Dynamic Risk Management for Safely Automating Connected Driving Maneuvers

Marta Grobelna
Fraunhofer IKS
Munich, Germany
marta.grobelna@iks.fraunhofer.de

João-Vitor Zacchi
Fraunhofer IKS
Munich, Germany
joao-vitor.zacchi@iks.fraunhofer.de

Philipp Schleiß
Fraunhofer IKS
Munich, Germany
philipp.schleiss@iks.fraunhofer.de

Simon Burton
Fraunhofer IKS
Munich, Germany
simon.burton@iks.fraunhofer.de

***Abstract*—Autonomous vehicles (AV)s have the potential for significantly improving road safety by reducing the number of accidents caused by inattentive and unreliable human drivers. Allowing the AVs to negotiate maneuvers and to exchange data can further increase traffic safety and efficiency. Simultaneously, these improvements lead to new classes of risk that need to be managed in order to guarantee safety. This is a challenging task since such systems have to face various forms of uncertainty that current safety approaches only handle through static worst-case assumptions, leading to overly restrictive safety requirements and a decreased level of utility. This work provides a novel solution for dynamic quantification of the relationship between uncertainty and risk at run time in order to find the trade-off between system's safety and the functionality achieved after the application of risk mitigating measures. Our approach is evaluated on the example of a highway overtake maneuver under consideration of uncertainty stemming from wireless communication channels. Our results show improved utility while ensuring the freedom of unacceptable risks, thus illustrating the potential of dynamic risk management.**

***Index Terms*—connected autonomous driving, dynamic safety management, risk assessment, uncertainty quantification**

I. Introduction

According to the US National Highway Traffic Safety Administration, human error can be attributed to approximately 94% of accidents on the roads, whereby about 41% of them were caused by recognition errors that include driver's inattention, distractions, and inadequate surveillance [1]. Autonomous vehicles (AV)s have the potential for making roads significantly safer by restricting the impact of potentially unreliable human drivers. However, the introduction of AVs comes at the price of new classes of risk that must be managed before the systems can be considered safe. In particular, the safety of the perception and decision making subsystems needs to be assured as they determine the AVs' behavior. Unfortunately, the functional safety standard for the automotive domain, ISO 26262 [2], does not provide guidance on dealing with hazards related to functional deficits of these subsystems. Consequently, there is an urgent need for approaches solving these problems.

The origins of the hazards might be uncertainties, i.e. lacks of knowledge, that might exacerbate the AV's capability to understand a driving situation. The uncertainty may arise from the difficulty to correctly understand a certain situation due to environmental conditions that may affect the performance of the perception architecture [3], [4]. Further, the AV cannot be certain about the behavior of other traffic participants, in particular because the actions of the AV influence the actions of other traffic participants, and vice versa [5].

While the former source of uncertainty can be reduced by provision of a range of sensors required to achieve a reliable level of perception, the latter can be reduced by extending the perception horizon of AVs by the use of wireless communication like Vehicle-to-Vehicle (V2V) communication, thus enabling a further increase in utility and safety of AVs [6]. Specifically, the use of V2V communication enables AVs to identify and circumvent hazardous situations that could not have been anticipated by solely relying on an AV's individual environment perception sensors [7]. Further, since the information wirelessly exchanged in vehicular networks is less sensitive to weather conditions and occlusion than sensors, costs as well as the complexity of the AV induced by redundant sensors can be reduced. However, V2V communication itself may introduce additional uncertainties due to latency and packet drop related issues that must be counteracted within the system safety concept.

The focus of this work is on the quantification of uncertainties provided by poor quality of the V2V communication links and provides means that can minimize their impact. The remainder of this paper is organized as follows. Sec. II introduces the required formalization. In Sec. III the proposed maneuver monitoring system is discussed in detail. Sec. IV presents the uncertainty model in the Cooperative Awareness Message (CAM) data, as well as the risk model used for collision prediction. Sec. V contains numerical evaluation of the proposed approach based on a highway overtake maneuver example. Sec. VI briefly discusses how the proposed approach needs to be extended to be applicable to more complex scenarios. Finally, Sec. VII concludes the paper and proposes future work.

II. Preliminaries

The terms and notation that are used throughout this paper are briefly introduced in this section.

The set of real numbers is denoted by $\mathbb{R}$, the set of positive (negative) real numbers including zero is denoted by $\mathbb{R}_{\geq 0}$ ($\mathbb{R}_{\leq 0}$), and the set of positive (negative) real excluding zero by $\mathbb{R}_{>0}$ ($\mathbb{R}_{<0}$).

In this work we consider a single host vehicle (HV) $\mathcal{V}_{\mathrm{H}}$ and a set of n remote vehicles (RV)s denoted by $\mathcal{V}_i$ where i is the identification number of the RV, hence, $i \in \{1, \ldots, n\}$. Further the placeholder $\Diamond$ is used whenever either HV or any of the RVs is meant, thus $\Diamond \in \{H\} \cup \{1, \ldots, n\}$. All vehicles are equipped with on-board sensors such as cameras, radar, Global Navigation Satellite System (GNSS) receivers, or Light Detection and Ranging (LiDAR), as well as V2V communication modules and a sensor fusion module. All vehicles have a common understanding of time. The point in time at which the connections among all vehicles are established is denoted by t_0. The current time is denoted by t_{cur}. Further, all vehicles are aware of a global left-handed Cartesian coordinate system.

Each vehicle is characterized by a number of parameters, called state, that can vary during run time.

Definition 1 (**State $\mathbf{s}_\Diamond^t$**). *A* state *of a vehicle $\mathcal{V}_\Diamond$ at a point in time $t \in \mathbb{R}_{\geq 0}$ is the tuple $\mathbf{s}_\Diamond^t := \left(\tilde{x}_\Diamond^t, \tilde{y}_\Diamond^t, \tilde{\varphi}_\Diamond^t, \tilde{v}_\Diamond^t, \tilde{a}_\Diamond^t\right)$, consisting of the x and y positions of the geometric center of the rectangle representing the vehicle $\left(\tilde{x}_\Diamond^t, \tilde{y}_\Diamond^t\right) \in \mathbb{R}_{\geq 0}^2$, the heading $\tilde{\varphi}_\Diamond^t \in [-90°, 90°] \subset \mathbb{R}$, the scalar velocity $\tilde{v}_\Diamond^t \in \mathbb{R}_{\geq 0}$, and the scalar acceleration $\tilde{a}_\Diamond^t \in \mathbb{R}$. The state at t_0 is called the* initial state.

During the maneuver execution CAMs are continuously exchanged among the vehicles in order to gain information about each other states. A CAM generated by a vehicle $\mathcal{V}_\Diamond$ at time $t_{\mathrm{gen}} \in \mathbb{R}_{\geq 0}$ contains the state of the RV at the generation time point, i.e. $\mathbf{s}_\Diamond^{t_{\mathrm{gen}}}$. For the sake of simplicity, the generation time of the CAM t_{gen} in $\mathbf{s}_\Diamond^{t_{\mathrm{gen}}}$ as well as in the components of the state will be omitted and instead $\mathbf{s}_\Diamond$ and $\left(\tilde{x}_\Diamond, \tilde{y}_\Diamond, \tilde{\varphi}_\Diamond, \tilde{v}_\Diamond, \tilde{a}_\Diamond\right)$ is written.

Definition 2 (**CAM Age Δ_{CAM}**). *The* age of a CAM *(or* CAM age*) Δ_{CAM} that was generated at $t_{gen,\Diamond}$ is defined as the difference between the current time t_{cur} and $t_{gen,\Diamond}$, hence, $\Delta_{CAM} := t - t_{gen,\Diamond}$.*

Given a CAM from an RV $\mathcal{V}_i$ the HV forecast the state that $\mathcal{V}_i$ will reach within the next $k \in \mathbb{R}_{\geq 0}$ seconds, i.e. at a future point in time $t_{\mathrm{fut}} := t_{\mathrm{cur}} + k$. The prediction horizon for this RV is then defined as follows

Definition 3 (**Prediction Horizon τ_i**). *Given the last received CAM from an RV $\mathcal{V}_i$ and a future time point t_{fut} at which the HV needs to know the state of the RV. The* prediction horizon *regarding $\mathcal{V}_i$ is given by the difference of the two points in time, $\tau_i := t_{fut} - t_{gen,i}$.*

The state that the RV will reach within a prediction horizon τ_i is called future state and is given by $\mathbf{s}_\Diamond^{t_{\mathrm{fut}}}$.

The longitudinal velocity of a $\mathcal{V}_\Diamond$, $v_{\Diamond,x}$, is given by $v_{\Diamond,x} := v_\Diamond \cdot \cos\left(\varphi_\Diamond\right)$ and the lateral velocity, $v_{\Diamond,y}$, is given by $v_{\Diamond,y} := v_\Diamond \cdot \sin\left(\varphi_\Diamond\right)$. There is an explicit differentiation between acceleration and deceleration of a vehicle that is denoted by $\overline{a}_\Diamond$ and $\underline{a}_\Diamond$, respectively. The acceleration (deceleration) $\overline{a}_\Diamond$ ($\underline{a}_\Diamond$) can be decomposed into longitudinal acceleration (deceleration) $\overline{a}_{\Diamond,x} := \overline{a}_\Diamond \cdot \cos\left(\varphi_\Diamond\right)$ ($\underline{a}_{\Diamond,x} := \underline{a}_\Diamond \cdot \cos\left(\varphi_\Diamond\right)$) and lateral acceleration (deceleration) $\overline{a}_{\Diamond,y} := \overline{a}_\Diamond \cdot \sin\left(\varphi_\Diamond\right)$ ($\underline{a}_{\Diamond,y} := \underline{a}_\Diamond \cdot \sin\left(\varphi_\Diamond\right)$).

The goal of estimating the future states is the assessment of the risk that a collision will occur within the prediction horizon. The following definition provides the risk term as given by the functional safety standard IEC 61508.

Definition 4 (**Risk $\mathcal{R}$**). Risk *is the combination of the probability of occurrence of harm, the severity of that harm and the controllability.*

Despite the application of risk reduction measures during the design time, it is infeasible to fully eliminate the risk of a harm. A certain residual risk will always remain that needs to be decreased to an acceptable level. In this work, it is assumed that the level of an acceptable residual risk is a parameter that is specific to the function and is determined during development by the vehicle manufacturer or dictated by future standards or regulations.

Despite the fact that the HV estimates the risk of a collision at equidistant points in time, it also continuously estimates the risk at critical points of its planned trajectory which are associated with a certain RV.

Definition 5 (**Critical Point $\mathcal{P}_i$**). *A* critical point *of a trajectory associated with an RV $\mathcal{V}_i$, is the point obtained by intersecting the trajectories of the RV and the HV.*

III. Approach

Safety assurance of AV is one of the central topics of this research field as it is one of the main factors that can convince the society about the benefits of AVs. Unfortunately, assuring that such system will behave safely under any conditions is a challenging task. Due to the complexity and the non-determinism, not all dangerous situations can be tested during the design time of the AV. Consequently, a monitor is necessary that can estimate the safety of a maneuver during run time when more details about the states of the vehicles in the proximity of the AV and the environment are available. Based on this information, collision risk during run time can be estimated and, if necessary, adaptation steps can be planned in order to reduce the risk which will provide dynamic risk management for the system [8].

A maneuver is safe when at each point in time the AV executing the maneuver can maintain a safe distance to every vehicle within its proximity, i.e the vehicles immediate in front, behind and next to it. The prominent Responsibility-Sensitive Safety (RSS) approach [9] proposes a set of mathematical formulas describing basic traffic laws, such as safe longitudinal and lateral distances, that have to be respected in order to guarantee safety. The approach, however, disregards two important issues. First, RSS does not consider the fact that all sensors suffer from noise which causes uncertainty about the vehicle's true state. This problem was already addressed in [10], however, the authors only provided general approaches to solve the problem. Still a mathematical approach is missing that would enable fast and easy evaluation of the RSS formulas under consideration of uncertainties. Another approach was proposed in [11] where the uncertainty was considered in the state prediction by performing reachability analysis whereby reachable sets were over-approximated in order to account for uncertainties. However, the authors only considered uncertainties caused by measurement imprecision. Issues such as data aging were not considered.

The second issue that RSS does not consider is the fact that it is more valuable to forecast if a collision will occur in the future, since this information could be used to adjust the trajectory before the violation of a safety requirement. RSS does not explain how to make such predictions, and in particular it disregards the problem of uncertainty propagation for such predictions.

This work addresses the two shortcomings of RSS. Thus, the contribution of this paper is the following.

- We propose an approach for predicting vehicle states in order to evaluate the RSS formulas at a future point in time;
- We develop a risk model that considers data uncertainty and its propagation during the prediction.

There are many sources of uncertainty that can influence the collision risk assessment such as imprecision of the sensor measurements, the unpredictability of the environment, or the ambiguous behavior of machine learning algorithms. However, in this paper we focus on uncertainty caused by poor quality of V2V communication channels [3].

We consider the situation where a single HV plans to execute a cooperative maneuver with a number of RVs it exchanges CAMs with, using for instance, the protocol presented in [12] that consists of a maneuver negotiation, maneuver planning and maneuver execution phases. We focus on the phase when the maneuver negotiation was already finished and all vehicles agreed on the desired cooperative maneuver that now shall be planned and monitored.

Given the CAM data from all RVs participating in the maneuver, the HV can plan the desired trajectory. To this end, first the HV predicts future states of the RVs. Hereby the quality of service of the communication link plays the key role, as the prediction precision crucially depends on it. In particular, the worse the communication quality is, the more pessimistic the predictions of the RVs' parameters are. This is caused by the fact that poor communication quality increases the probability of message losses which in turn increases the age of the data contained in a CAM. This relationship has also a direct impact on HV's decisions regarding the maneuver safety. More pessimistic predictions will cause a higher number of false positives, meaning that the HV will more often classify a maneuver as unsafe, even though, with more recent CAM data, the HV would have classified the same maneuver as safe.

A. Trajectory Planning and Maneuver Monitoring

The goal of the maneuver planning phase is twofold. First, a roughly safe trajectory is planned where already a risk reducing measure in form of a static safety distance is integrated. Second, the residual risk of a collision is estimated and in case the predicted level of the residual risk is unacceptable, a further risk reducing measure is applied. The estimation of the residual risk is based on a collision prediction at critical points (see Def. 5) of the planned maneuver trajectory. Note that in this phase it is sufficient to focus only on critical points, since it is infeasible to predict safety for the entire maneuver due to the non-deterministic behavior of the environment. Instead, the goal is to estimate a rough safety of the maneuver that is still better than not estimating the safety at all. To guarantee safety at the remaining points of the trajectory, a monitor is deployed that continuously estimates the risk at equidistant time points during the maneuver execution. The monitor predicts the future states of the RVs that they will reach within a prediction horizon (see Def. 3) and estimates the residual risk of a collision under consideration of the current level of uncertainty in the CAM data. In case the level of the residual risk is too high, the HV will execute a minimal risk maneuver.

Further, a mechanism for maneuver parameter adjustment is provided in order to increase HV's reliability. If the estimated residual risk is too high at any point in time, the HV can propose adjustments of RVs' maneuver parameters, such as velocity and acceleration, in order to decrease the risk again to an acceptable level. However, one has to take into account that the proposed adjustments might not be feasible for an RV due to obstacles not visible to the HV or other technical limits. In such case, the HV is forced to execute a minimal risk maneuver. Otherwise, the HV can proceed as planned.

IV. Uncertainty and Risk Model

The estimation of the residual risk of a potential collision requires forecasting the future states of the HV as well as of the RVs' driving in its proximity. This section discusses the three main components of the approach. First, the model of uncertainty in the CAM data is explained. Second, the functions needed to calculate the future states are presented. Finally, the risk model is introduced.

A. Uncertainty Model for CAM Data

In this work we focus on the case where the only source of information about the current sates of the vehicles in the proximity of the HV are the CAMs exchanged between the HV and the RVs. In such case poor quality of a communication channel, that cause CAM losses, leads to uncertainty about the true state of the corresponding RV. Further, in order to *prevent* a dangerous situation the HV has to predict the state of the RV that it will reach within the next k seconds from the current point in time on, based on the data shared in the CAMs. Thus, the uncertainty caused by a lost CAM is propagated throughout the entire prediction horizon. In particular, the HV cannot be certain if the corresponding RV accelerated, decelerated or stayed at constant velocity after the generation of the last CAM. In order to ensure safety of the maneuver the HV wants to execute, this uncertainty has to be quantified. For this purpose the HV has to make assumptions about the behavior of the RVs.

Consider an RV $\mathcal{V}_i$ that generated its last CAM at t_{gen} and the prediction horizon for this RV is τ_i. The first assumption concerns the velocity of the RV.

(A 1) $0 \leq v_i(t) \leq v^{\max},\ \forall t \in [t_{\text{gen}}, \tau_i]$.

It is assumed that during the prediction horizon the velocity of the RV is non-negative and has an upper bound which might be determined by the speed limit of the road.

Due to the fact that each vehicle has a limited acceleration and deceleration capability, for each vehicle the HV assumes that, at each point in time, its acceleration will remain within a certain fixed interval. Hence, the second assumption regards the boundaries of the acceleration of the RV.

(A 2) $b_i^{\max} \leq a_i(t) \leq a_i^{\max},\ \forall t \in [t_{\text{gen}}, \tau_i]$.

Finally, the change in the acceleration over time, i.e. the jerk, is also limited. This means that at each point in time the acceleration of an RV can neither decrease nor increase faster than a threshold j_i^{asp}. Therefore, the last assumption made by HV is the following

(A 3) $\left|\frac{da_i(t)}{dt}\right| \leq j_i^{\text{asp}},\ \forall t \in [t_{\text{gen}}, \tau_i]$.

The uncertainty in the CAM data is reflected by j_i^{asp}, which defines the upper and lower bound for the change in the acceleration that might have happened since the generation of the last CAM. The older the CAM is, the greater the assumed deviation in the acceleration of the corresponding RV is assumed by the HV. In order to avoid over-conservative assumptions about j_i^{asp}, the value of this parameter is selected based on the jerk of the corresponding RV that the HV measured in the past. In case the absolute value of the jerk, $|\tilde{j}_i|$, was lower than a jerk that still guarantees comfortable ride j^{cmf}, then the HV assumes that the corresponding RV will proceed driving with the comfortable jerk during the entire prediction horizon. As soon as this value is exceeded, the HV assumes that the RV behaves more aggressively and sets j_i^{asp} to a maximal value of $j^{\max}(> j^{\text{cmf}})$. All in all, j_i^{asp} regarding an RV $\mathcal{V}_i$ is given by

$$j_i^{\text{asp}}(\tilde{j}_i) := \begin{cases} j^{\text{cmf}}, & \left|\tilde{j}_i\right| \leq j^{\text{cmf}} \\ j^{\max}, & \left|\tilde{j}_i\right| > j^{\text{cmf}} \end{cases} \tag{1}$$

For the sake of simplicity, from now on we write j_i^{asp} when $j^{\text{asp}}(\tilde{j}_i)$ is meant.

B. Motion Prediction

Given the uncertainty model, the function of time for forecasting the acceleration of an RV can be defined. The velocity and position of the vehicle can be obtained by integration of the function with respect to time.

Since the HV cannot know if the corresponding RV will accelerate or decelerate after the generation of the last CAM, the HV has to consider both cases. For the estimation of the velocity and the position, the HV assumes the worst case, i.e., the case for which the distance to the corresponding RV is smaller. If the distance calculated under the assumption of acceleration is smaller than the distance calculated under the assumption of deceleration, the velocity and the position are calculated under consideration of acceleration. Otherwise, deceleration is assumed. Since the calculations for the acceleration and deceleration are similar, here only the calculations under the assumption of acceleration are explained.

Due to (A 2) the HV cannot assume that during the entire prediction horizon the jerk is constantly at j_i^{asp} but has to drop to zero as soon as the upper bound of the acceleration or velocity is reached. The point in time of reaching the maximal acceleration, denoted by $t_{a,i}^{\max}$, can be calculated using the basic law of motion

$$t_{a,i}^{\max} = \frac{a_i^{\max} - \tilde{a}_i}{j_i^{\text{asp}}}, \tag{2}$$

where $\tilde{a}_i$ is the acceleration of $\mathcal{V}_i$ shared in the last CAM. Now the question is whether the time of reaching the maximal acceleration is smaller than the time of reaching the maximal velocity. This can be evaluated using the inequality

$$\underbrace{\frac{1}{2} \cdot j_i^{\text{asp}} \cdot (t_{a,i}^{\max})^2 + \tilde{a}_i t \cdot t_{a,i}^{\max} + \tilde{v}_i}_{=:\Psi} \overset{?}{<} v^{\max} \tag{3}$$

where $\tilde{v}_i$ is the velocity of $\mathcal{V}_i$ shared in the last CAM. If (3) holds, i.e. $\Psi < v^{\max}$, then the time of reaching the upper bound for the acceleration is smaller than the time of reaching the upper bound for the velocity $t_{v,i}^{\max}$. The time $t_{v,i}^{\max}$ is given by

$$\begin{aligned} t_{v,i}^{\max} = \frac{1}{a_i^{\max}} \cdot \Big(-\frac{1}{2} \cdot j_i^{\text{asp}} \cdot (t_{a,i}^{\max})^2 - \\ \tilde{a}_i \cdot t_{a,i}^{\max} + a_i^{\max} \cdot t_{a,i}^{\max} + v_i^{\max} - \tilde{v}_i \Big) \end{aligned} \tag{4}$$

when (3) holds. Otherwise, $t_{v,i}^{\max}$ can be obtained by solving the following equation for $t_{v,i}^{\max}$

$$v_i^{\max} = \frac{1}{2} \cdot j_i^{\text{asp}} \cdot (t_{v,i}^{\max})^2 + \tilde{a}_i \cdot t_{v,i}^{\max} + \tilde{v}_i. \tag{5}$$

This equation delivers two solutions for $t_{v,i}^{\max}$, however, only the minimal non-negative solution is considered.

Given the two points in time, the prediction function for the upper bound of acceleration as a function of time, denoted by $\overline{a}_i$, can be defined. Fig. 1 illustrates the acceleration depending on time in case (3) holds. Until reaching $t_{a,i}^{\max}$, the acceleration can increase linearly at the constant rate of j_i^{asp}. When the time $t_{a,i}^{\max}$ is reached, the acceleration stays constant at $a^{\max}$ until the maximal velocity at time $t_{v,i}^{\max}$ is reached and the acceleration has to fall to zero in order to respect assumption (A 1).

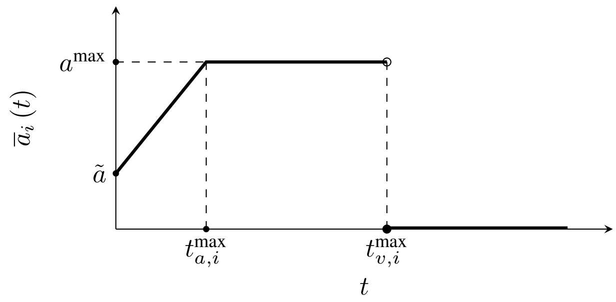

Fig. 1. HV's model of the maximal acceleration for the case when the point in time of reaching the maximal acceleration is smaller than the time of reaching the maximal velocity.

All in all, the prediction function for acceleration as a function of the time horizon is defined as follows

$$\overline{a}_i\left(\tau_i, \tilde{a}_i, \tilde{v}_i, \tilde{j}_i\right) :=$$

$$\begin{cases} j_i^{\text{asp}} \cdot \tau_i + \tilde{a}_i, & \tau_i < t^{\max}_{a,i} \text{ and } \Psi < v^{\max} \text{ or } \tau_i < t^{\max}_{v,i} \\ & \text{and } \Psi \geq v^{\max}, \\ a^{\max}, & t^{\max}_{a,i} \leq \tau_i < t^{\max}_{v,i} \text{ and } \Psi < v^{\max}, \\ 0, & \tau_i \geq t^{\max}_{v,i}. \end{cases} \tag{6}$$

The first case corresponds to the situation where the vehicle can neither reach its maximal acceleration nor its maximal velocity during the prediction horizon. The second case refers to the situation when the vehicle is already driving with its maximal acceleration, however, the maximal velocity was not reached yet. Finally, the last case corresponds to the situation where the vehicle reached its maximal velocity and cannot accelerate further.

It remains to define when a distance is considered to be safe and how the risk of a collision can be estimated.

C. Safe Distance

Given the predicted positions and velocities of the RVs, the HV can estimate if it will maintain a safe distance within the next k seconds. A distance between two vehicles is assumed to be safe if a vehicle can properly react to an emergency brake of a vehicle driving in front of it. Here, a proper reaction means that the distance after both vehicles come to a standstill is non-negative. The safety of the longitudinal distance can be evaluated using the following formula provided by RSS:

$$\mathcal{D}_{\text{x}} := \underbrace{\left(x_F - \frac{v_F^2}{2 \cdot b_F^{\text{max,x}}}\right)}_{\text{Front vehicle}} - \underbrace{\left(x_R + v_R \cdot \rho - \frac{v_R^2}{2 \cdot b_R^{\text{min,x}}}\right)}_{\text{Rear vehicle}}. \tag{7}$$

Here, x_F (x_R) is the x positions of the front (rear) vehicle, v_F (v_R) is the velocity of the front (rear) vehicle, $b_F^{\text{max,x}}$ is the maximal longitudinal brake capacity of the front vehicle, and $b_R^{\text{min,x}}$ is the minimal longitudinal brake capacity of the rear vehicle. The first term describes the distance covered by the front vehicle and the second term describes the distance covered by the rear vehicle. Note that for the calculation of the distance covered by the rear vehicle a reaction time ρ was considered. The evaluation of the lateral distance $\mathcal{D}_{\text{y}}$ can be calculated analogously.

If the longitudinal or the lateral distance is non-negative, the HV can assume that the distance will remain safe for the next k seconds. Otherwise, the HV cannot be sure if the safety distance will be maintained.

D. Risk Model

In context of road safety, a natural indicator for safety is the distance between the vehicles. The larger the distance is, the lower is the probability of a collision. Consequently, the idea for a risk assessment function, and thus its associated reduction measure is to assign probability of a collision to a distance. Hence, a mapping from the set of real numbers to the real-valued interval $[0, 1]$ is needed. A well-known function that computes such a mapping is the *logistic function*. In order to assign lower risk to greater distances, the risk function is symmetric to the logistic function with respect to the y-axis. Further, the prediction horizon is considered in the model since a larger prediction horizon causes more pessimistic predictions. However, the risk of a collision that was estimated using a longer prediction horizon should be lower, as within a longer prediction horizon the situation on the road might change considerably. In order to capture this relationship, the prediction horizon is included into the risk assessment. Simultaneously, one has to consider the CAM age Δ_{CAM} (see Def. 2) that was used to predict the future state of an RV $\mathcal{V}_i$. The greater Δ_{CAM} is, the more unreliable is the data contained in it, resulting in a more imprecise predicted state of the RV. Consequently, the model assigns higher risk to distances that were calculated with older CAMs. All in all, the risk assessment function $\mathcal{R}_{\text{x}}$ is given by

$$\mathcal{R}_{\text{x}}(\mathcal{D}_{\text{x}}, \Delta_{\text{CAM}}, \tau_i) := \frac{\Delta_{\text{CAM}}}{1 + \tau_i \cdot \exp(c \cdot \mathcal{D}_{\text{x}})}. \tag{8}$$

Note that the velocities of the vehicles are implicitly considered in the risk model in the calculation of $\mathcal{D}_{\text{x}}$ (see (7)). The risk in lateral direction can be calculated analogously. An additional constant c allows to tune the slope of the tangent at the turning point of the curve making the mapping between the distances and risk more distinguishable to prevent rounding errors.

Fig. 2 illustrates the risk function. For larger t_{pred} the turning point of the curve is more on the negative side of the x-axis,

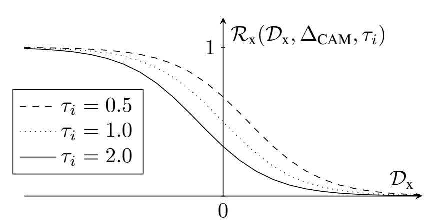

Fig. 2. Collision risk assessment function.

which means that it assigns a smaller risk to distances that were predicted using a larger prediction horizon compared to the risk assigned to the same distance but predicted using a shorter prediction horizon. Note that here it is assumed that the severity and controllability are constant for every collision and can consequently be disregarded. However, in future work models for collision severity and controllability will be provided.

E. Maneuver Parameter Adjustment

As soon as the HV forecasts that the risk of a collision is too high, it calculates adjustments for the maneuver parameters for the RV that can reduce the collision risk to an acceptable level. As already mentioned, the risk threshold for acceptable risk denoted by $\mathcal{R}_{\text{tr}}$ is specified during the development time of the system. Since the risk function given in (8) is invertible, one can compute the critical distance $\mathcal{D}^*$ corresponding to the risk threshold using the inverse function as follows

$$\mathcal{D}^* := \ln\left(\frac{\Delta_{\text{CAM}} - \mathcal{R}_{\text{tr}}}{\mathcal{R}_{\text{tr}} \cdot \tau_i}\right) \cdot \frac{1}{c}, \tag{9}$$

Hence, $\mathcal{D}^*$ denotes a distance threshold that has to be maintained in order to keep the collision risk at an acceptable level. Given the distance threshold, the HV can estimate the velocity v^{opt} of the RV that will respect the threshold. In case the RV is the front vehicle, its velocity must be adjusted such that the distance defined in (7) is equal to the distance threshold. Consequently, the maximal acceptable velocity of the RV is attained by solving the above equation for v^{opt} which is given by

$$v_x^{\text{opt}} = \sqrt{2 \cdot b_F^{\text{max,x}} \cdot \left(-\mathcal{D}_x^* + x_F - x_R - v_R^x \cdot r + \frac{(v_R^x)^2}{2 \cdot b_R^{\text{min,x}}}\right)} \tag{10}$$

whereby $\mathcal{D}_x^*$ is the required longitudinal component of $\mathcal{D}^*$. The calculations are analogous for the lateral direction and the case where the RV is the rear vehicle. In case the calculated velocity can be achieved by the corresponding RV such that the acceleration and jerk limits given in assumptions (A 2) and (A 1) can be respected, the HV can send a proposition to the RV. Otherwise, if the HV notices that the assumptions cannot be respected, it asks the corresponding RV to accelerate or decelerate with the maximal possible acceleration. However, this is only allowed a limited number of times. The exact threshold for the number of trials will be estimated during the evaluation.

V. Experimental Results

The approach is applied to an analysis of a highway overtake maneuver. To this end, a MATLAB framework was developed allowing simulations of randomly generated overtake maneuvers with the general setup depicted in Fig. 3. The scenario involves one HV $\mathcal{V}_{\text{H}}$ and two RVs, $\mathcal{V}_1$ and $\mathcal{V}_2$. The HV intends to overtake the RV $\mathcal{V}_2$ driving in front of it. It is assumed that the maneuver negotiation phase is already finished and the execution phase begins. The overtake trajectory of the HV is calculated using the optimal control approach based on Frenet-Serret Frames proposed in [13]. The HV needs to maintain a safe distance to the RV driving in front of it, as well as to the RV driving on the overtaking lane as it is the HV's responsibility to perform a safe lane change. At the beginning the HV first forecasts the safety of the maneuver at the two critical points $\mathcal{P}_1$ and $\mathcal{P}_2$ marked by the two rectangles in Fig. 3.

TABLE I. PARAMETER VALUES FOR THE SIMULATION.

Parameter	Value	Unit
j^{max}	2	$[\text{m}\,\text{s}^{-3}]$
j^{cmf}	0.9	$[\text{m}\,\text{s}^{-3}]$
CAM frequency	10	[Hz]
safety check frequency	20	[Hz]
speed limit (v^{max})	130	$[\text{km}\,\text{h}^{-1}]$
t_{pred}	2	[s]
lane width	3	[m]
$\mathcal{R}_{\text{tr}}$	0.033	-

The framework classifies a maneuver as *safe* when safe distances were maintained at each point in time and the maneuver was successful. In case a safe distance could not be maintained the maneuver is classified as *unsafe* and the simulation is immediately interrupted.

The simulation framework requires the setting of several parameters that are given in Table I. The boundaries for the jerk were selected according to the values proposed in [14]. The maximal jerk value is set to $2\,\text{m}\,\text{s}^{-3}$ which models the behavior of an aggressive driver, while the comfortable jerk is set to $0.9\,\text{m}\,\text{s}^{-3}$ which refers to a normal driving behavior. The CAMs should be exchanged every $0.1\,\text{s}$, so the HV has to estimate the maneuver safety at half frequency of the CAM frequency in order to execute the needed calculations using the most recent CAM data. The speed limit on the road, that is equal to v^{max} from (A 1), is limited to $130\,\text{km}\,\text{h}^{-1}$. The amount of time the HV wants to see into the future is set to $2\,\text{s}$. The threshold for the acceptable risk $\mathcal{R}_{\text{tr}}$ was derived using (8). Here, the distance after an emergency brake was set to zero as proposed by RSS. In best case the CAM age is equal to the time between two successive CAMs, i.e $0.1\,\text{s}$ as the CAM frequency is set to $10\,\text{Hz}$. The prediction time is set here to $2\,\text{s}$. If the values are set into (8) one obtains the value 0.033.

In order to showcase our approach, 400 random overtake scenarios were generated, where the *x* position of the front vehicle, and the velocities of all vehicles were selected randomly. Table II shows the parameter values used to generate the scenarios. In order to generate sensible scenarios, i.e. those that are initially legal, some restrictions regarding the initial *x* position and the velocities were undertaken. The upper bounds for the velocity of $\mathcal{V}_1$ and $\mathcal{V}_{\text{H}}$ were set to the road speed limit of $130\,\text{km}\,\text{h}^{-1}$. The lower bound of HV's velocity was set to the speed of the vehicle $\mathcal{V}_2$, that HV aims to overtake, plus $10\,\text{km}\,\text{h}^{-1}$ such that HV's velocity is sufficiently high to overtake the front vehicle. The boundaries

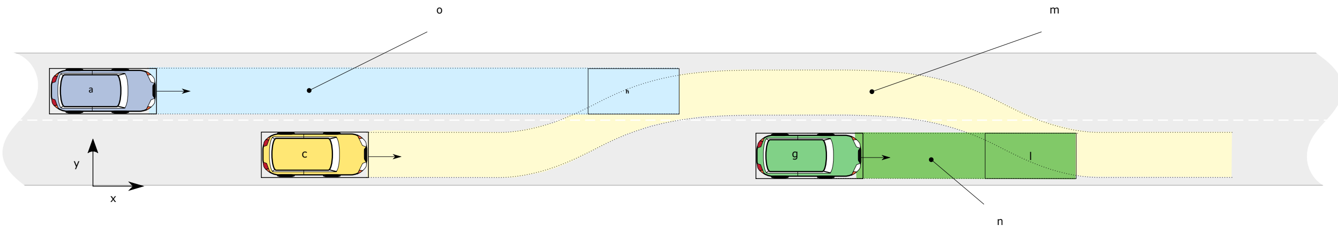

Fig. 3. Highway overtake scenario considered for the evaluation of the approach.

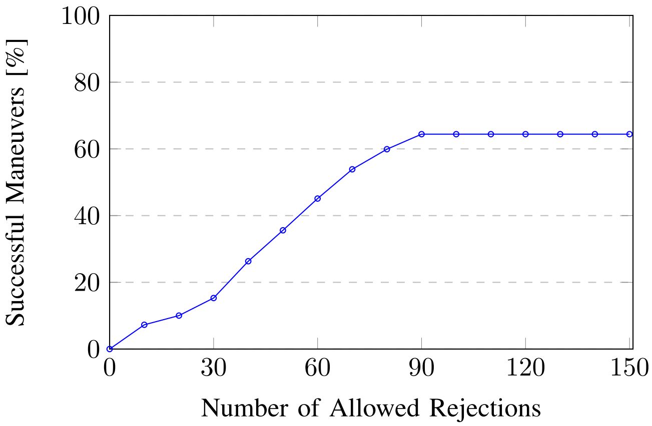

Fig. 4. Safe scenarios depending on the allowed number of adjustment rejections in row.

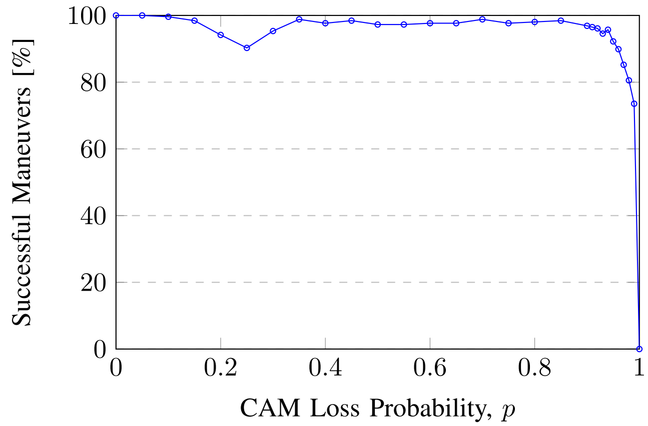

Fig. 5. Maneuver success rate depending on the CAM loss probability.

of the x positions were selected with respect to the German rule of thumb for safety distance called half speedometer which says that each vehicle needs to keep a distance to a front vehicle that is at least as big as the half of the velocity showed by the speedometer. All in all, in each scenario the initial distances between the vehicles are different, as well as the initial velocities.

A. Maneuver Parameter Adjustments

As already mentioned, the HV can propose velocity adjustments to a RV once the HV forecasts that the collision risk exceeds the threshold $\mathcal{R}_{\mathrm{tr}}$. However, since the HV is aware of the fact that the risk assessment relies on the assumption of maximal acceleration or deceleration, and the optimal velocity might require a too high jerk, the HV allows the RVs to reject an immediate velocity adjustment. Instead, the RV adjusts its velocity with its current capability. The number of consecutive rejections should be limited though, as in some cases the adjustment might be too slow. In order to estimate the threshold for the number of rejections, all 400 scenarios were run with different rejection thresholds within the range of 0 to 150 rejections. Fig. 4 shows the obtained results. One can see that the maximal number of successful overtake maneuvers is at about 64% which can be achieved when the allowed number of consecutive rejections is at least 90. Consequently, for further evaluations the threshold of 90 consecutive rejections is selected. A thresholds lower than 90, would decrease the number of safe maneuvers and so increase the number of risk reducing countermeasures such as minimal risk maneuvers that decreases the HV's utility.

TABLE II. INITIAL PARAMETER VALUES FOR $\mathcal{V}_1$ AND $\mathcal{V}_2$

Parameter	$\mathcal{V}_1$	$\mathcal{V}_2$	$\mathcal{V}_{\mathrm{H}}$	Unit
x	0	$[50, 200]$	$[10, 100]$	$[\mathrm{m}]$
y	4.5	1.5	1.5	$[\mathrm{m}]$
v	$[80, 130]$	$[80, 120]$	$[80, 130]$	$[\mathrm{km\,h^{-1}}]$
a	0.0	0.0	0.0	$[\mathrm{m\,s^{-2}}]$
ρ	1.0	1.0	1.0	$[\mathrm{s}]$
φ	0	0	0	$[^\circ]$
$a^{\max}$	4.0	4.0	4.0	$[\mathrm{m\,s^{-1}}]$
$b^{\max}$	-4.0	-4.0	-4.0	$[\mathrm{m\,s^{-1}}]$
j	0.3	0.2	0.0	$[\mathrm{m\,s^{-3}}]$
l	4.0	4.0	4.0	$[\mathrm{m}]$
w	1.8	1.8	1.8	$[\mathrm{m}]$

B. Influence of CAM Loss on Maneuver Success

Within the scope of this evaluation the impact of the CAM loss probability p on the maneuver success is investigated. Each of the 400 scenarios was run with different CAM loss probabilities reaching from 0 to 1. In case the CAM loss probability is equal to zero, the CAM frequency is at the constant value of $10\,\mathrm{Hz}$. Otherwise, every $0.1\,\mathrm{s}$ the RV generates a CAM that the HV will receive with a probability of $1 - p$. This might cause an overall decreased CAM frequency and as such an impaired prediction horizon with more imprecise parameter estimations. The consequence of an imprecise parameter estimation is the increased likelihood that the maneuver monitor will abort the maneuver execution, even though the maneuver could be executed safely. Such false positive alarms decrease the utility of the HV, as it has to fall back and execute a minimal risk maneuver or make a driver request.

For each tested CAM loss probability the number of successful overtake maneuvers was logged and divided by the total number of the scenarios resulting in a percentage of successful maneuvers. For the evaluation only the initially safe scenarios were considered, i.e., 257 out of 400 scenarios. The obtained results for the particular CAM loss probabilities are depicted in Fig. 5. As expected, the amount of safe scenarios for low CAM loss probabilities is high. The percentage constantly drops when the CAM loss probability is higher than 85 until reaching 0 for the case when all CAMs are lost.

These results indicate a robustness of the approach against a high number of random CAM drops for overtake scenarios. Even for very high CAM loss probabilities such as 98%, about 81% were still classified as safe. The reason for that high number of safe scenarios for such high CAM loss probabilities is the fact that the CAMs are dropped randomly and not consecutive, which simulates the effects of fast-fading channels in burst transmissions; these effects are normally present in vehicular wireless networks.

VI. Discussion

In this section, we briefly discuss how this approach can be extended in order to be applicable to other scenarios such as urban traffic.

The previous section illustrated that the proposed approach is applicable to highway scenarios and the communication based prediction is sufficient for these scenarios. However, in urban traffic this might be not the case. Consequently, the proposed approach needs several extensions. First, the remaining RSS rules must be integrated such that safety distances for situations where the vehicles are driving in opposite directions can be relatively restricted and requires extension such that simulation of consecutive CAM losses is possible, e.g., by integrating channel models. Further, the predictions based on other sensor data require new risk assessment functions that can quantify the sensor-specific uncertainty. Moreover, interactions between the traffic participants should be considered to further decrease the conservatism of the predictions.

VII. Conclusion and Future Work

This paper demonstrated an approach for dynamic risk management applied to overtaking maneuvers of autonomous vehicles. The evaluation showed that the traffic predictions are resilient to high CAM loss probabilities as well as noise in data. This work is an initial step towards reliable traffic prediction based on V2V communication, enabling safety guarantees regarding vehicles that are beyond a individual vehicle's field of view. The efficacy of the dynamic risk management was validated via simulation, which was also used to determine the level of uncertainty in the communication medium that could be tolerated before an unacceptable level of risk was encountered.

For the future work it is planned to improve the motion planning algorithm, such that it can recalculate the trajectories once the estimated collision risk is too high. In addition, to improve the reliability of the AV, the prediction algorithm will be improved, such that the predictions are less conservative. Further, a more realistic communication model will be integrated. Finally, scalability issues should be investigated, meaning that the approach will be tested for scenarios involving a higher number of vehicles.

VIII. Acknowledgement

The research leading to theses results has received founding from the European Union's Horizon 2020 research and innovation program under teh Marie Skłodowska-Curie grant agreement No 812.788 (MSCA-ETN SAS). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: http://etn-sas.eu/.

References

[1] S. Singh, "Critical reasons for crashes investigated in the national motor vehicle crash causation survey," *Traffic Safety Facts - Crash Stats*, 2015.

[2] International Organization for Standardization, "Road vehicles– functional safety," 2019.

[3] K. Czarnecki and R. Salay, "Towards a framework to manage perceptual uncertainty for safe automated driving," *Computing Research Repository*, 2019.

[4] I. Kurzidem, A. Saad, and P. Schleiß, "A systematic approach to analyzing perception architectures in autonomous vehicles," in *International Symposium on Model-Based Safety and Assessment*. Springer, 2020.

[5] M. Bahram, A. Lawitzky, J. Friedrichs, M. Aeberhard, and D. Wollherr, "A game-theoretic approach to replanning-aware interactive scene prediction and planning," *IEEE Transactions on Vehicular Technology*, 2016.

[6] Y. Luo, G. Yang, M. Xu, Z. Qin, and K. Li, "Cooperative lane-change maneuver for multiple automated vehicles on a highway," *Automotive Innovation*, 2019.

[7] L. Hobert, A. Festag, I. Llatser, L. Altomare, F. Visintainer, and A. Kovacs, "Enhancements of V2X communication in support of cooperative autonomous driving," *IEEE Communications Magazine*, 2015.

[8] M. Trapp, D. Schneider, and G. Weiss, "Towards safety-awareness and dynamic safety management," in *2018 14th European Dependable Computing Conference*, 2018.

[9] S. Shalev-Shwartz, S. Shammah, and A. Shashua, "On a formal model of safe and scalable self-driving cars," *Computing Research Repository*, 2017.

[10] P. Koopman, B. Osyk, and J. Weast, "Autonomous vehicles meet the physical world: RSS, variability, uncertainty, and proving safety (expanded version)," *arXiv:1911.01207 [cs]*, 2019.

[11] P. F. Orzechowski, K. Li, and M. Lauer, "Towards responsibility-sensitive safety of automated vehicles with reachable set analysis," in *2019 International Conference on Connected Vehicles and Expo*, 2019.

[12] B. Häfner, J. Jiru, K. Roscher, J. Ott, G. A. Schmitt, and Y. Sevilmis, "CVIP: A protocol for complex interactions among connected vehicles," in *2020 IEEE Intelligent Vehicles Symposium (IV)*, 2020.

[13] M. Werling, J. Ziegler, S. Kammel, and S. Thrun, "Optimal trajectory generation for dynamic street scenarios in a Frenet frame," in *IEEE International Conference on Robotics and Automation*, 2010.

[14] I. Bae, J. Moon, J. Jhung, H. Suk, T. Kim, H. Park, J. Cha, J. Kim, D. Kim, and S. Kim, "Self-driving like a human driver instead of a robocar: Personalized comfortable driving experience for autonomous vehicles," *arXiv preprint arXiv:2001.03908*, 2020.