vinel@hh.se).

Aleksei Fedorov is with Lund University, SE-221 00 Lund, Sweden (e-mail: aleksei.fedorov@eit.lth.se).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIV.2022.3209910.

Digital Object Identifier 10.1109/TIV.2022.3209910

3) The minimum initial distance between vehicles is found such that trajectories obtained in the second step reach the minimum safe braking set exactly at τ seconds.

In this paper, we expand on this methodology by explicitly applying it to a special scenario of the RSS model on the one hand and addressing more general cases with arbitrary acceleration/deceleration profiles of the follower vehicle on the other. We extend both [5] and [15], and present two novel contributions:

- First, in Section II we demonstrate how the 3-step methodology can be applied to the setting considered in the RSS model, where the ego vehicle accelerates or moves with a constant velocity until switching to the emergency braking mode by applying its maximum possible deceleration $\bar{a}_2$. We show that RSS-based IVDs become insufficient when the ego vehicle has a higher decelerating capacity $\bar{a}_2$ than its preceding vehicle $\bar{a}_1$, and present the comprehensive formula and the explicit conditions when such a formula should be applied.
- Second, in Section III we provide a procedure for calculation of minimum safe IVDs versus the response time for follower vehicle with an *arbitrary control law*. We show that for a function bounding the controller from above, the methodology results in distances with higher safety guarantees compared to the ones corresponding to the real controller. A tighter limiting function results in a tighter bound and thus shorter IVD. Several examples are presented in Section IV illustrating how the appropriate choice of bounding function makes it easier to calculate sufficient safe minimum distances.

Our contributions are also applicable for the safety analysis of V2V-enabled *cooperative* AD [14]. Indeed, if the decision for emergency braking can be made with some probability P during the response time, then the chosen IVD can guarantee no-collision behavior with a probability no less than P. In such a setting, the probability of the decision to brake would correspond to the probability of receiving at least one braking message by the ego vehicle from the preceding vehicle during interval $[0;\tau]$.

II. RSS Assumptions: Constant Acceleration

A. Safety Analysis

We consider two vehicles, which we call a leader and a follower, moving along the road with a short IVD. At some point, the leader abruptly emergency brakes with its maximum braking capacity $\bar{a}_1$ (e.g., due to a pedestrian appearing on the road), and the follower has to brake in response to avoid a rear-end collision. During the response time τ, the following vehicle is unaware of the preceding vehicle's critical braking and keeps moving with a constant speed or even accelerates with maximum possible acceleration a_2^{ac} (in the pessimistic case). Once the response time τ passes, the decision of emergency braking is made by the follower, and it applies maximum possible deceleration $\bar{a}_2$. Note that by deceleration $\bar{a}_i$ we refer to the amplitude of negative acceleration. The problem that we tackle here is to find a minimum safe distance that guarantees collision-free behavior. Such distance is dependent on the response time τ and the controller that the follower is using during this time.

Below, we apply the 3-step methodology in order to find minimum safe distances in the considered scenario. The "minimum safe braking set" required by the first step can be directly obtained from [15]. However, derivations in steps 2 and 3 differ from [15] due to different assumptions of the follower's controller.

Step 1: The "minimum safe braking set" comprises a two-dimensional hyper-surface in a 3-dimensional space [15]:

$$\partial\mathcal{S} = \{(d^*, v_1^*, v_2^*) : d = f(v_1^*, v_2^*)\}, \tag{1}$$

where v_1 and v_2 are velocities of the leader and follower, respectively; d is IVD; and superscript * denotes the corresponding variable at time τ. If the dynamic parameters of the vehicles, i.e., d, v_1, and v_2 attain values in this set, the follower has to apply the maximum possible deceleration $\bar{a}_2$ immediately in order to avoid a rear-end crash.

The explicit form of f is given below [15]:

$$f(v_1^*, v_2^*) = \begin{cases} \frac{{v_2^*}^2}{2\bar{a}_2} - \frac{{v_1^*}^2}{2\bar{a}_1} & \text{if } \Delta v^* \le v_1^*\left(1 - \sqrt{\frac{\bar{a}_2}{\bar{a}_1}}\right) \\ 0 \quad \text{if } \Delta v^* > v_1^*\left(1 - \sqrt{\frac{\bar{a}_2}{\bar{a}_1}}\right), \end{cases} \tag{2}$$

if $\bar{a}_1 \ge \bar{a}_2$,

$$f(v_1^*, v_2^*) = \begin{cases} \frac{{v_2^*}^2}{2\bar{a}_2} - \frac{{v_1^*}^2}{2\bar{a}_1} & \text{if } \Delta v^* \le v_1^*(1 - \frac{\bar{a}_2}{\bar{a}_1}) \\ \frac{(\Delta v^*)^2}{2(\bar{a}_2 - \bar{a}_1)} & \text{if } v_1^*(1 - \frac{\bar{a}_2}{\bar{a}_1}) < \Delta v^* < 0 \\ 0 \quad \text{if } \Delta v^* \ge 0 \end{cases} \tag{3}$$

if $\bar{a}_1 < \bar{a}_2$.

Here, $\Delta v^* = v_1^* - v_2^*$.

We recall that this set was obtained by considering both vehicles braking with their maximum possible decelerations, i.e., $\ddot{x}_i = -\bar{a}_i$, starting with initial velocities $v_i^* = v_i(\tau)$ and initially placed exactly on the distance d^*. The necessary and sufficient condition for avoiding a collision is that the distance $d(t) = x_1(t) - x_2(t)$ between vehicles is not negative for all $\tau \le t \le \frac{v_2^*}{\bar{a}_2}$. Note, $x_1(t)$ and $x_2(t)$ are coordinates of the leader's rear end and the follower's forward end, respectively. If the leader is still moving at $t = \frac{v_2^*}{\bar{a}_2}$, the IVD will be only increasing for $\frac{v_2^*}{\bar{a}_2} \le t \le \frac{v_1^*}{\bar{a}_1}$, and thus this interval is out of our interest.

If $\bar{a}_1 \ge \bar{a}_2$, it is enough to check the distance between vehicles at the moment when the following vehicle has stopped, i.e., at $t = \frac{v_2^*}{\bar{a}_2}$. If $\bar{a}_1 < \bar{a}_2$, the IVD comprises a parabola with branches up. Thus, there can be a case when $x_1(t) - x_2(t)$ decreases up to the vertex and then increases again. For such a case, it is not sufficient to consider only the distance at $t = \frac{v_2^*}{\bar{a}_2}$. Instead, it is crucial to ensure that at the parabola's vertex, the IVD is equal to zero, i.e., only touching occurs. This condition leads to a second equation in formula (3). All possible cases corresponding to formulas (2)- (3) are shown in Fig. 1 for an illustration purpose.

Step 2: Now, let us consider the motion of the two considered vehicles during the first τ seconds when the follower accelerates with $a_2^{ac} \ge 0$:

$$\dot{x}_1 = v_1,$$

$$\dot{v}_1 = \begin{cases} -\bar{a}_1 & \text{for } 0 \le t \le T_l \\ 0 & \text{for } t > T_l, \end{cases},$$

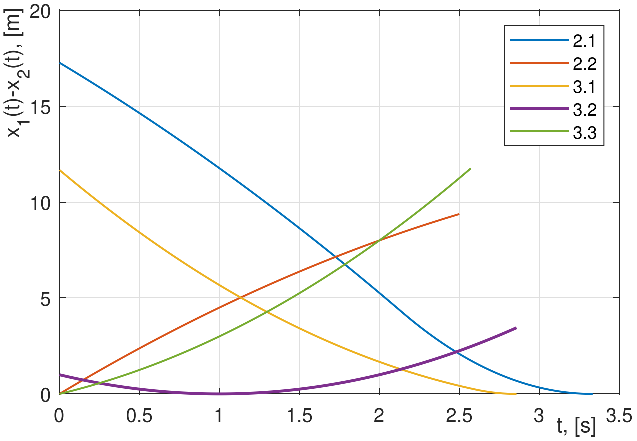

Fig. 1. Different cases of IVD evolution needed for "minimum braking set" derivation. Here, the case "i.j" corresponds to equation "j" in the formula "i". Thus, the more interesting case "3.2" corresponds to the second equation in formula (3).

$$\begin{aligned}\dot{x}_2 &= v_2,\\ \dot{v}_2 &= a_2^{ac},\end{aligned}\tag{4}$$

with initial conditions $x_1(0)=d_0,\ x_2(0)=0,\ v_1(0)=v_1^0,\ v_2(0)=v_2^0$.Here, $T_l=\frac{v_1^0}{\bar{a}_1}$ is the time when the leader comes to a full stop.

The solution of (4) at the time point τ has the form below:

$$\begin{aligned}&x_1(\tau){-}x_2(\tau)\\ &\quad=\begin{cases}d_0+\left(v_1^0{-}v_2^0\right)\tau-\frac{\tau^2}{2}\left(\bar{a}_1{+}a_2^{ac}\right) & \text{if } \tau\le T_l,\\ d_0+\frac{\left(v_1^0\right)^2}{2\bar{a}_1}-v_2^0\tau-\frac{a_2^{ac}}{2}\tau^2 & \text{if } \tau> T_l,\end{cases}\\ &v_1(\tau)=\begin{cases}v_1^0-\bar{a}_1\tau & \text{if } \ \tau\le T_l,\\ 0 & \text{if } \ \tau>T_l,\end{cases}\\ &v_2(\tau)=v_2^0+a_2^{ac}\tau.\end{aligned}\tag{5}$$

Step 3: Now, we combine steps 1 and 2 such that $x_1(\tau)-x_2(\tau)=f(v_1(\tau),v_2(\tau))$. Obviously, we also take into account that $d_0\ge 0$. Having this, we obtain the following:

$$\begin{aligned}&d_0(\tau)\\ &=\left[\frac{a_2^{ac}}{2}\left(\frac{a_2^{ac}}{\bar{a}_2}{+}1\right)\tau^2{+}v_2^0\left(\frac{a_2^{ac}}{\bar{a}_2}{+}1\right)\tau{+}\left(\frac{(v_2^0)^2}{2\bar{a}_2}{-}\frac{(v_1^0)^2}{2\bar{a}_1}\right)\right]_+\end{aligned}\tag{6}$$

if $\bar{a}_1\ge\bar{a}_2$, and

$$\begin{aligned}&d_0(\tau)\\ &=\begin{cases}\left[\left(v_2^0{-}v_1^0\right)\tau+\frac{\tau^2}{2}\left(\bar{a}_1{+}a_2^{ac}\right)+\frac{\left(v_1^0{-}v_2^0{-}(\bar{a}_1{+}a_2^{ac})\tau\right)^2}{2(\bar{a}_2{-}\bar{a}_1)}\right]_+\\ \quad\text{if } \ \tau\in\left[\frac{v_1^0-v_2^0}{a_2^{ac}+\bar{a}_1};\ \frac{v_1^0\frac{\bar{a}_2}{\bar{a}_1}-v_2^0}{a_2^{ac}+\bar{a}_2}\right]\\ \left[\frac{a_2^{ac}}{2}\left(\frac{a_2^{ac}}{\bar{a}_2}{+}1\right)\tau^2{+}v_2^0\left(\frac{a_2^{ac}}{\bar{a}_2}{+}1\right)\tau{+}\left(\frac{(v_2^0)^2}{2\bar{a}_2}-\frac{(v_1^0)^2}{2\bar{a}_1}\right)\right]_+\\ \quad\text{otherwise}\end{cases}\end{aligned}\tag{7}$$

if $\bar{a}_1<\bar{a}_2$.

Here, $[x]_+$ denotes $\max\{x,0\}$.

It can be explicitly shown that the scalar product of the normal vector to the surface (2)–(3) and the tangent vector of the system trajectories (5) at the point of the surface's punch always has a negative sign. Thus, trajectories can punch the surface only once, at the moment τ. Also, it is worth noting that (6)–(7) is a monotonically increasing function of a_2^{ac}. Thus, the bigger acceleration a_2^{ac} during the first τ seconds, the bigger distance required to ensure safe braking.

B. Comparison With RSS Models

Formulas (6)–(7) provide a full and comprehensive recipe for calculating minimum safe longitudinal distances. They comprise a generalization of our previous results [6], [14] where the follower is moving with a constant velocity, i.e., $a_2^{ac}=0$, during the response time τ. In [5], safe longitudinal distance was received under the assumption that the follower accelerates with $a_2^{ac}\ge 0$ during the response time τ before switching to emergency braking by applying maximum deceleration $\bar{a}_2$, i.e., the same setting as considered in Section II. The provided results [5] coincide with (6) covering only the case $\bar{a}_1\ge\bar{a}_2$, which intuitively can be thought of as the worst-case scenario since the follower has lower braking capability than the leader. Thus, the assumption could be that formula (6) provides distances no shorter than those required for the case $\bar{a}_1<\bar{a}_2$, and thus it can be used for $\bar{a}_1<\bar{a}_2$ as well. However, in the case $\bar{a}_1<\bar{a}_2$, longer safe distances can be required than those provided by the original RSS (6). This comes from the fact that for some initial distances, the trajectories of the two vehicles can come to touch, after which the IVD increases again. Such a special case where safety cannot be guaranteed with the original RSS distances is reported in [4]. However, the resulting formulas [4] are missing one important condition which defines when this special case should be applied. In more detail, according to [4], the original RSS formulas can not guarantee non-collision behavior if:

- the follower vehicle braking capability greater than the leader vehicle braking: $\bar{a}_2>\bar{a}_1$;
- at the end of the response time τ, the follower moves faster than the leader, i.e., $v_2^0+a_2^{ac}\tau>v_1^0-\bar{a}_1\tau$.

The third condition, namely $\tau\le\frac{v_1^0\frac{\bar{a}_2}{\bar{a}_1}-v_2^0}{a_2^{ac}+\bar{a}_2}$, is missing.

In Fig. 2, the minimum safe distance is plotted versus the delay τ for different combinations of $\bar{a}_1$ and $\bar{a}_2$. As can be seen, for τ between 0.45 s and 1.3 s, longer minimum safe distances are required for the case $\bar{a}_1<\bar{a}_2$ (yellow line) than those resulting from the original RSS equation (6) (blue dashed line). The black line represents the solution presented in [4]. As can be seen, the missed condition leads to unnecessary long distances for $\tau>1.3$ s. Thus, for the presented example, the minimum distance corresponding to $\tau=2\,s$ equals 32.2 m whereas solution [4] proposes 38.2 m, which is a more pessimistic and unnecessary requirement. In other words, for such parameters, distances obtained through solution [4] are safe but can not be called minimum.

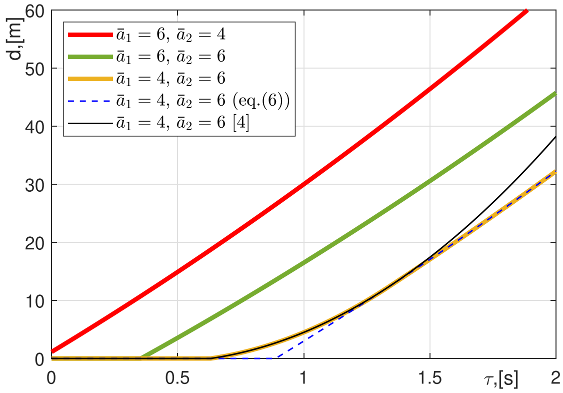

Fig. 2. The minimum safe distance calculated for the scenario with a constant acceleration of the follower. Here, $v_1^0 = 18\,m/s$, $v_2^0 = 15\,m/s$, $a_2^{ac} = 3\,m/s^2$. The deceleration capabilities of vehicles vary according to the legend.

Compared to those in [5] and [4], formulas (6)–(7) allows for correct calculating of minimum safe distances for any parameters, including any combinations of $\bar{a}_1$ and $\bar{a}_2$, and any values of τ. We emphasize that our formulas were obtained with our 3-step methodology that allowed us to receive results in an easy way without missing any conditions.

III. General Case

Now, we generalize the results above for follower's controller given by $h(t)$, where $h(t)$ is a well-behaved twice integrable bounded function: $-\bar{a}_2 \leq h(t) \leq a_2^{ac}$ for $\forall t$ where a_2^{ac} - the maximum possible acceleration. In other words, during the delay τ, the follower's acceleration/deceleration changes by the law:

$$\dot{v}_2 = h(t), \tag{8}$$

The solution of the system at the time point τ has the form below:

$$x_1(\tau) - x_2(\tau) = \begin{cases} d_0 + (v_1^0 - v_2^0)\tau - \frac{\bar{a}_1 \tau^2}{2} - H_2(\tau) \\ \quad \text{if } \tau \leq T_l, \\ d_0 + \frac{(v_1^0)^2}{2\bar{a}_1} - v_2^0 \tau - H_2(\tau) \\ \quad \text{if } \tau > T_l, \end{cases}$$

$$v_1(\tau) = \begin{cases} v_1^0 - \bar{a}_1 \tau & \text{if } \tau \leq T_l, \\ 0 & \text{if } \tau > T_l, \end{cases}$$

$$v_2(\tau) = v_2^0 + H_1(\tau), \tag{9}$$

where $H_1(\tau) = \int_0^\tau h(x)\,dx$, $H_2(\tau) = \int_0^\tau H_1(y)\,dy$.

Again, by combining (9) with the minimum braking set, we obtain the formulas for calculating the minimum safe distance. We summarize the obtained results in Prop. 1 below:

Proposition 1: Assume the following is given: τ - the response time during which the follower is unaware of emergency braking and uses the controller $h(t)$; v_1^0, v_2^0 - the initial velocities of vehicles; $\bar{a}_1$, $\bar{a}_2$ - the maximum deceleration capacities of vehicles. Then the minimum safe distance required to avoid a rear-end collision is given by:

$$d_0(\tau, h(t)) = \left[\frac{(H_1(\tau) + v_2^0)^2}{2\bar{a}_2} - \frac{(v_1^0)^2}{2\bar{a}_1} + v_2^0 \tau + H_2(\tau) \right]_+ \tag{10}$$

if $\bar{a}_1 \geq \bar{a}_2$,

$$d_0(\tau, h(t)) = \begin{cases} \Big[\frac{\bar{a}_1 \tau^2}{2} - v_1^0 \tau + v_2^0 \tau + H_2(\tau) + \\ + \left(v_2^0 + H_1(\tau) - \left(v_1^0 - \bar{a}_1 \tau \right) \right)^2 \frac{1}{2(\bar{a}_2 - \bar{a}_1)} \Big]_+ \\ \quad \text{if} \quad v_1(\tau) \leq v_2(\tau) \leq \frac{\bar{a}_2}{\bar{a}_1} v_1(\tau) \\ \left[\frac{(H_1(\tau) + v_2^0)^2}{2\bar{a}_2} - \frac{(v_1^0)^2}{2\bar{a}_1} + v_2^0 \tau + H_2(\tau) \right]_+ \\ \text{otherwise} \end{cases} \tag{11}$$

if $\bar{a}_1 < \bar{a}_2$.

Here, we require, $H_1(\tau) + v_2^0 \geq 0$ since this is exactly the follower's velocity at time τ.

Now let us assume that there exists a well-behaved function $g(t)$ such that $h(t) \leq g(t)$ for all interval $[0; \tau]$. Obviously, it follows:

$$\int_0^\tau h(x)\,dx \leq \int_0^\tau g(x)\,dx \tag{12}$$

and

$$\int_0^\tau \int_0^y h(x)\,dx\,dy \leq \int_0^\tau \int_0^y g(x)\,dx\,dy \tag{13}$$

Moreover,

$$0 \leq v_2^0 + \int_0^\tau h(x)\,dx \leq v_2^0 + \int_0^\tau g(x)\,dx \tag{14}$$

Furthermore, if $\bar{a}_1 < \bar{a}_2$ and $v_1(\tau) \leq v_2(\tau) \leq \frac{\bar{a}_2}{\bar{a}_1} v_1(\tau)$, then:

$$0 \leq v_2^0 + \int_0^\tau h(x)\,dx - v_1(\tau) \leq v_2^0 + \int_0^\tau g(x)\,dx - v_1(\tau) \tag{15}$$

Proposition 2: Assume the following is given: τ - the response time during which the follower is unaware of emergency braking and uses the controller $h(t)$; v_1^0, v_2^0 - the initial velocities of vehicles; $\bar{a}_1$, $\bar{a}_2$ - the maximum deceleration capacities of vehicles. Furthermore, there exists a well-behaved function $g(t)$ such that $h(t) \leq g(t)$ for all interval $[0; \tau]$. Then, the minimum safe distance required to avoid collisions using the real controller $h(t)$ is no longer than the distance required for the controller $g(t)$:

$$d_0(\tau, h(x)) \leq d_0(\tau, g(x)) \tag{16}$$

Proof: The proof follows directly from formulas (10)- (11) for the minimum safe distance and inequalities (12)–(15). ■

Thus, we can bound the follower's controller with some well-behaved function $g(t)$ and receive a guaranteed estimation of the minimum safe distance. Substituting the real controller $h(t)$ with computationally more tractable function $g(t)$ increases the required minimum safe distance, but can allow for an elegant form of d_0. The closer function $g(t)$ to $h(t)$, the closer obtained bound to the real one. The function $g(t)$ can have discontinues as long as the condition of twice integrability is fulfilled.

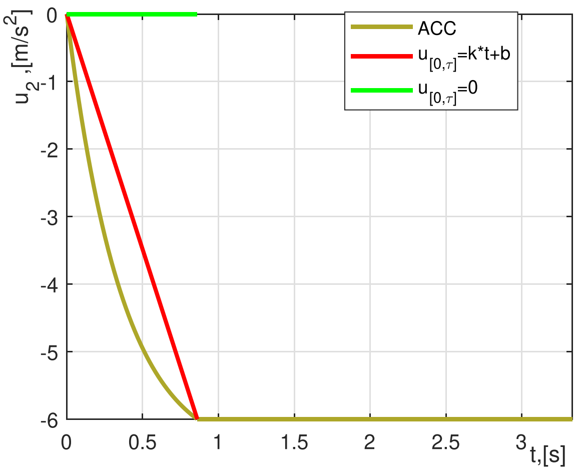

Fig. 3. The follower's controller and two bounding above functions. The ACC controller is given as $u_2(t) = k_1(x_1(t) - x_2(t) - d_0) + k_2(v_1(t) - v_2(t))$. Here, $v_1^0 = v_2^0 = 20\,m/s$, $\bar{a}_1 = \bar{a}_2 = 6\,m/s^2$, $k_1 = 1\,s^{-2}$, $k_2 = 3\,s^{-1}$.

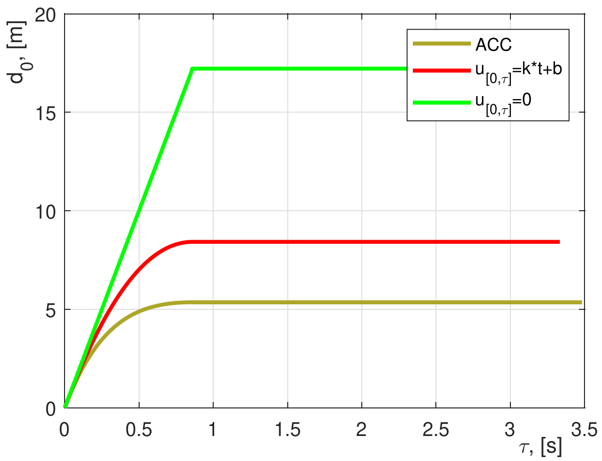

Fig. 4. The minimum safe distance calculated for the controllers presented in Fig. 3. Here, $v_1^0 = v_2^0 = 20\,m/s$, $\bar{a}_1 = \bar{a}_2 = 6\,m/s^2$.

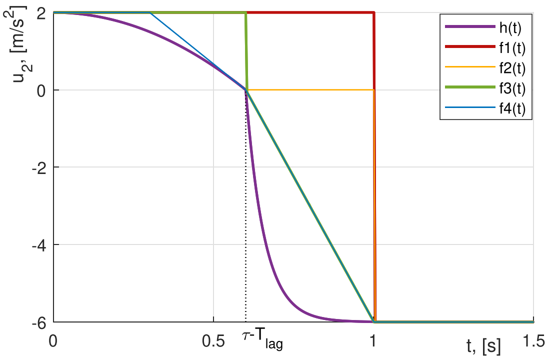

Fig. 5. The controller $h(t)$, and bounding functions $f_1(t)$, $f_2(t)$, $f_3(t)$, and $f_4(t)$. Here, $\bar{a}_1 = 5\,m/s^2$, $\bar{a}_2 = 6\,m/s^2$, $a_2^{ac} = 2\,m/s^2$, $v_1^0 = 20\,m/s$, $v_2^0 = 15\,m/s$, $\tau = 1$ s, $T_{lag} = 0.4$ s.

It is worth mentioning that the controller $h(t)$ can be dependent on time through other variables, i.e., $h(t) = \tilde{h}(x_1(t), x_2(t), v_1(t), v_2(t))$. If we have some knowledge about function $\tilde{h}$ and it is possible to find $g(t)$ such that $\tilde{h}(x_1(t), x_2(t), v_1(t), v_2(t)) \leq g(t)$, then the results above are valid, and function $g(t)$ can be used to obtain bounds on the minimum safe distance.

IV. Numerical Results

The scope of the general case presented in Section III is very wide. It is comprehensive and includes such special cases as the RSS scenario where the follower accelerates with constant acceleration or moves with a constant speed during the response time, or, as considered in [15], ACC with a constant distance policy. Among all possible special cases that can be handled with the presented in Section III formulas, the RSS assumptions can always be taken as the worst-case scenario. It means that for any follower's control law $-\bar{a}_2 \leq h(t) \leq a_2^{ac}$, we can take the bounding function $g(t) = a_2^{ac}$ and calculate safe distances with formulas (6)–(7). However, such distances are, in general, larger than necessary. It is more realistic to assume that, before reaching the maximum possible deceleration $\bar{a}_2$, the follower's controller is not constantly equal to the maximum possible acceleration a_2^{ac}. Knowledge of the follower's controller, such as intervals of accelerating/decelerating and jerk, allows for smaller safe IVDs as compared to those obtained under the RSS assumptions.

In [15], we used the 3-step approach to calculate minimum safe distances for the case when the follower uses ACC controller with a constant distance policy. Obviously, the controller $u_2(t) = k_1(x_1(t) - x_2(t) - d_0) + k_2(v_1(t) - v_2(t))$ is dependent on time through the relative distance $x_1(t) - x_2(t)$ and velocity $v_1(t) - v_2(t)$. In Fig. 3, the value of the follower's controller $h(t)$ is plotted versus time with 'ACC' label. Here, one of the possible options for an above-bounding can be a linear function in the form $k\tau + b$ (red line) or 0 (green line) corresponding to the assumption of a constant velocity during the response time. Note that at $\tau = 0.83$, ACC controller comes to the saturation point as well as the linear bounding function $k\tau + b$. In the case of the 0 bounding function, for consistent comparison, it is also assumed that the bounding controller switches to $-\bar{a}_2$ at the same moment. Corresponding minimum distances calculated by the proposed approach are depicted in Fig. 4. As can be seen, the higher the bounding function lies, the bigger distances are received. The closer the bounding function to the real controller, the tighter the bound is.

Formulas (10)–(11) in Section III assume that at the response time τ, the follower's controller reaches its lower limit, i.e., the maximum possible deceleration. However, all obtained results can be extended to a more realistic setting when after the follower made a decision to emergency brake at τ_2, it takes some time, T_{lag}, for the follower's controller to reach the maximum possible deceleration $\bar{a}_2$. In such assumptions, $\tau = \tau_2 + T_{lag}$, and an immediate decision to brake, i.e., $\tau_2 = 0$, corresponds to $\tau = T_{lag}$.

In the next example, during the response time τ_2, the follower's acceleration changes from a_2^{ac} to 0 in a parabolic manner. In the described assumptions, the controller $h(t)$ consists of two parts as shown in Fig. 5. We consider four different bounding functions for the controller $h(t)$: $f_1(t) = a_2^{ac}$ for $0 \leq$

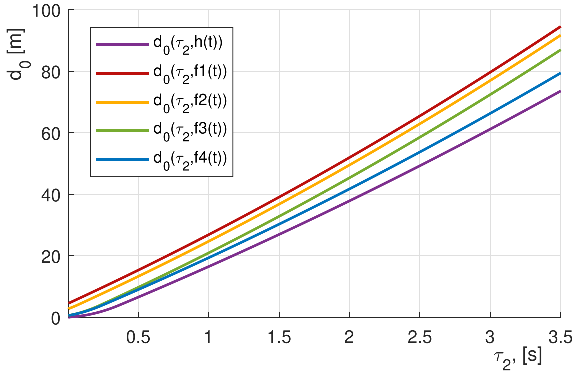

Fig. 6. The minimum safe distance calculated for the controllers $h(t)$, $f_1(t)$, $f_2(t)$, $f_3(t)$, and $f_4(t)$. Here, $\bar{a}_1 = 5\,m/s^2$, $\bar{a}_2 = 6\,m/s^2$, $a_2^{ac} = 2\,m/s^2$, $v_1^0 = v_2^0 = 15\,m/s$.

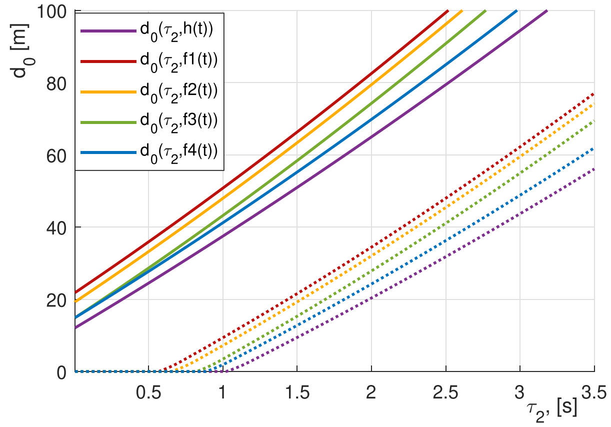

Fig. 7. The minimum safe distance calculated for the controllers $h(t)$, $f_1(t)$, $f_2(t)$, $f_3(t)$, and $f_4(t)$. Here, $\bar{a}_1 = 5\,m/s^2$, $\bar{a}_2 = 6\,m/s^2$, $a_2^{ac} = 2\,m/s^2$. Group of solid bold lines corresponds to the case $v_1^0 = 15\,m/s$, $v_2^0 = 20\,m/s$; group of dashed lines - $v_1^0 = 20\,m/s$, $v_2^0 = 15\,m/s$.

$t \leq \tau_2 + T_{lag}$ is the most pessimistic estimation; $f_2(t) = a_2^{ac}$ for $0 \leq t \leq \tau_2$ and $f_2(t) = 0$ for $\tau_2 \leq t \leq \tau_2 + T_{lag}$; $f_3(t)$ coincides with $f_1(t)$ and $f_2(t)$ on the interval $[0; \tau_2]$ whereas comprises a tighter bound for $\tau_2 \leq t \leq \tau_2 + T_{lag}$ in the form of a linear function; $f_4(t)$ is a piece-wise linear function of three parts and comprises the tightest bound from all the considered. In Fig. 5, $h(t)$ and all four bounding functions are shown for $T_{lag} = 0.4$ s [16] and $\tau = 1$ s ($\tau_2 = 0.6$ s). The minimum safe distances corresponding to the real controller $h(t)$ and four considered bounding controllers were calculated according to formulas (10)–(11) and are plotted in Figs. 6–7 for different initial velocities. As can be seen, the tighter the bounding function, the shorter safe distance corresponds to it. Thus, the function $f_1(t)$, which has the same assumptions as the RSS law, corresponds to the highest required distances. The tightest bound $f_4(t)$ gives the closest distances to the ones required by the real controller $h(t)$. It is worth noting that since functions $f_3(t)$ and $f_4(t)$ coincide during the period required for the controller to reach its saturation $-\bar{a}_2$, they require the same distance for $\tau_2 = 0$. However, since for $\tau_2 > 0$, $f_3(t) > f_4(t)$, it follows that $d_0(\tau_2, f_3(t)) > d_0(\tau_2, f_4(t))$.

V. Conclusion

We present novel contributions on the way toward the development of a complete safety framework for longitudinal driving. We extend safety analysis from [15], where a typical ACC controller with a constant space policy is assumed, by considering an arbitrary control law used by the follower during the response time. Furthermore, we enhance the RSS model [5], [4] by constructing safe IVDs for general scenarios with arbitrarily chosen deceleration capacities.

Acknowledgment

Halmstad University acknowledges the support from Knowledge Foundation ("Safety of Connected Intelligent Vehicles in Smart Cities – SafeSmart" project), from VINNOVA ("Emergency Vehicle Traffic Light Preemption in Cities – EPIC" project) and from ELLIIT Strategic Research Network. Karlsruhe Institute of Technology acknowledges the support from Helmholtz Program "Engineering Digital Futures".

References

[1] E. Uhlemann, "Peculiar times being used to analyze and plan ahead [Connected and autonomous vehicles]," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 135–138, Dec. 2020.

[2] R. Doná and B. Ciuffo, "Virtual testing of automated driving systems. A survey on validation methods," *IEEE Access*, pp. 24349–24367, 2022.

[3] J. Ploeg, E. de Gelder, M. Slavík, E. Querner, T. Webster, and N. de Boer, "Scenario-based safety assessment framework for automated vehicles," 2021. [Online]. Available: https://arxiv.org/abs/2112.09366

[4] P. Koopman, B. Osyk, and J. Weast, "Autonomous vehicles meet the physical world: Rss, variability, uncertainty, and proving safety," in *Proc. Comput. Saf., Rel., Secur.*, 2019, pp. 245–253.

[5] S. Shalev-Shwartz, S. Shammah, and A. Shashua, "On a formal model of safe and scalable self-driving cars," 2017, *arXiv:1708.06374*.

[6] J. Thunberg, N. Lyamin, K. Sjöberg, and A. Vinel, "Vehicle-to-vehicle communications for platooning: Safety analysis," *IEEE Netw. Lett.*, vol. 1, no. 4, pp. 168–172, Dec. 2019.

[7] P. F. Orzechowski, K. Li, and M. Lauer, "Towards responsibility-sensitive safety of automated vehicles with reachable set analysis," in *Proc. IEEE Int. Conf. Connected Veh. Expo*, 2019, pp. 1–6.

[8] M. Naumann et al., "On responsibility sensitive safety in car-following situations - A parameter analysis on German highways," in *Proc. IEEE Intell. Veh. Symp.*, 2021, pp. 83–90.

[9] Y. Huang, M. S. Elli, J. Weast, Y. Lou, S. Lu, and Y. Chen, "Rss model calibration and evaluation for AV driving safety based on naturalistic driving data," *IFAC-PapersOnLine*, vol. 54, no. 20, pp. 430–436, 2021.

[10] A. Rodionova, I. Alvarez, M. S. Elli, F. Oboril, J. Quast, and R. Mangharam, "How safe is safe enough? Automatic safety constraints boundary estimation for decision-making in automated vehicles," in *Proc. IEEE Intell. Veh. Symp.*, 2020, pp. 1457–1464.

[11] C. Chai, X. Zeng, X. Wu, and X. Wang, "Safety evaluation of responsibility-sensitive safety (RSS) on autonomous car-following maneuvers based on surrogate safety measurements," in *Proc. IEEE Intell. Transp. Syst. Conf.*, 2019, pp. 175–180.

[12] C. Chai, X. Zeng, X. Wu, and X. Wang, "Evaluation and optimization of responsibility-sensitive safety models on autonomous car-following maneuvers," *Transp. Res. Rec.*, vol. 2674, no. 11, pp. 662–673, 2020.

[13] S. Liu et al., "Calibration and evaluation of responsibility-sensitive safety (RSS) in automated vehicle performance during cut-in scenarios," *Transp. Res. Part C: Emerg. Technol.*, vol. 125, 2021, Art. no. 103037.

[14] G. Sidorenko, J. Thunberg, K. Sjöberg, A. Fedorov, and A. Vinel, "Safety of automatic emergency braking in platooning," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2319–2332, Mar. 2022.

[15] G. Sidorenko, D. Plöger, J. Thunberg, and A. Vinel, "Emergency Braking with acc: How much does v2v communication help?," *IEEE Netw. Lett.*, vol. 4, no. 3, pp. 157–161, Sep. 2022.

[16] S. Kallenbach, "Truck platooning—A pragmatic approach," *Fahrerassistenz–Systeme*, pp. 132–157, 2019.