A legal safety concept for highly automated driving on highways

Benoit Vanholme, Dominique Gruyer, Sebastien Glaser, Said Mammar

A Legal Safety Concept for Highly Automated Driving on Highways

Benoit Vanholme, Dominique Gruyer, *Member, IEEE*,
Sébastien Glaser, *Member, IEEE* and Saïd Mammar, *Member, IEEE*

***Abstract*— This paper discusses the design of an Advanced Driver Assistance System (ADAS) that ensures safety when traffic rules are respected by all road users. This concept, referred to as *legal safety*, is proposed as a basis that permits human and automated drivers to share the road infrastructure. It is illustrated for a Highly Automated driving System with speed keeping, distance keeping and lane changing functionalities on highways (HAS). The requirements legal safety places upon HAS components are presented, with a special focus on the co-pilot which calculates a safe trajectory for the vehicle based on perception of lanes and traffic signs and prediction of the trajectories of objects in the environment. A *lane coordinate system* is proposed as a powerful reference for the trajectory calculations of the co-pilot. The system controls the vehicle and communicates with the driver, according to an automation mode scheme inspired by the horse-rider metaphor (H-metaphor).**

I. Introduction

The physical transport of people and goods has always been an essential part of society. Since the creation of the Internet, digital alternatives exist (e.g. teleworking and teleshopping) [1] but road transport is still increasing in volume, raising several challenges. Road traffic accidents in the European Union claim around 40000 lives and leave almost 2 million people injured annually. They correspond to an estimated annual cost of around 200 billion euros, or 2 % of the EU's Gross Domestic Product (GDP) [2]. Accident analysis shows that human-inherent errors by distraction, drowsiness, emotion or miscalculation are almost always amongst the causes of these accidents [3]. Costs related to road traffic congestion and environmental pollution not only account for 2 % of the EU's GDP but also have an impact on the health of its citizens.

Automated driving systems could be one of the solutions for a safer, more comfortable and cleaner transport in the future [4]. One approach is to directly shift to automated driving, as demonstrated by the ARGO experience [5], the DARPA Challenge [6] and CyberCars [7]. With expensive, high-tech equipment, automated driving on a separated infrastructure with limited interaction with other vehicles is possible. But for economical, legal and psychological reasons, the approach chosen by most policy makers and car manufacturers is the incremental introduction of simple Advanced Driver Assistance Systems (ADAS). They rely on a limited number of economical, safe and modular hardware components that allow driving on the public road in cooperation with the human driver. Low-level vehicle control assistance with Anti-lock Braking Systems (ABS) and Electronic Stability Control (ESC) are now standard on most vehicles. Customer interest in ADAS has increased significantly due to higher-level systems that combine safety with comfort such as Adaptive Cruise Control (ACC), Intelligent Speed Adaptation (ISA), Lane Keeping Systems (LKS) and Lane Change Assistance (LCA) [8], [9], [10].

As ADAS trend toward higher levels of automation, the question arises of how an automated driving system should interact with other drivers in the environment. Could traffic rules manage the safety and efficiency of mixed human and automated traffic in the same way as they do for traffic with human drivers? It is the thesis of this paper, referred to as *legal safety*. The next question is how the system can interact with the human co-driver optimally. The European 7th Framework Program (FP7) project HAVEit (Highly Automated Vehicles for Intelligent Transport) [11], [12] proposes a cooperation along different *automation modes*. This is the context in which this paper develops the Highly Automated driving System for highways (HAS).

This paper is organized as follows. Section II presents the *legal safety* concept and its application to HAS. Section III discusses the architecture of HAS and the requirements legal safety places upon its perception, co-pilot and control components. Sections IV and V explain how the co-pilot predicts the trajectories of objects and calculates safe trajectories for the vehicle of interest (ego vehicle). The management of the automation mode during normal driving and during system failure is presented in Section VI. Section VII presents results of the system on the use cases defined by HAVEit. Section VIII concludes and provides a perspective on future work.

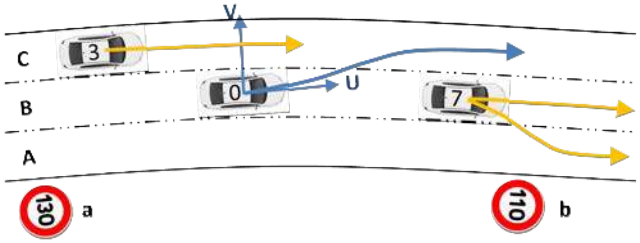

Fig. 1. Highway environment with ego vehicle (0), lanes (A, B, C), traffic signs (a, b) and object vehicles (3, 7)

This work was funded by the HAVEit project of the European Commission and the ABV project of the French National Research Agency (ANR)

B. Vanholme, D. Gruyer and S. Glaser are with Laboratoire sur les Interactions Véhicule-Infrastructure-Conducteur (LIVIC, IFSTTAR), Versailles, France benoit.vanholme@ifsttar.fr, dominique.gruyer@ifsttar.fr, sebastien.glaser@ifsttar.fr

S. Mammar is with Université d'Evry-Val-d'Essonne (UEVE), Evry, France said.mammar@iup.univ-evry.fr

II. Legal Safety in an Application Zone

A. Legal Safety

The word *traffic* comes from the Arabic *taraffaqa* meaning slowly walking along together, today certainly not the most common type of road traffic. Today's traffic is complex because of the diversity of its participants (e.g. the personality of the driver, the type of vehicle) and of its infrastructure (e.g. multiple lanes, junctions, intersections, traffic signs). Traffic rules have been developed to promote safety and efficiency.

If future vehicles are to begin driving autonomously, they will likely need to share the infrastructure with human-driven vehicles; a distant future where all vehicles would drive autonomously would be preceded by a transient period where automated and non-automated vehicles coexist. One alternative to sharing the infrastructure, to assign a part of the existing infrastructure (e.g. one lane) exclusively to automated driving, could be difficult to implement as argued in [13]. The other alternative, to create a separate infrastructure for automated driving, would come at a large cost and reduce its application zone (e.g. in rugged environments and cities).

This paper discusses the design of a highly automated system that ensures safety when traffic rules are respected by all road users. In the opposite case, when traffic rules are offended by a road user, the system avoids an accident if it can and does an emergency brake if it cannot. This concept, legal safety, is proposed as a natural way to let human and automated drivers share the infrastructure. The ethical question concerning the acceptability of a lethal accident between a legally safe driving system and a human driver that goes against the traffic rules is left open.

B. The Vienna Convention in the Application Zone

Basic traffic rules are defined by an international treaty under the authority of the United Nations, the 1968 Vienna Convention on Road Traffic [14]. It has not been signed by all countries, and local variations in practice can be found among signatories. Many of the local specificities do not directly apply on automated driving (e.g. driving under intoxication, day lighting, the seat belt use, tyre equipment), but some of them do. However, these local rules are not discussed in the paper. Rather, we focus on the application of the Vienna Convention on HAS which integrates speed keeping, distance keeping, lane keeping and lane changing functionalities on highways, excluding entry and exit points, during day and night, as in Fig. 1. This might be the first environment where automated driving will be possible as its simple lane structure and unidirectional flow of large objects facilitate perception, co-pilot and control algorithms. The description assumes that driving is on the right side of the road; translation for left-side driving is straightforward. The environment, the functionalities and additional conditions (e.g. lane changing, speed range, day/ night driving) in which the system ensures safety are referred to as the *application zone*.

The application of the articles of the Vienna Convention that apply to the application zone of HAS is given below. The original index of the article in the text of the convention is indicated between parentheses.

Article 1 (7): Road users should avoid damage to road infrastructure or to other road users.

Article 2 (8): The vehicle should always be controlled by a driver in a fit physical and mental condition.

Article 3 (10): Driving should be on the right-most lane if possible, except for overtaking.

Article 4 (11, 14): Overtaking is only on the left, except in congested traffic where right overtaking is also allowed. An overtaking maneuver can only be started if the vehicles in front and in back of the ego vehicle in the same lane have neither indicated nor started to overtake another vehicle, if vehicles in the target lane are not hindered by the maneuver and if continuous lane markings are not crossed. The corresponding indicator of the vehicle must stay on during the entire maneuver.

Article 5 (13): The speed of the vehicle must be adapted to road and weather conditions (e.g. visibility and road friction), speed limit signs and other vehicles. The distance between vehicles must be such that a collision can be avoided in the case of emergency braking. The driver also must be capable of avoiding collisions with any foreseeable obstacles out of the perception horizon.

Article 6 (17): Braking should only be done for safety reasons and must be indicated with braking lights.

Article 7 (25): Only motor vehicles are allowed on highways. Vehicles on the highway have priority over vehicles entering. If the vehicle is to be stopped for a technical reason, this must be done on the emergency lane, if possible.

Article 8 (32): The lighting of the vehicle should be adapted to the visibility conditions.

Article 9 (34): Priority vehicles are exempt from traffic rules, except from Art. 1 (7).

Sections III to VI discuss how HAS has been designed to cover the traffic rules described above.

III. System Architecture

The functional architecture of HAS is shown in Fig. 2. Similar to most ADAS, it imitates human driving functions with perception, decision and action components. The perception module, which processes data from sensors such as cameras, laser scanners and radar, imitates the function of human vision (tracking lanes, traffic signs and objects). The co-pilot module is the decision-making part of the system; it calculates a trajectory that is legally safe with respect to the environment detected by the perception module. The control module commands the actions of the powertrain, brakes and front wheels to maintain vehicle trajectory, or communicates back to the driver using the pedals and steering wheel. The dashed arrows indicate the connection of the automation modules to the Human Machine Interface (HMI) that manages interaction with the human driver.

All information exchanged between perception, co-pilot and control modules is described in a coordinate axis UV attached to the ego vehicle, with origin in the geometric

center of the vehicle, U in the longitudinal direction and V in the lateral direction as shown in Fig. 1.

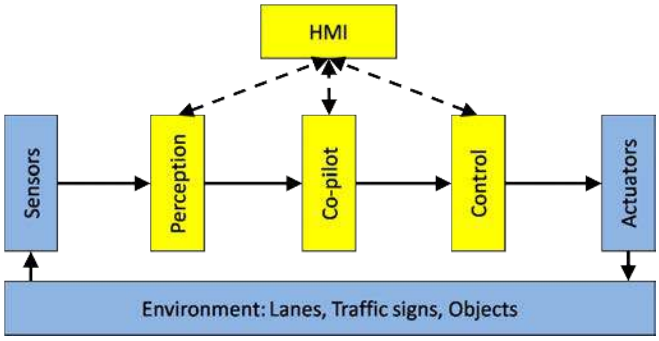

Fig. 2. System architecture

This section focuses on the requirements of legal safety on perception and control components. Sections IV and V will discuss the design of the co-pilot component.

A. Legal Safety of Perception

Perception of the lane of the ego vehicle and the lanes to its immediate right and left is essential as indicated by the articles presented in the previous section, Art. 1, 3, 4 and 7. In this paper they will be referred to as the *ego lane*, *right lane* and *left lane*, labeled A, B and C respectively. The lanes change when the origin of UV crosses the lane marking. The lane description must be available ahead of and behind the ego vehicle, during both night and day. Extensive research has been done on lane detection and tracking using Differential GPS (DGPS) [15], laser scanners [16], radar [17] and vision [18]. Vision seems most appropriate for distinguishing continuous from discontinuous lane markings for Art. 4 and normal lanes from emergency lanes for Art. 7. Robust vision-based perception of a single lane is already available in the market as Lane Departure Warning (LDW) and Lane-Keeping Systems (LKS). Ongoing research is working to enhance perception performance and extend it to multiple lanes [19]. The description of highway exit and entry lanes is not required by Art. 7. Art. 5 implies an estimation of road friction without affecting vehicle control, such as in [20].

Art. 5 also requires the perception of traffic signs (speed limits and lane closures). An approach based on Infrastructure-to-Vehicle (I2V) communication is proposed in [21], [22]. Legal safety would require the implementation of a robust I2V for all traffic signs in the application zone. A more general approach could be offered by traffic sign recognition by vision, which is commercially available as a part of ISA systems.

The last essential function of the sensor and perception components of HAS is the detection and tracking of objects in the ego, right and left lanes (if existing), both ahead of and behind the ego vehicle, Art. 1, 4, 5, 6, 7, 9. At night it should at least detect the objects which have an appropriate lighting, Art. 8. Object perception is possible using laser scanners, radar [23], vision [24] or a fusion of sensors [25]. Additionally, Vehicle-to-vehicle (V2V) communication could provide more information. For information that is critical to the driving task, however, V2V could only be relied upon if integrated in all vehicles in the environment, which might be difficult as discussed in Section II. Though object positions and movements are today most accurately estimated by laser scanners and radar, vision will probably always be a part of the system as indicator detection [26] is required by Art. 4, at least for objects in the ego lane.

B. Legal Safety of Control

Art. 4 and 5 imply a lateral control component, which corresponds with lane-keeping and lane-changing and a longitudinal control component, which in its extreme case corresponds to emergency braking. Ego vehicle control is probably the area on which research is most advanced. Longitudinal control [27] is available today on many vehicles as a part of the ACC system. Some of the lateral control algorithms of LKS [28] could be used to track a trajectory as in Fig. 1.

C. System Safety

Apart from the traffic rules for assuring legal safety with respect to the vehicle's environment, additional internal rules are imposed upon each component to ensure the integrity of the other components of the system, as listed below.

Specification 1: Within a given range, the lane descriptions are of predefined precision.

Specification 2: Within a given range, object descriptions are of predefined precision, which is such that a correct lane assignment can be made.

Specification 3: The ranges in Spec. 1 and 2 change at a predefined rate.

Specification 4: The objects in the environment are reduced or clustered to a maximum of eight as shown in Fig. 3: six of which are the nearest objects ahead of and behind the vehicle in each of the three lanes, and two of which are the objects on either side of the vehicle.

Specification 5: The position, orientation, velocity and acceleration of the ego vehicle proposed by the trajectories of the co-pilot are within a predefined range.

Specification 6: The control component maintains vehicle trajectory and speed profiles with a predefined error.

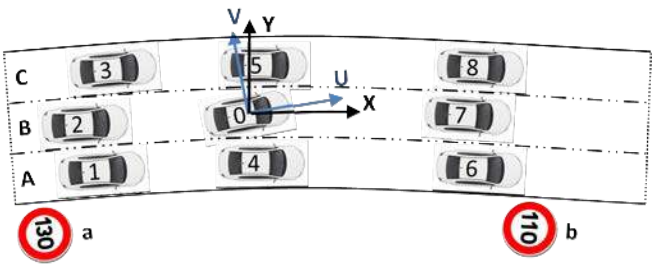

Fig. 3. Highway environment with ego vehicle (0), lanes (A, B, C), traffic signs (a, b) and object vehicles (1-8)

IV. Prediction of the Object and Phantom Trajectories

A. State of the Art

An important part of the co-pilot is the prediction of the trajectories of objects in the ego vehicle's environment. A common approach in collision avoidance systems is to assume that the object will continue its current movement. A Kalman filter or one of its derivatives in combination with a motion model such as Constant Turning Rate and Acceleration (CTRA) are used in [29]. In previous work, the authors proposed to considering the relationship between an object and the infrastructure (e.g. its Time to Lane Crossing, TLC) [30]. By not taking legal driving into account, these approaches might underestimate (e.g. when an object is going straight with its indicators on) or overestimate (e.g. when an object moves to the middle of its lane) the danger an object represents. Section IV describes the prediction of object trajectories according to the legal safety concept.

B. Lane Coordinate System

For the co-pilot, a natural environment for calculating with trajectories (in this and next section) is a curvilinear *lane coordinate system* XY, with the same origin of the ego vehicle system UV, the X-axis parallel with the lane and the Y-axis perpendicular on X, as indicated in Fig. 3. The first step of the co-pilot algorithm consists of transforming the perceived environment from UV to XY as shown in Fig. 4. This translates the parallel lanes of a highway environment into Y-coordinate lines, allowing a simple description of ego and object trajectories as a combination of transient (polynomial) and permanent (linear) sections in XY. In a final step, presented in Section V, the co-pilot applies an inverse transformation to the ego trajectories from XY to UV for the control and HMI modules. In UV, the permanent section of the trajectories meet the geometry of the lanes, which is usually based on a clothoid model.

C. Trajectory Generation

Fig. 4 presents the possible trajectories for the 8 potential objects (1-8) around the ego vehicle (0), assuming that the objects are driving legally. They are labeled as IJK with I as the index of the object, J as the index of the target lane and K as the index of the variant of two trajectories in the same target lane (only for object 4 and 5). The first trajectory calculated for each object is the one without lane changes ($1A$, $3C$, $4A'$, $4A''$, $5C'$, $5C''$, $6A$, $7B$, $8C$), except for object 2 which is assumed to keep an appropriate distance from the ego vehicle, Art. 5. Because this $2B$ trajectory has no influence on the decisions of the co-pilot, it is eliminated. According to Art. 4, objects 2 and 7 are allowed to change lanes ($2A$, $2C$, $7A$, $7C$) when their indicators are activated. The same article stipulates that no object should hinder the ego vehicle when changing lanes, therefore no object trajectories towards lane B are calculated, regardless of the state of the objects' indicators. As explained in the next section, this guarantees that a legally safe trajectory in the ego lane can always be found, corresponding to keeping a safe distance from object 7 according to Art. 5.

The system is more defensive than strictly needed by legal safety by predicting a (non-legal) object trajectory towards lane B when it is crossing a lane mark of B without the activation of indicators, except for objects 1 and 3; as object 2, they are assumed to keep an appropriate distance from the ego vehicle. It is also defensive in the sense that it considers that objects can change lanes crossing continuous lane markings, despite of Art. 4 and that objects can keep driving on the left, despite of Art. 3.

Note that for an object (legally or not) changing lanes, two trajectories (the lane keeping and lane changing trajectory) are predicted as if it were expanding in the future. This reflects the uncertainty whether the lane change will actually take place or not. Moreover, as the dynamism of the lane change cannot be known, a worst-case maneuver (a very fast lane change) is assumed.

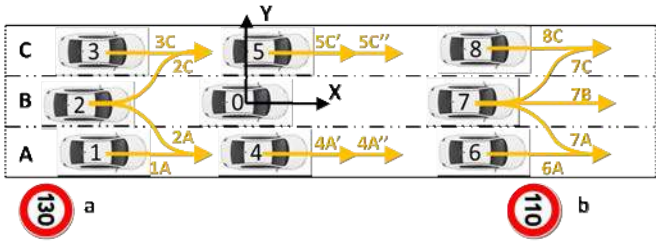

Fig. 4. Prediction of object trajectories

According to Art. 5 the ego vehicle must be capable of avoiding collisions with potential objects out of its perception horizon. For this purpose, the trajectories of worst-case *phantom* objects at the edge of the perception zone (Spec. 1, Spec. 2) are calculated, as displayed in Fig. 5. Assuming that driving in the opposite direction is prohibited, the worst-case phantoms ahead of the ego are standing still, indices IV, V and VI. This will let the ego vehicle control its speed so that it is able to stop for a traffic jam, as explained in the next section. In the rear of the vehicle, phantom III is a vehicle traveling at the speed limit, preventing the ego vehicle from changing lanes to the left when its speed and rear perception horizon are too low. Phantom I can be ignored as right overtaking is not allowed by Art. 4, except in congestion where it takes the same trajectory as III. Phantom II is discarded as the ego vehicle has priority over it by Art. 5.

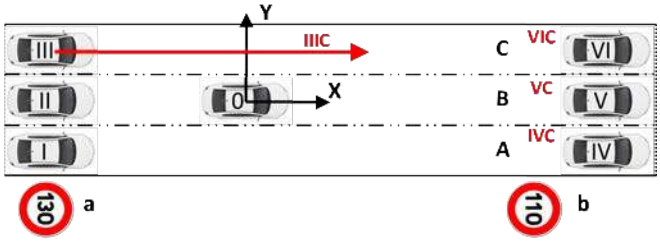

Fig. 5. Prediction of phantom trajectories

The worst-case legal speed profile for the objects (1-8) and phantoms (I-VI) is shown in Fig. 6, with time axis T and speed axis V. Phantoms ahead of and behind the ego vehicle have a constant speed corresponding to standstill and the speed limit, respectively. Objects behind the ego vehicle are assumed to continue accelerating if they were or to hold their speed if they were not ($1A$, $2A$, $2C$, $3C$). Analogously, objects in the front decelerate (but have a minimum speed of zero) or hold speeds ($6A$, $7A$, $7B$, $7C$, $8C$). Objects 4 and 5 are believed to expand in the future between minimum (') and maximum speed profiles (") according to the uncertainty on their acceleration, as in Spec. 2.

The system is more defensive than needed by legal safety by allowing objects to overtake on the right and exceed speed limits.

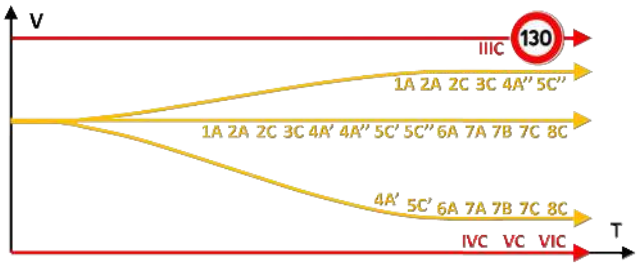

Fig. 6. Prediction of object and phantom speed profiles

D. Mathematical Description of Trajectories and Speed Profiles

The mathematical model of the object trajectories in XY is a combination of a polynomial part and a linear part, for both the X-position p_x as a function of time t (1) and the Y-position p_y as a function of p_x (2), referred to as model A in this paper.

$$\begin{cases} p_x(t) = a_4 t^4 + ... + a_1 t + a_0 & \text{if } t < T \\ p_x(t) = b_1 t + b_0 & \text{if } t >= T \end{cases} \quad (1)$$

$$\begin{cases} p_y(p_x) = c_5 p_x^5 + ... + c_1 p_x + c_0 & \text{if } p_x < X \\ p_y(p_x) = d_0 & \text{if } p_x >= X \end{cases} \quad (2)$$

The parameters a_i, b_i, c_i, d_i, T and X can be found from the initial and final conditions (3)-(6), with velocities v and accelerations a, as described in [30]. The superscript 0 indicates the initial state, 2 the final state at T or X and 02 the average between these two.

$$\begin{cases} p_x(0) = p_{x_0} & \dot{p}_x(0) = v_{x_0} & \ddot{p}_x(0) = 0 \\ & \dot{p}_x(T) = v_{x_2} & \ddot{p}_x(T) = 0 \end{cases} \quad (3)$$

$$T = (v_{x_2} - v_{x_0})/a_{x_{02}} \quad (4)$$

$$\begin{cases} p_y(0) = p_{y_0} & \dot{p}_y(0) = 0 & \ddot{p}_y(0) = 0 \\ p_y(X) = p_{y_2} & \dot{p}_y(X) = 0 & \ddot{p}_y(X) = 0 \end{cases} \quad (5)$$

$$X = (p_{y_2} - p_{y_0})/v_{y_{02}} \quad (6)$$

The initial values (superscript 0) are known and the values v_{x_2}, $a_{x_{02}}$, p_{y_2} and $v_{y_{02}}$ follow from the discussion on object trajectories in this section. Model A also serves for the calculation of ego trajectories, as described in next section.

V. Calculation of the Ego Trajectories

A. State of the Art

The co-pilot computes a safe ego trajectory for each of the three considered lanes (ego, right and left) based both on the description of lanes and traffic signs and on the prediction of object trajectories. In the vast literature of motion planning, most algorithms fall into one of two families. Combinatorial motion planning finds the absolute, best solution (according to a chosen performance metric) in the complete solution space, while sampling-based motion planning finds an acceptable solution by only evaluating a part of the solution space [31]. As for driving, a wide range of valid trajectories exists (think of drivers with different personalities) and calculation speed is crucial, therefore the algorithm presented is designed according to the latter family.

Heuristic analysis limits the algorithm to the generation and evaluation of a total of ten trajectories. Six of these are for normal functioning of the system; one trajectory per lane with two possible speed profiles, index 0 in Fig. 7 and Fig. 8. Four safe state/ emergency trajectories have a terminal velocity of zero and are to be used during a failure of the system, index F in Fig. 7 and 8. In following sections, each of these trajectories is discussed.

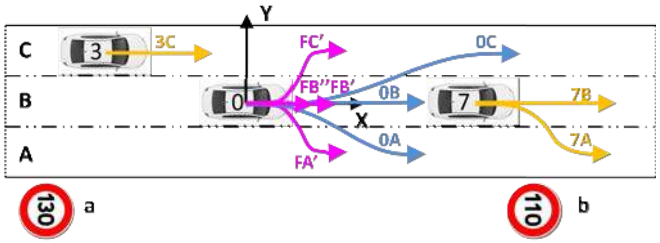

Fig. 7. Calculation of ego trajectories

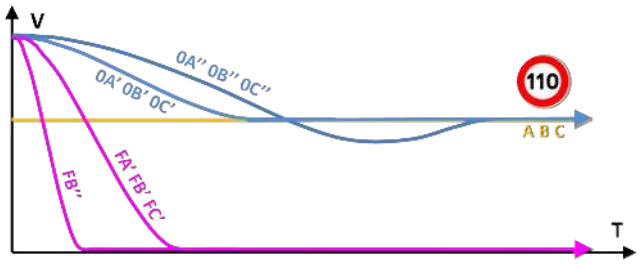

Fig. 8. Calculation of ego speed profiles

B. Heuristics for Sampling

The limitations legal safety places upon the trajectories and speed profiles of the ego vehicle are expressed in the equations of this section, which are applied to each target lane. The exponents R and F correspond to the objects to the rear and front of the ego vehicle respectively, and variables

without exponent correspond to the ego vehicle itself. When referring to an object, the one with a trajectory towards the corresponding target lane (according to Section IV) is meant. For objects 4 and 5, R corresponds to variant $''$ and F to $'$. The variables p is indicate position, v velocity and a acceleration. Similar to section IV, the subscript 0 refers to the initial state, 2 the final state and 02 the average value between them.

Art. 4 and 5 refer implicitly to a safety distance to be kept from the objects with the same target lane to the rear and front of the ego vehicle, leading to (7). The first equation is for the target position p_{x_2} which includes a safety distance p_{x_S}, which is proportional with the object speed with a factor t_{x_S} (i.e. a "X-second rule" for safe following distances). The second equation is for the target speed v_{x_2}, which is adapted to that of the objects to maintain the safety distance beyond the evaluation period. Avoiding right overtaking in Art. 4 also gives (7), now referring to the objects with target lanes left of the target lane of the ego vehicle.

$$\begin{cases} p^R_{x_2} + p^R_{x_S} \leq p_{x_2} \leq p^F_{x_2} - p^F_{x_S} \\ v^R_{x_2} \leq v_{x_2} \leq v^F_{x_2} \end{cases} \tag{7}$$

Art. 5 implies that the target speed v_{x_2} is such that a collision with phantom objects (introduced in Section IV) can be avoided if needed, giving (8). Here, the indices R and F refer to phantoms and a^E_x is the extreme deceleration or acceleration capacity of the vehicles (in absolute value), which depends on road conditions. The equation expresses that extreme braking of the rear phantom avoids the ego vehicle and that extreme braking of the ego vehicle avoids the front phantom.

$$v^R_{x_0} - \sqrt{\frac{2a^E_x}{-p^R_{x_0}}} \leq v_{x_2} \leq v^F_{x_0} + \sqrt{\frac{2a^E_x}{p^F_{x_0}}} \tag{8}$$

The first equation in (9) shows the adaptation of the target speed v_{x_2} to the speed limit v^S_x, Art. 5. When a new speed limit v^S_x lower than the ego vehicle speed v_{x_0} appears at a distance p^S_x, the first equation is not sufficient. The second equation indicates that v_{x_S}, the speed of the ego vehicle at p^S_x, must also adopt the speed limit v^S_x.

$$\begin{cases} v_{x_2} \leq v^S_x \\ v_{x_S} \leq v^S_x \end{cases} \tag{9}$$

The speed in curves is adapted to keep the lateral acceleration below a maximum value a^E_y (depending on road conditions, similar to a^E_x) in order to avoid loosing vehicle control, as in Art. 5. In (10), c^C_x is the maximum curvature (in absolute values) of the lane at a distance p^C_x and v_{x_C} the corresponding maximum speed of the ego vehicle. Exceeding longitudinal system limits is avoided by bounding the deceleration and acceleration to a^E_x.

$$\begin{cases} v_{x_2} \leq \sqrt{\frac{a^E_y}{c^C_x}} \\ v_{x_C} \leq \sqrt{\frac{a^E_y}{c^C_x}} \\ -a^E_x \leq a_{x_{02}} \leq a^E_x \end{cases} \tag{10}$$

To ensure the integrity of the perception and control modules (Spec. 5) the target speed and average acceleration are bounded by (11), where v^H_x and v^H_y are the maximum longitudinal and lateral speed set by specification or by the human driver and a^h_x and a^H_x are the extreme deceleration and acceleration.

$$\begin{cases} 0 \leq v_{x_2} \leq v^H_x \\ 0 \leq v_{y_2} \leq v^H_y \\ a^h_x \leq a_{x_{02}} \leq a^H_x \end{cases} \tag{11}$$

C. Trajectory Generation

Based on the equations above, the speed profiles are generated. They have a time horizon of $10\,s$, which is enough for a to decelerate from highway speed to zero if needed. Speed profile $0I'$ in Fig. 8 is built according to model A (a polynomial followed by a linear section), which is defined by the parameters v_{x_2} and $a_{x_{02}}$ as given in Section IV. For $0I'$, the parameter v_{x_2} is set to the maximum value allowed by (7)-(11). An upper bound on the parameter $a_{x_{02}}$ is directly indicated by the third equation of (10) and (11). An additional upper bound is implicitly set by the first equation of (7), which is written as a function of $a_{x_{02}}$ in the first equation of (12). A component related to the error on the safety distance ($p^F_{x_0} - p^F_{x_S}$), to the difference in speed between ego and object ($v^F_{x_2} - v_{x_0}$) and to the acceleration of the object ($v^F_{x_2} - v^F_{x_0}$) can be recognized. The second equations of (9) and (10) can be written as the second and third equation of (12) respectively. If the initial speed is legally safe, then using model A, the conditions on v_{x_2} and $a_{x_{02}}$ imply that all speeds between the initial and the final state are safe.

$$\begin{cases} a_{x_{02}} \leq \frac{\frac{1}{2}(v^F_{x_2} - v_{x_0})^2}{\frac{1}{2}\frac{(v^F_{x_2} - v^F_{x_0})^2}{a^F_{x_{02}}} - (p^F_{x_0} - p^F_{x_S})} \\ a_{x_{02}} \leq -\frac{(v_{x_0} + v^S_x)}{2}\frac{(v_{x_0} - v^S_x)}{p^S_x} \\ a_{x_{02}} \leq -\frac{(v_{x_0} + v^C_x)}{2}\frac{(v_{x_0} - v^C_x)}{p^C_x} \end{cases} \tag{12}$$

A model B for speed profiles is shown by $0I''$ in Fig. 8. It corresponds to a sequence which consists of a polynomial (from v_{x_0} to v_{x_1} over time T_{01}), a linear section (at v_{x_1} during T_{11}), a second polynomial (from v_{x_1} to v_{x_2} over a time T_{12}) and a second linear section (at v_{x_2}). Its mathematical description can be easily adapted from (1)-(6) and is defined by the parameters v_{x_1} and v_{x_2}. For parameter v_{x_2}, the upper bound is specified by (7)-(11), as for model A. The value for v_{x_1} is calculated so that the final position of the ego trajectory meets the first equation of (7). This results in (13).

$$v_{x_1} = v_{x_0} + k_p(p^F_{x_0} - p^F_S) + k_v(v^F_{x_2} - v_{x_0}) + k_a\frac{(v^F_{x_2} - v^F_{x_0})^2}{2a^F_{x_{02}}}$$

$$\begin{cases} k_p = -k_a = \frac{1}{T_{01}/2 + T_{11} + T_{12}/2} \\ k_v = \frac{T_{01} + T_{11} + T_{12}/2}{T_{01}/2 + T_{11} + T_{12}/2} \end{cases} \tag{13}$$

Similar as for model A, a component linked to the error in safety distance, to the speed difference and to the object acceleration appears. Once the parameters k_p, k_v and k_a are

tuned for an optimal object distance control, T_{01}, T_{11} and T_{12} are defined.

Speed profile $0I'$ integrates all conditions in (7)-(11), unlike model $0I''$ which does not take into account the second equation of (9) and (10). While model $0I'$ is well-suited for adapting a certain speed and approaching a slower object, distance keeping to an object is only possible with $0I''$. A correct solution is always given by one of both speed profiles (the one corresponding with the lowest value of v_{x_2}).

Note that the conditions that depend on objects and phantoms R (behind the ego vehicle) in equations (7) and (8) are not integrated in the generation of the speed profiles $0I'$ and OI''. If the trajectory evaluation step (discussed in next section) shows a collision with these objects or phantoms, the trajectory is excluded. As Section IV shows, no object R has a legal trajectory that ends in the ego lane; therefore, at least for the ego lane a legally safe trajectory is guaranteed.

The safe state speed profile FI' and emergency speed profile FB'' in Fig. 8 use model A with a target speed v_{x_2} of zero and a moderate or extreme acceleration $a_{x_{02}}$. They protect against unexpected object behavior or system failure, as will be described in Section VI.

Fig. 7 shows the trajectories OI, FI' and FB'' which are calculated with the speed profiles $0I'$, $0I''$, FI' and FB'' according to the lateral component of model A described in Section IV. The parameter p_{y_2} depends on the target lane and $v_{y_{02}}$ is found in (14). This equation specifies that the ego vehicle should be on the linear section of the trajectory (in the middle of the lane target) when it is in the same position p_{x_G} as the object F.

$$\frac{p_{y_2}-p_{y_0}}{p_{x_G}} \leq v_{y_{02}} \quad \text{with } p_{x_G} = p_x^F \tag{14}$$

D. Evaluation of Trajectories

After trajectory generation, the aspects of legal safety that were not already explicitly integrated in (7)-(14), are evaluated. Driving in the right-most lane, Art. 3, is encouraged by a positive performance indicator (a negative performance cost) for the right target lane. Medium performance costs are attached to trajectories that correspond to crossing a continuous lane marking (Art. 4) or that correspond with an emergency lane (Art. 7).

The integrity of each trajectory is verified by a collision analysis between the ego and object vehicles for each of the states between the initial and final state. If a collision is detected, a high performance cost is attributed, which is proportional to the speed difference between the two vehicles at the time of collision.

In legal driving scenarios, there is always a safe trajectory $0B$ in the ego lane which corresponds to a zero performance cost, as discussed in Section V-C. When an illegal object behavior leads to a positive performance cost for $0B$ (indicating a collision), the emergency trajectory FB'' is chosen. The trajectory towards the right lane $0A$ is proposed by the co-pilot if it has a target speed which is not lower than that of the trajectory in the ego lane and no collision cost. The trajectory to the left lane $0C$ is suggested if it allows an increase in target speed without performance cost.

In a last step, the co-pilot converts the ego trajectories from the lane coordinate system XY (Fig. 7) to the ego vehicle coordinate system UV (Fig. 1).

VI. Management of Automation Mode

The design of the interface between the human driver and the driving system is crucial for legal safety. Art. 2 stipulates that a physically and mentally fit driver should always be present. In HAS, the *driver* can be the automated driving system (in the application zone), the human driver or the combination of both. This last option is extensively studied in the HAVEit project [12] as well as in [32], [33] which describe the interaction between the human driver and driving system along the horse-rider metaphor (H-metaphor). An essential aspect in the interaction between rider and horse is the distinction between *loose-rein* and *tight-rein* control. Under tight reins, the rider controls the horse directly. The horse can, however, resist the commands of the rider and balk when it judges a maneuver too dangerous. In loose-rein riding the horse has more autonomy, but the rider still gives some high-level instructions and corrects when necessary.

In HAS, this type of two-way communication is implemented along four automation modes. In the *human mode*, the human driver maintains contact with the steering wheel and pedals, giving direct control over the vehicle. When there is contact with the pedals, the *speed mode* is activated, engaging an automated speed control (including ACC and ISA functionalities) with a maximum speed set by the human driver. High-level driving is offered in the *cruise mode* where the driver loosens his grip on the steering wheel and HAS performs speed control, distance control, lane keeping and, if acknowledged via an indicator, lane changes. When the *auto mode* is activated, lane changes are done without this acknowledgement.

As between the rider and horse, this automation mode can be changed by the human driver or the driving system. The human driver must take over the control of the vehicle if the application zone is left during normal functioning (e.g. for taking an exit) or because of system failure (e.g. due to a hardware problem). If the human driver does not respond as requested by HAS, the system brings the vehicle to standstill along the safe state or emergency trajectories presented in Section V, as stipulated by Art. 6 and 7. Similarly, HAS takes over control when a maneuver performed by the human driver is considered dangerous, e.g. it applies hard braking if that is the only way to prevent a collision, it provides feedback to the steering wheel when a lane change is unsafe and stiffens the gas pedal when a speed limit is reached.

VII. Results

Fig. 9 shows a simulation result of HAS in *cruise mode* along the use cases defined in the HAVEit project, with v_x the speed of the ego vehicle, p_y its lateral position with respect to the right-most lane and p_x the position of an object vehicle. The use case *driving in a lane with obstacles* is shown from 1 to 2. The system converges to a constant safety distance to the object. It proposes a lane change which

is acknowledged at 2 and finished at 3, corresponding to the *driving with lane change* use case. From 3 to 4, *driving with speed limit change* is shown, causing the object to become closer to the ego vehicle again. The speed limit is increased and at 5 a lane change to the original lane is made, while accelerating to the maximum speed allowed by the driver 6. The system reduces its speed at 7 in preparation for the curve from 8 to 9. From 6 to 9 it controls the vehicle in the middle of the lane, *normal driving in a lane without obstacles*.

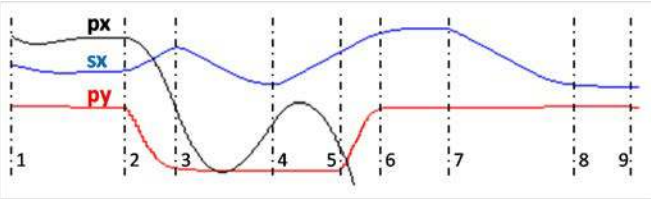

Fig. 9. Calculation of ego speed profiles

VIII. Conclusion and Perspectives

This paper proposes legal safety as a natural way to let human drivers and automated driving systems interact. The concept was developed for the HAS system for speed keeping, distance keeping, lane keeping and lane changing on highways. The requirements legal safety places upon its components were described, with a focus on the co-pilot and HMI during normal system functioning and system failure.

Future work will be on migration from the simulator towards the demonstration vehicles of the HAVEit project. In parallel, the application zone of HAS will be enlarged to highway entries and exits.

IX. Acknowledgements

The authors would like to thank the HAVEit project of the 7th Framework Program (FP7) of the European Commission and the ABV project of the French National Research Agency (ANR) for funding this work and the anonymous reviewers for their constructive comments.

References

[1] J. M. Eger, *The Internet vs. The Automobile*. Government Technology, 2007.
[2] European Road Safety Observatory. (2008) Annual statistical report.
[3] V. Neale, T. Dingus, S. Klauer, J. Sudweeks, and M. Goodman, "An overview of the 100-car naturalistic study and findings," in *19th International Technical Conference on Enhanced Safety of Vehicles*. Citeseer, 2005.
[4] B. Vanholme. (2010) Personal mobility in 2050: bicycles or autonomous vehicles? The Young European Arena of Research (YEAR), TRA Conference. [Online]. Available: http://year2010.fehrl.org/?m=24&mode=view&id=190
[5] A. Broggi, M. Bertozzi, A. Fascioli, and G. Conte, *Automatic vehicle guidance: the experience of the ARGO autonomous vehicle*. World Scientific Pub Co Inc, 1999.
[6] Defense Advanced Research Projects Agency (DARPA). (2007) The DARPA Grand Challenge. [Online]. Available: http://www.darpa.mil/grandchallenge
[7] M. Parent, "Advanced urban transport: automation is on the way," *IEEE Intell. Syst.*, vol. 22, no. 2, pp. 9 –11, Mar. 2007.
[8] S. Moon, I. Moon, and K. Yi, "Design, tuning, and evaluation of a full-range adaptive cruise control system with collision avoidance," *Control Engineering Practice*, vol. 17, no. 4, pp. 442–455, 2009.
[9] O. Carsten and F. Tate, "Intelligent speed adaptation: accident savings and cost-benefit analysis," *Accident Analysis & Prevention*, vol. 37, no. 3, pp. 407–416, 2005.
[10] S.-J. Wu, H.-H. Chiang, J.-W. Perng, C.-J. Chen, B.-F. Wu, and T.-T. Lee, "The heterogeneous systems integration design and implementation for lane keeping on a vehicle," *IEEE Trans. Intell. Transp. Syst.*, vol. 9, no. 2, pp. 246 –263, Jun. 2008.
[11] R. Hoeger, A. Amditis, M. Kunert, A. Hoess, F. Flemisch, H. Krueger, A. Bartels, A. Beutner, and K. Pagle, "Highly automated vehicles for intelligent transport: HAVEit approach," in *ITS World Congress*, 2008.
[12] HAVEit Consortium. (2011) Highly Automated VEhicles for Intelligent Transport, European Union 7th Framework Program. [Online]. Available: http://www.haveit-eu.org
[13] S. Shladover, "Truck automation operational concept alternatives," in *Intelligent Vehicles Symposium (IV), IEEE*, Jun. 2010, pp. 1072 –1077.
[14] United Nations. (1968) Convention on road traffic (Vienna). [Online]. Available: http://www.unece.org/trans/conventn/crt1968e.pdf
[15] H. Weigel, H. Cramer, G. Wanielik, A. Polychronopoulos, and A. Saroldi, "Accurate road geometry estimation for a safe speed application," in *Intelligent Vehicles Symposium (IV), IEEE*, 2006, pp. 516 –521.
[16] A. Kirchner and C. Ameling, "Integrated obstacle and road tracking using a laser scanner," in *Intelligent Vehicles Symposium (IV), IEEE*, 2000, pp. 675 –681.
[17] A. Polychronopoulos, A. Amditis, N. Floudas, and H. Lind, "Integrated object and road border tracking using 77 GHz automotive radars," *Radar, Sonar and Navigation, IEE*, vol. 151, no. 6, pp. 375 – 381, Dec. 2004.
[18] J. Siegemund, D. Pfeiffer, U. Franke, and W. Fondrstner, "Curb reconstruction using conditional random fields," in *Intelligent Vehicles Symposium (IV), IEEE*, Jun. 2010, pp. 203 –210.
[19] S.-S. Ieng, J. Vrignon, D. Gruyer, and D. Aubert, "A new multi-lanes detection using multi-camera for robust vehicle location," in *Intelligent Vehicles Symposium (IV), IEEE*, Jun. 2005, pp. 700 – 705.
[20] B. Chen and H. Cheng, "A review of the applications of agent technology in traffic and transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 11, no. 2, pp. 485 –497, Jun. 2010.
[21] SAFESPOT Consortium. (2010) Cooperative vehicles and road infrastructure for road safety, European Union 6th Framework Program. [Online]. Available: http://www.safespot-eu.org
[22] B. Vanholme, D. Gruyer, S. Glaser, and S. Mammar, "Fast prototyping of a highly autonomous cooperative driving system for public roads," in *Intelligent Vehicles Symposium (IV), IEEE*, Jun. 2010, pp. 135 –142.
[23] U. Scheunert, P. Lindner, E. Richter, T. Tatschke, D. Schestauber, E. Fuchs, and G. Wanielik, "Early and multi level fusion for reliable automotive safety systems," in *Intelligent Vehicles Symposium (IV), IEEE*, Jun. 2007, pp. 196 –201.
[24] D. Pfeiffer and U. Franke, "Efficient representation of traffic scenes by means of dynamic stixels," in *Intelligent Vehicles Symposium (IV), IEEE*, Jun. 2010, pp. 217 –224.
[25] E. Richter, R. Schubert, and G. Wanielik, "Radar and vision based data fusion - advanced filtering techniques for a multi object vehicle tracking system," in *Intelligent Vehicles Symposium (IV), IEEE*, Jun. 2008, pp. 120 –125.
[26] A. Fossati, P. Schönmann, and P. Fua, "Real-time vehicle tracking for driving assistance," *Machine Vision and Applications*, pp. 1–10, 2010.
[27] B. Minoiu, S. Mammar, S. Glaser, and B. Lusetti, "Composite lyapunov based vehicle longitudinal control assistance," in *European Control Conference (ECC)*, 2009.
[28] S. Chaib, M. Netto, and S. Mammar, "H-infinity, adaptive, PID and fuzzy control: a comparison of controllers for vehicle lane keeping," in *Intelligent Vehicles Symposium (IV), IEEE*, Jun. 2004, pp. 139 – 144.
[29] R. Schubert, E. Richter, and G. Wanielik, "Comparison and evaluation of advanced motion models for vehicle tracking," in *Information Fusion*, 302008-july3 2008, pp. 1 –6.
[30] S. Glaser, B. Vanholme, S. Mammar, D. Gruyer, and L. Nouveliere, "Maneuver-based trajectory planning for highly autonomous vehicles on real road with traffic and driver interaction," *IEEE Trans. Intell. Transp. Syst.*, vol. 11, no. 3, pp. 589 –606, Sep. 2010.
[31] S. LaValle, *Planning algorithms*. Cambridge Univ Pr, 2006.
[32] F. Flemisch, C. Adams, S. Conway, K. Goodrich, M. Palmer, and P. Schutte, "The H-metaphor as a guideline for vehicle automation and interaction," in *Nat. Aeronautics Space Admin.*, 2003.
[33] D. Norman, *The design of future things*. Basic Books, 2009.