Design of a lane departure driver-assist system under safety specifications

Daniel Hoehener[1], Geng Huang[2] and Domitilla Del Vecchio[3]

***Abstract*— We use a controlled invariance approach to design a semi-autonomous lane departure assist system that is guaranteed to keep the vehicle in the lane. The controlled invariant safe set is the set of system states from which an input exists that can keep the vehicle in the lane. First we provide theoretical conditions under which the controlled invariant safe set has a simple characterization that can be quickly computed in real-time. We then use this characterization to derive a feedback strategy that keeps the vehicle in the lane and overrides the driver only if he/she could otherwise force a future lane departure. We also provide a detailed description of the above mentioned conditions, including algorithmic approaches that allow to verify whether these conditions are satisfied.**

I. Introduction

The development of autonomous vehicles has made rapid progress over the past 30 years, yet there remain important challenges, among which the ability to verify that systems can operate safely and robustly [7]. Nevertheless, already today it is possible to benefit from this progress via semi-autonomous safety systems. A good example are lane departure assist systems (LDAS) which already on their own have a large potential benefit for improving traffic safety. Indeed, according to the NHTSA FARS database [20], in 2013 12,703 people died in the United States after a lane departure, i.e. 42% of all traffic fatalities were preceded by a lane departure.

Most major car manufacturers are currently offering some type of lane departure assistance. The spectrum ranges from pure warning systems to lane keeping systems that proactively keep the vehicle in the center of the lane. These are vision based systems that use the vehicle position in the lane, its heading and a limited look-ahead horizon (based on the sensor capacity) to determine whether a warning or steering input is necessary, see for instance [8], [23]. The drawback of such a design is that it does not provide formal safety guarantees.

Approaches which provide guarantees that the vehicle will stay in a given lane can mainly be found in the autonomous driving literature. Such safety tools are in general referred to as lane keeping assistance systems, since they actively try to keep the vehicle in the center of the lane. One way to achieve this objective is to consider the lane keeping task as stabilization problem, where one tries to keep the distance to the center equal to zero [12], [24]. Notice that in these approaches the longitudinal speed is assumed to be constant. In a related approach [25], a two level architecture is proposed. The higher level uses a model predictive control scheme to determine a safe (meaning in the lane) state trajectory. The lower level controller then tracks this trajectory. Another stability-based approach using Lyapunov functions and a potential field was presented in [22]. It is also shown that this approach is robust under bounded time-varying disturbances.

When designing driver-assist systems such as LDAS, a crucial question is how the system should interact with the driver. Studies show that the acceptance of human drivers of systems that provide assistance in lane keeping is higher for systems that interfere less with the driver's steering [11]. The present work focuses on the design of a LDAS that is guaranteed to keep the vehicle in the lane while overriding the driver only when necessary to keep the vehicle inside the lane. The difference with the above cited approaches is that here we apply control input only when a lane departure is imminent, while the other approaches continuously apply steering to keep the vehicle near the center of the lane.

The major challenge in designing such a system is that it requires a procedure that allows to identify the system states from which there exists an admissible steering input that can keep the vehicle in the lane. The set of these states is called controlled invariant safe set. Determining whether a state is in this set (a safety verification task) often requires computationally intensive algorithmic procedures. Therefore the application of controlled invariance to real-world engineering problems has been limited to systems with special structures or small dimensions, see [3], [9], [10], [14] and references therein. Here we show that under certain conditions, that we specify, the controlled invariant safe set has a simple characterization that can be computed efficiently online. We therefore propose a system architecture that performs an initial safety check at the time the driver requests activation of the LDAS. If activation is safe (based on the above mentioned conditions), the system is enabled and continuously monitors the driver's steering inputs. The driver's inputs are overridden only if necessary to keep the vehicle in the lane.

The remainder of the paper starts with a discussion of the model and the formal statement of the problem in Section II. Section III contains the description of the proposed driver-assist system. The implementation of this system is discussed in Section IV which is followed by some concluding remarks in Section V.

[1]Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, USA hoehener@mit.edu

[2]Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, USA gengh@mit.edu

[3]Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, USA ddv@mit.edu

II. Model and problem formulation

We start this section with a description of the lane departure assist system (LDAS) that we want to design. In the second part of the section we introduce the model and provide a formal problem statement.

A. Lane Departure Assist

We consider a vehicle equipped with sensors, for instance a camera, that are able to determine the vehicle's distance from the left and right lane boundary, denoted by d_l and d_r respectively. In addition we assume that measurements on the vehicle's dynamics are available. In particular we assume the vehicle's sensors provide measurements of the longitudinal and lateral velocity U and V, yaw rate r and heading angle ψ, see Figure 1. Notice that estimates of yaw rate and lateral velocity could be obtained from measurements of lateral acceleration, see for instance [13]. The LDAS then

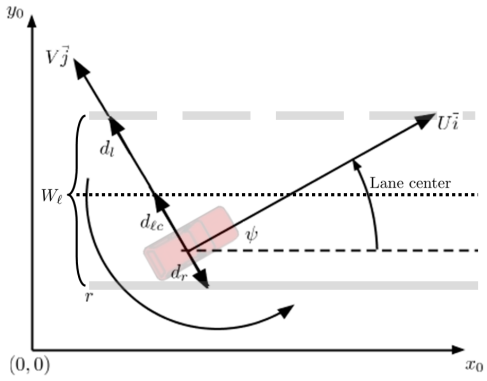

Fig. 1. The vehicle's longitudinal and lateral velocity U and V, as well as the oriented distances to the lane center, right and left lane boundary $d_{\ell c}$, d_r, d_l (arrows indicate direction of positive sign) are given with respect to a body-fixed coordinate frame with unit vectors $\vec{i}$ and $\vec{j}$. Heading angle ψ and yaw rate r are measured with respect to an inertial coordinate frame with axes (x_0, y_0).

uses this information to override the driver when a lane departure is imminent. It is therefore a *semi-autonomous* vehicle function that should act only when otherwise safety cannot be guaranteed. We call such a vehicle function a *safety supervisor*. Here we consider the case of a straight lane, see Assumption 1 below. Moreover, LDAS is restricted to use either right steering to avoid crossing the left lane boundary or left steering to avoid the right lane boundary and it cannot change the vehicle's speed, i.e. the longitudinal velocity U must remain constant during interventions of LDAS. In this setting the requirements for the safety supervisor are:

- Guarantee that the car remains in the lane at all times;
- Least conservative; meaning that the driver's steering input should be overridden only when necessary to prevent a lane departure.

Traditional lane departure warning systems use the distance to the lane boundaries to determine whether a warning has to be given to the driver, see for instance [16]. However, in general such an approach cannot guarantee safety as there are vehicle states from which the left steering needed to avoid crossing the right lane boundary might force the vehicle to eventually cross the left boundary. This is illustrated in Figure 2. For a provably safe design it is therefore important to guarantee that a steering override applied to prevent crossing one lane boundary will never cause an unavoidable lane departure on the opposite boundary.

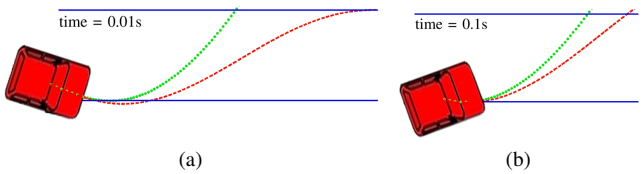

Fig. 2. The pictures show subsequent positions of the vehicle. The dotted and dashed trajectories represent the position of the vehicle while full left and full right steering is applied respectively. The solid lines represent boundaries that the center of gravity of the car should not cross. The simulations were carried out with the dynamical model presented in Section II-B, assuming that the vehicle has a large initial yaw rate, making the vehicle turn left independent of the steering angle. In Figure (a) left steering is required to keep the car in the lane. Steering first left however makes the avoidance of the left lane boundary impossible as shown in (b).

B. Notations and vehicle-lane dynamics

The vehicle dynamics take place in the continuous state space $X \subset \mathbb{R}^6$. In the following we will use a *body-fixed* reference frame that is fixed to the ego-vehicle's center of gravity, see Figure 1. All dynamical interactions will be described within this reference frame. The major simplifying assumption that we make is that the road lane is straight.

Assumption 1:

(i) The road lane is straight at all times;
(ii) The lane width $W_\ell > 0$ is known and constant.

The system states are (see Figure 1)

- (U, V) – longitudinal and lateral speed along, respectively perpendicular to the vehicle's path;
- (r, ψ) – yaw rate and heading angle with respect to a fixed reference frame;
- d_l, d_r – Distance between the vehicle and the left, respectively right lane boundary measured perpendicularly to the vehicle heading. They are both signed distances which are negative if the vehicle is on the wrong side of the corresponding lane boundary, see Figure 1.

and the (bounded) inputs are

- $\tau_w \in [-\bar{\tau}_w, \bar{\tau}_w]$ – wheel torque which represents brake torque if it is negative and $\bar{\tau}_w > 0$ is some constant;
- $\delta_f \in [-\bar{\delta}_f, \bar{\delta}_f]$ – front wheel steering angle and $\bar{\delta}_f > 0$ is some constant.

The full system state will be denoted by

$$x := (U, V, r, \psi, d_l, d_r) \in X.$$

For the vehicle dynamics we use a standard model, see for instance [21]. For the convenience of the reader we provide the derivation of the differential equation for d_l in the

Appendix. A description of the constants of the dynamical model is given in Table I.

$$\dot{U} = \frac{R}{J_w + mR^2}\Big(\tau_w - \frac{\rho_{air}}{2} C_D A_f U^2 R - C_{rr} mg - Rmg\sin(\theta_{road})\Big),$$

$$\begin{pmatrix}\dot{V}\\ \dot{r}\end{pmatrix} = \begin{pmatrix} -\frac{c_f + c_r}{mU} & \frac{c_r l_r - c_f l_f}{mU} - U \\ \frac{c_r l_r - c_f l_f}{J_z U} & -\frac{c_f l_f^2 + c_r l_r^2}{J_z U}\end{pmatrix}\begin{pmatrix} V \\ r\end{pmatrix} + \begin{pmatrix}\frac{c_f}{m}\\ \frac{c_f l_f}{J_z}\end{pmatrix}\delta_f,$$

$$\dot{\psi} = r,$$

$$\begin{pmatrix}\dot{d}_l\\ \dot{d}_r\end{pmatrix} = \tan(\psi) r \begin{pmatrix} d_l \\ d_r\end{pmatrix} + \begin{pmatrix} -U\tan(\psi) - V \\ U\tan(\psi) + V\end{pmatrix} =: f_\ell(x). \tag{1}$$

Notice that we use the standard abbreviations $c_f = \mu c_{f0}$ and $c_r = \mu c_{r0}$.

TABLE I

PARAMETERS OF THE VEHICLE DYNAMICS MODEL

Notation	Unit	Description
J_w	kg·m^2	Wheel inertia
J_z	kg·m^2	Moment of inertia with respect to vertical axis
m	kg	Vehicle mass
R	m	Tire radius
l_f	m	Distance center of gravity to front axle
l_r	m	Distance center of gravity to rear axle
C_D	–	Drag coefficient
A_f	m^2	Projected front area of the vehicle
c_{f0}	N/rad	Cornering stiffness front wheel at dry road
c_{r0}	N/rad	Cornering stiffness rear wheel at dry road
g	m/s^2	Acceleration due to gravity
ρ_{air}	kg/m^3	Air density
C_{rr}	–	Rolling resistance coefficient
θ_{road}	rad	Road gradient
μ	–	Road adhesion coefficient, takes values in $]0, 1]$.

For a set $A \subset \mathbb{R}^n$, $S(A)$ denotes the set of piecewise continuous signals with images in A. The *flow* of the dynamical system $\mathbf{x}\colon \mathbb{R}_+ \times S([-\bar\tau_w, \bar\tau_w]) \times S([-\bar\delta_f, \bar\delta_f]) \times X \to X$ is the map such that for all $x \in X$, $\mathbf{t}_w \in S([-\bar\tau_w, \bar\tau_w])$, $\mathbf{d}_f \in S([-\bar\delta_f, \bar\delta_f])$, $t \mapsto \mathbf{x}(t; \mathbf{t}_f, \mathbf{d}_f, x)$ solves the differential equation (1) with τ_w and δ_f replaced by $\mathbf{t}_w(t)$ and $\mathbf{d}_f(t)$ respectively. The component functions of the flow $\mathbf{x}$ are denoted by $\mathbf{x}_i$, $i \in \{1, \dots, 6\}$ and represent the trajectories of the corresponding state. For instance, $\mathbf{x}_4(t; \mathbf{t}_w, \mathbf{d}_f, x)$ is the vehicle's heading angle at time t, when the vehicle was controlled by $\mathbf{t}_w$ and $\mathbf{d}_f$ and in state $x \in X$ at time 0.

The model of vehicle dynamics is valid only under normal driving conditions. In particular it uses a linear model for the lateral tire forces which is realistic for small tire sideslip angles, see for instance [1]. Precisely the model is valid if

- Front and rear slip angles, denoted by β_f and β_r, are such that $\tan(\beta_f) \approx \beta_f$, respectively $\tan(\beta_r) \approx \beta_r$;
- Lateral tire forces can accurately be approximated by a linear model;
- The matrix in the lateral dynamics (1) is stable;
- Rolling and pitching motion of the car can be neglected.

To formulate these requirements in an explicit assumption, first recall that in our model the front and rear sideslip angles are given by

$$\beta_f \coloneqq (V + rl_f)/U \qquad \text{and} \qquad \beta_r \coloneqq (V - rl_r)/U,$$

see for instance [21, p. 30]. Front and rear tire slip angles, which shall be denoted by α_f and α_r, are functions of the steering angle and the front and rear sideslip angles,

$$\alpha_f \coloneqq \delta_f - \beta_f \qquad \text{and} \qquad \alpha_r \coloneqq -\beta_r.$$

Under good road conditions lateral tire forces can be accurately approximated by a linear model as long as the tire sideslip angles satisfy $-\pi/18 \le \alpha_f, \alpha_r \le \pi/18$, see for instance [21, p. 202]. We summarize this in the following:

Assumption 2:

(i) $c_{r0} l_r - c_{f0} l_f > 0$ and $l_r/2 < l_f < 2l_r$;

(ii) $-\pi/4 \le \beta_f \le \pi/4$ and $-\pi/18 \le \beta_r, \delta_f - \beta_f \le \pi/18$.

Assumption 2 (i) assures the stability requirement and is satisfied by cars and trucks, see [17, Sec. 6]. The second assumption guarantees small sideslip and tire slip angles respectively. For a more detailed discussion on the validity of this model see for instance [1], [21].

C. Problem statement

As described in Section II-A, the objective is to guarantee that the vehicle remains in the lane for all time. Hence the *safe set*, that is, the set of all states $x \in X$ that are in the lane, is given by

$$\mathcal{S} \coloneqq \{(U, V, r, \psi, d_l, d_r) \in X \mid \min\{d_l, d_r\} \ge 0\}. \tag{2}$$

In the following *safety* will always mean that the system state x belongs to the safe set $\mathcal{S}$. Since the LDAS that we investigate is a semi-autonomous vehicle function, we seek a feedback control strategy that keeps the state x in $\mathcal{S}$ for all time and overrides the driver steering only when necessary to do so. Such a feedback strategy will be called a *safety supervisor*. The principle is illustrated in Figure 3.

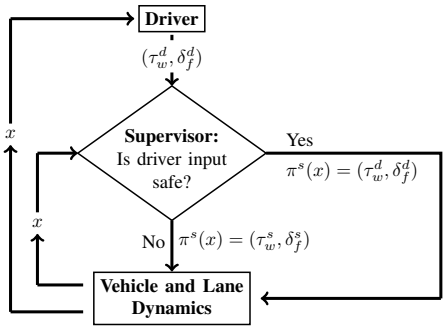

Fig. 3. Diagram shows the interaction between safety supervisor, driver and vehicle-lane dynamics. The system state is x, driver's input and the supervisor's input are denoted by (τ_w^d, δ_f^d) and (τ_w^s, δ_f^s) respectively. The supervisor's feedback control strategy π^s equals the driver's input whenever this input is safe.

Problem 1: Let $x \in X$ be the current system state. Find a feedback strategy $\pi^s\colon X \rightsquigarrow [-\bar\tau_w, \bar\tau_w] \times [-\bar\delta_f, \bar\delta_f]$ such that the corresponding flow satisfies

$$\mathbf{x}(t; \pi^s, x) \in \mathcal{S} \qquad \forall\, t \in \mathbb{R}_+.$$

We use in the following the convention that $\pi^s(x) = [-\bar\tau_w, \bar\tau_w] \times [-\bar\delta_f, \bar\delta_f]$ when the supervisor is inactive.

III. LANE DEPARTURE ASSIST SYSTEM

In this section we provide a solution to Problem 1. Assumption 1 shall hold throughout this section, hence the road lane is straight.

A. System architecture

As discussed in Section II-A, the safety supervisor is restricted to keep the longitudinal speed constant and to use the following steering strategies:

1. Steer left to avoid right lane boundary;
2. Steer right to avoid left lane boundary.

Since the focus in this paper is on steering control, to satisfy the requirement on longitudinal speed we make the following assumption.

Assumption 3: For every given longitudinal speed U, there exists a (feedback) torque input τ_w^s that allows to keep the longitudinal speed constant at U.

Notice that in practice such a torque input could be obtained from cruise control.

Recall that for a provably safe design that respects the above mentioned restrictions it is important to assure that the steering required to prevent the crossing of one lane boundary will not cause an unavoidable crossing of the other, see Figure 2. Finally, as discussed in Section II-B, the dynamical model is only valid when Assumption 2 holds true. To enforce these constraints in a semi-autonomous manner, we propose an architecture that has three main components, see Figure 4.

The first component is an initialization check, performed when the driver first tries to switch on the LDAS. The role of this check is to guarantee that the safety supervisor is not enabled while the driver is performing an extreme maneuver because in this case the safety supervisor might not be able to keep the vehicle in the lane. Mathematically this corresponds to the conditions outlined in Figure 4, where $U_{min}, U_{max}, \tilde{V}, \tilde{r}$ and $\tilde{\psi}$ are design parameters of the system. The appropriate selection of these parameters is discussed in Section III-C. If the initialization check is successful the status variable `enabled` is set to true. Otherwise the system remains disabled.

The second component is a status update, which continuously monitors whether the driver is keeping the speed and front wheel steering angle within the allowed range of operation, $[U_{min}, U_{max}]$ and $[-\bar{\delta}_f, \bar{\delta}_f]$ respectively. Here $\bar{\delta}_f$ is a design parameter. The necessity of this check comes from the fact that the system does not actively constrain the driver's wheel torque requests or front wheel steering angle. Instead, if the check fails the LDAS is disabled by setting the status variable `enabled` to false.

The last component is the actual safety supervisor. When the status variable `enabled` is true, it checks whether the driver's input will lead to an unavoidable lane departure and overrides the driver when this is the case. The next Section III-B is devoted to a detailed discussion of this supervisor and contains the statement of the formal safety guarantees, Theorem 3.1.

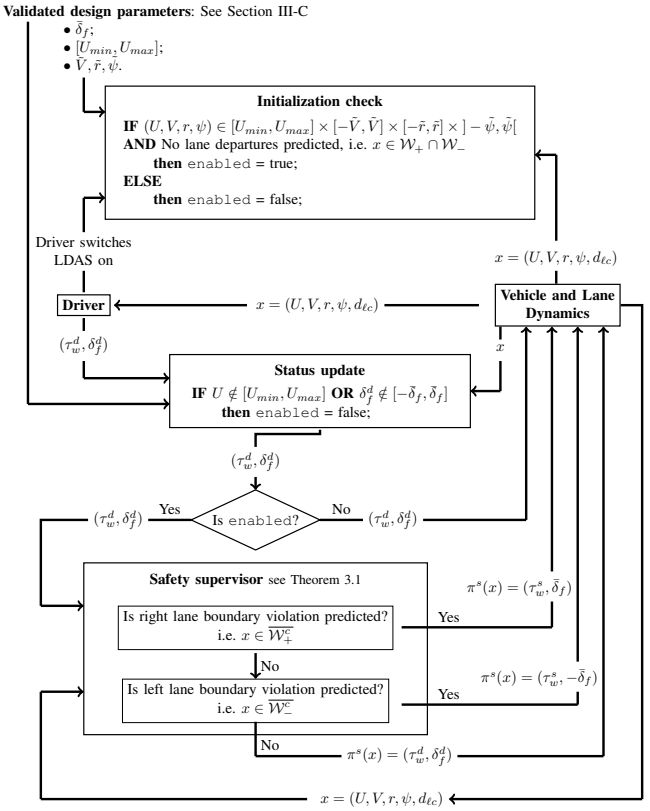

Fig. 4. Block diagram of the LDAS. The sets $\mathcal{W}_+$ and $\mathcal{W}_-$ are defined in (3). The system has a number of design parameters that have to be validated offline before the safety supervisor is guaranteed to keep the vehicle in the lane at all time.

B. Safety supervisor

In this section we design the feedback strategy π^s that provides a solution to Problem 1. The design requires three conditions that are introduced and discussed in the following three paragraphs. These conditions can be checked offline as described in Section III-C. In the fourth paragraph we formally define π^s and elaborate on the safety guarantees that it provides.

1) Range of operation of the system: Throughout this section $\bar{\tau}_w$ and $\bar{\delta}_f$ are positive constants as in Section II-B. Similarly, in accordance with the previous Section III-A, U_{min}, U_{max}, $\tilde{V}$, $\tilde{r}$ and $\tilde{\psi}$ are positive constants. The choice of these constants is the subject of the next section. The *reachable set* of a control system from a given set A of initial conditions, is the set of states $x \in X$ for which there exists an input signal that allows to steer the corresponding state trajectory from the set A to x. In the following the reachable set of the lateral dynamics plays an important role:

$$\mathcal{R}(\tilde{V}, \tilde{r}) := \Big\{ (\mathbf{x}_2, \mathbf{x}_3)(t; \mathbf{t}_w, \mathbf{d}_f, x) \;\Big|\; \mathbf{d}_f \in S([-\bar{\delta}_f, \bar{\delta}_f]), \\ \mathbf{t}_w \in S([-\bar{\tau}_w, \bar{\tau}_w]),\ (x_2, x_3) \in [-\tilde{V}, \tilde{V}] \times [-\tilde{r}, \tilde{r}], \\ t \in \mathbb{R}_+,\ \mathbf{x}_1(s; \mathbf{t}_w, \mathbf{d}_f, x) \in [U_{min}, U_{max}],\ \forall s \leq t \Big\}.$$

An *over approximation of the reachable set* is any set $\Omega \subset \mathbb{R}^2$ such that $\mathcal{R}(\tilde{V}, \tilde{r}) \subset \Omega$. The concept is illustrated in

Figure 5.

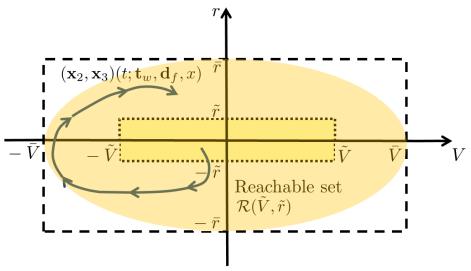

Fig. 5. Lateral velocity and yaw rate trajectories starting in the set $[-\tilde{V}, \tilde{V}] \times [-\tilde{r}, \tilde{r}]$ remain in the corresponding reachable set $\mathcal{R}(\tilde{V}, \tilde{r})$. The box $[-\bar{V}, \bar{V}] \times [-\bar{r}, \bar{r}]$ is an over approximation of this reachable set.

Condition 1:

(i) There exists an over approximation $\mathcal{R}$ of $\mathcal{R}(\tilde{V}, \tilde{r})$ such that
- $\max\{|(V - rl_f)/U_{min}| \mid (V, r) \in \mathcal{R}\} \leq \pi/18$;
- $\max\left\{\left|\bar{\delta}_f - \frac{V+rl_f}{U_{min}}\right| \,\middle|\, (V, r) \in \mathcal{R}\right\} \leq \pi/18$;

(ii) $\sqrt{\frac{(l_f+l_r)^2(c_{r0}l_r - c_{f0}l_f)}{4J_z}} < U_{min} \leq U_{max}$.

Notice that if the longitudinal speed remains within $[U_{min}, U_{max}]$ and the steering input in $[-\bar{\delta}_f, \bar{\delta}_f]$, then (i) guarantees that Assumption 2 (ii) is satisfied. Condition (ii) is a stability requirement, assuring that the lateral velocity and yaw rate reach their steady state in finite time.

2) Separation of steering tasks: In general it is not possible to consider the objectives: 1) stay left of the right lane boundary; 2) stay right of the left lane boundary; as independent control tasks, see Fig. 2. In the following we provide a condition under which a decoupling of these tasks is possible. Hence this condition allows to design a safety supervisor that respects the restrictions on the steering actions that were imposed in Section II-A.

First, for all $x = (U, V, r, \psi, d_l, d_r) \in X$, $\mathbf{t}_w \in \mathcal{S}([-\bar{\tau}_w, \bar{\tau}_w])$ and $\mathbf{d}_f \in \mathcal{S}([-\bar{\delta}_f, \bar{\delta}_f])$ we introduce the slightly altered state trajectory $\hat{\mathbf{x}}(\cdot; \mathbf{t}_w, \mathbf{d}_f, x)$ which for $i \in \{1, 2, 3\}$ is defined by $\hat{\mathbf{x}}_i(t; \mathbf{t}_w, \mathbf{d}_f, x) = \mathbf{x}_i(t; \mathbf{t}_w, \mathbf{d}_f, x)$ for all $t \in \mathbb{R}_+$. Moreover, using the abbreviation $[t] := (t; \mathbf{t}_w, \mathbf{d}_f, x)$,

$$\hat{\mathbf{x}}_4[t] = \begin{cases} \tilde{\psi} & \text{if } \mathbf{x}_4[t] \geq \tilde{\psi}, \\ \mathbf{x}_4[t] & \text{if } \mathbf{x}_4[t] \in]-\tilde{\psi}, \tilde{\psi}[, \\ -\tilde{\psi} & \text{if } \mathbf{x}_4[t] \leq -\tilde{\psi}, \end{cases}$$

and $(\hat{\mathbf{x}}_5[t], \hat{\mathbf{x}}_6[t])$ are such that $(\hat{\mathbf{x}}_5[0], \hat{\mathbf{x}}_6[0]) = (d_l, d_r)$ and for all $t \in \mathbb{R}_+$, $(\dot{\hat{\mathbf{x}}}_5[t], \dot{\hat{\mathbf{x}}}_6[t]) = f_\ell(\hat{\mathbf{x}}[t])$ where f_ℓ is defined in (1).

Notice that $\hat{\mathbf{x}}[t] = \mathbf{x}[t]$ for all t such that $\mathbf{x}_4[s] \in]-\tilde{\psi}, \tilde{\psi}[$ for all $s \leq t$. This is important as we show in Theorem 3.1 that our safety supervisor guarantees that the heading angle remains in $]-\tilde{\psi}, \tilde{\psi}[$. Hence under the feedback control of our safety supervisor these state trajectories are identical. The reason for this change of dynamics is that it allows to exclude some pathological behavior that would come from heading angles outside of $]-\pi/2, \pi/2[$.

With this notation we define the following sets:

$$\begin{aligned} \mathcal{T}_+(x) &:= \left\{ t \in \mathbb{R}_+ \;\middle|\; \hat{\mathbf{x}}_4(t; \bar{\mathbf{t}}_w, \bar{\mathbf{d}}_f, x) < \tilde{\psi} \right\}, \\ \mathcal{W}_+ &:= \left\{ x \in X \;\middle|\; \hat{\mathbf{x}}_6(t; \bar{\mathbf{t}}_w, \bar{\mathbf{d}}_f, x) \geq 0,\ \forall t \in \mathcal{T}_+(x) \right\}, \\ \mathcal{W}_{0+} &:= \left\{ x \in \mathcal{W}_+ \;\middle|\; d_r \geq 0, \exists t \in \overline{\mathcal{T}_+(x)} \right. \\ &\qquad \left. \text{s.t. } \hat{\mathbf{x}}_6(t; \bar{\mathbf{t}}_w, \bar{\mathbf{d}}_f, x) = 0 \text{ and } \dot{\hat{\mathbf{x}}}_6(t; \bar{\mathbf{t}}_w, \bar{\mathbf{d}}_f, x) = 0 \right\}, \end{aligned} \tag{3}$$

where for a given set A, $\overline{A}$ denotes its closure and the control inputs $\bar{\mathbf{t}}_w \in S([-\bar{t}_w, \bar{t}_w])$, $\bar{\mathbf{d}}_f \in S([-\bar{\delta}_f, \bar{\delta}_f])$ are such that for all $t \in \mathbb{R}_+$,

$$\bar{\mathbf{t}}_w(t) = \tau_w^s \qquad \text{and} \qquad \bar{\mathbf{d}}_f(t) = \bar{\delta}_f.$$

Here τ_w^s is the torque input from Assumption 3 that allows the safety supervisor to keep the longitudinal speed constant. Since the torque required to do this is bounded, we will assume in the following that $|\tau_w^s| \leq \bar{\tau}_w$.

Intuitively, the set $\mathcal{W}_+$ is the controlled invariant safe set for the right lane boundary, that is, the set of states such that there exists an admissible steering input that keeps the vehicle on the correct side of the lane boundary. The set $\mathcal{W}_{0+}$ is a subset of the boundary of $\mathcal{W}_+$, see Figure 6. The sets $\mathcal{T}_-(x)$, $\mathcal{W}_-$ and $\mathcal{W}_{0-}$ are defined analogously, with $\hat{\mathbf{x}}_6$, and $\bar{\mathbf{d}}_f$ replaced by $\hat{\mathbf{x}}_5$ and $-\bar{\mathbf{d}}_f$ respectively and correspond to the controlled invariant safe set of the left lane boundary.

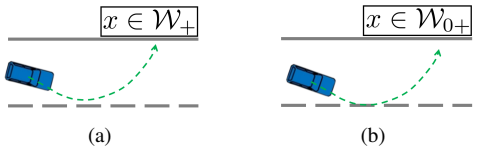

Fig. 6. The dashed arrow represents the vehicle's trajectory while left steering is applied. As long as this trajectory does not cross the right lane boundary the current state is in $\mathcal{W}_+$. If in addition there is a time at which the trajectory touches the lane boundary, see (b), then the state is in $\mathcal{W}_{0+}$.

It is intuitive that applying control only when a lane departure is imminent corresponds to overriding the driver when the supervisor's trajectory touches the lane boundary, i.e. when the current state is either in $\mathcal{W}_{0+}$ or $\mathcal{W}_{0-}$. We show that this is indeed a safe control strategy, see Theorem 3.1, if the following condition is satisfied.

Condition 2: $\mathcal{W}_{0+} \cap \mathcal{W}_{0-} = \emptyset$.

Notice that in practice this condition assures the non occurrence of the situation depicted in Figure 2.

3) Finite look-ahead horizon: The sets $\mathcal{W}_+$ and $\mathcal{W}_-$ are based on a prediction on the time horizon $\mathcal{T}_+$ and $\mathcal{T}_-$. As this time horizon is finite but we want to keep the vehicle in the lane on the infinite horizon $\mathbb{R}_+$, we need to ensure that at the end of the look-ahead horizons $\mathcal{T}_+$ and $\mathcal{T}_-$ there still exists a steering input that can keep the vehicle in the lane. As we show in Theorem 3.1 below, this is the case if the following conditions hold true:

Condition 3:

(i) For all $x = (U, V, r, \psi, d_l, d_r) \in X$ we have that
- if $\psi = \tilde{\psi}$ and $d_l \leq W_\ell / \cos(\tilde{\psi})$ then $x \in \mathcal{W}_-^c$;

- if $\psi = -\tilde{\psi}$ and $d_r \leq W_\ell / \cos(\tilde{\psi})$ then $x \in \mathcal{W}_+^c$;

(ii) $\sup \left\{ V/\tan(\tilde{\psi}) \;\middle|\; \exists r \text{ such that } (V,r) \in \mathcal{R} \right\} < U_{min}$,

where for a set A, A^c denotes its complement and $\mathcal{R}$ is the over approximation of $\mathcal{R}(\tilde{V}, \tilde{r})$ from Assumption 1.

Intuitively, this condition states that if the heading of the vehicle forms a large angle with the tangent to the lane, then the car cannot be kept on the road. The condition therefore simply reflects limitations due to the turning radius of the car, see Figure 7.

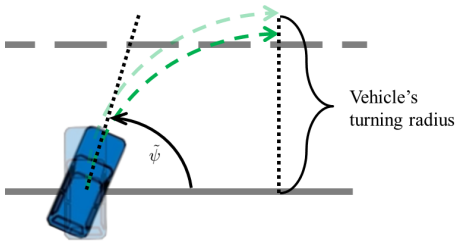

Fig. 7. If the vehicle's turning radius is larger than the lane width then for a large heading angle $\tilde{\psi}$ the car cannot remain in the lane.

4) Safety supervisor: We assume that all previously mentioned conditions are satisfied.

Theorem 3.1: Let $x^0 = (U^0, V^0, r^0, \psi^0, d_l^0, d_r^0) \in \mathcal{W}_+ \cap \mathcal{W}_-$ be such that

(i) $(U^0, V^0, r^0) \in [U_{min}, U_{max}] \times [-\tilde{V}, \tilde{V}] \times [-\tilde{r}, \tilde{r}]$;
(ii) $\psi^0 \in]-\tilde{\psi}, \tilde{\psi}[$.

Define $\pi^s \colon X \rightsquigarrow [-\bar{\tau}_w, \bar{\tau}_w] \times [-\bar{\delta}_f, \bar{\delta}_f]$ by

$$\pi^s(x) \coloneqq \begin{cases} (\tau_w^s, \bar{\delta}_f) & \text{if } x \in \overline{\mathcal{W}_+^c}, \\ (\tau_w^s, -\bar{\delta}_f) & \text{if } x \in \overline{\mathcal{W}_-^c} \setminus \overline{\mathcal{W}_+^c}, \\ [-\bar{\tau}_w, \bar{\tau}_w] \times [-\bar{\delta}_f, \bar{\delta}_f] & \text{otherwise.} \end{cases}$$

Then the corresponding flow satisfies for every $t \in \mathbb{R}_+$ such that $\mathbf{x}_1(s; \pi^s, x^0) \in [U_{min}, U_{max}]$ for all $s \in [0, t]$,

$$\mathbf{x}(t; \pi^s, x^0) \in \mathcal{S} \quad \text{and} \quad \mathbf{x}_4(t; \pi^s, x^0) \in]-\tilde{\psi}, \tilde{\psi}[. \tag{4}$$

A few remarks are in order. First notice that the conditions on x^0 correspond to the initialization check of the LDAS, see Figure 4. Thus if the initialization check is successful, then by (4) the vehicle is in the lane, as long as the longitudinal speed $\mathbf{x}_1(t; \pi^s, x^0) \in [U_{min}, U_{max}]$. That the safety guarantee only holds when the longitudinal velocity remains in $[U_{min}, U_{max}]$ corresponds to the status update of the LDAS, Figure 4. Moreover, by the definition of τ_w^s the longitudinal velocity remains constant when the safety supervisor overrides the driver. Finally, as we discuss in detail in Section IV, implementing this supervisor only requires to check whether a state is in $\mathcal{W}_+$ or $\mathcal{W}_-$ respectively. It follows directly from the definition of these sets that this test can be done by simple integration. Pseudo-code is provided in Section IV and a sketch of the proof is in the Appendix.

C. Bounds safety verification

Conditions 1-3 all impose some requirements on the design parameters U_{min}, U_{max}, $\tilde{V}$, $\tilde{r}$, $\tilde{\psi}$ and $\bar{\delta}_f$. Consequently, before the supervisor introduced in the previous section can be used to guarantee safety online, one has to verify offline that for the given choice of design parameters these conditions are satisfied. This verification process is depicted in Figure 8 and has two parts.

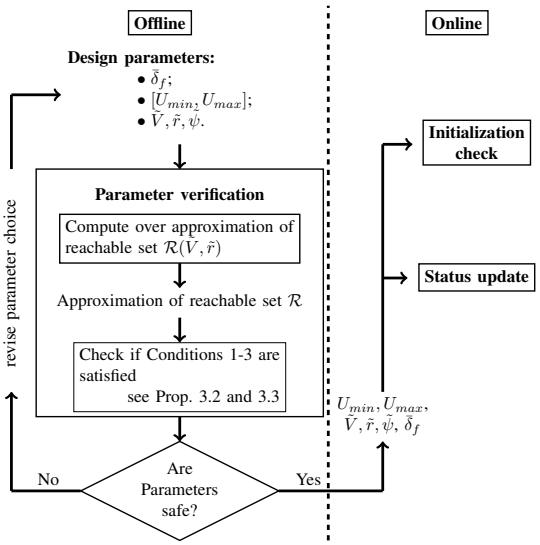

Fig. 8. We can test offline whether a set of parameters is valid. If the verification is successful these parameters can be used online to keep the system state up to date. Otherwise the parameter choice has to be revised.

First one has to compute an over approximation $\mathcal{R}$ of the reachable set $\mathcal{R}(\tilde{V}, \tilde{r})$. This is a well studied topic, see for instance [4], [6], [19], therefore we do not go into details here. Important considerations concerning the implementation of such an over approximation are provided in Section IV-B.

Then one uses the over approximation $\mathcal{R}$ to check whether Conditions 1-3 hold true. For Condition 1 this is straightforward. To check Condition 2-3 we introduce two auxiliary optimization problems, the value of which will then allow to formulate sufficient conditions for these assumptions.

Consider the nonlinear optimization problem

$$\underset{s \in \mathbb{R}_+, t \in \mathbb{R}_+, x \in X}{\text{Minimize}} \; \hat{\mathbf{x}}_5(t; \bar{\mathbf{t}}_w, -\bar{\mathbf{d}}_f, x)^2 + \hat{\mathbf{x}}_6(s; \bar{\mathbf{t}}_w, \bar{\mathbf{d}}_f, x)^2, \tag{5}$$

subject to

$$\begin{cases} \dot{\hat{\mathbf{x}}}_5(t; \bar{\mathbf{t}}_w, -\bar{\mathbf{d}}_f, x) = 0, \; \dot{\hat{\mathbf{x}}}_6(s; \bar{\mathbf{t}}_w, \bar{\mathbf{d}}_f, x) = 0, & \text{(6a)} \\ U \in [U_{min}, U_{max}], \; (V,r) \in \mathcal{R}, \; d_l, d_r \geq 0. & \text{(6b)} \end{cases}$$

It will be convenient to define the value of problem (5),

$$\mathcal{V}_1 \coloneqq \min \left\{ \hat{\mathbf{x}}_5(t; \bar{\mathbf{t}}_w, -\bar{\mathbf{d}}_f, x)^2 + \hat{\mathbf{x}}_6(s; \bar{\mathbf{t}}_w, \bar{\mathbf{d}}_f, x)^2 \;\middle|\; \text{subject to (6a)-(6b)} \right\}.$$

Notice that $\mathcal{V}_1$ is well defined since 0 is obviously a lower bound and the set of feasible points is closed.

Proposition 3.2: If $\mathcal{V}_1 > 0$ then Condition 2 holds true.

To check Condition 3 consider the problem

$$\underset{t \in \mathbb{R}_+, x \in X}{\text{Minimize}} \; -\hat{\mathbf{x}}_6(t; \bar{\mathbf{t}}_w, -\bar{\mathbf{d}}_f, x), \tag{7}$$

subject to

$$\begin{cases} \hat{\mathbf{x}}_4(t;\bar{\mathbf{t}}_w,\bar{\mathbf{d}}_f,x)=0, \quad U\in[U_{min},U_{max}] & \text{(8a)} \\ (V,r)\in\mathcal{R},\ \psi=-\tilde{\psi}, \quad d_r=W_\ell/\cos(\tilde{\psi}). & \text{(8b)} \end{cases}$$

As above we define the value of problem (7) by

$$\mathcal{V}_2 := \min\left\{-\hat{\mathbf{x}}_6(t;\bar{\mathbf{t}}_w,\bar{\mathbf{d}}_f,x) \;\middle|\; t,x \text{ satisfy (8a)-(8b)}\right\}.$$

As standard arguments allow to show that $\mathcal{T}_+(x)$ is bounded for all feasible $x\in X$, it is easy to see that the set of feasible points is compact and non empty. The value $\mathcal{V}_2$ is therefore well-defined.

Proposition 3.3: If $\mathcal{V}_2>0$ then Condition 3 holds true.

The proofs of these propositions are straightforward and therefore omitted.

As depicted in Figure 8, if the parameter verification fails one has to revise the parameter choice. By Propositions 3.2 and 3.3, the verification fails if either $\mathcal{V}_1$ or $\mathcal{V}_2$ is too small. Tightening the active constraints of the corresponding optimization problems (5) and (7) will usually increase the value and thus eventually lead to valid parameters.

IV. Implementation

The LDAS described in Section III has two main parts. Before the system is put into operation, we have to find a set of parameters that is safe according to the test outlined in Figure 8. Using a verified set of parameters, the safety supervisor depicted in Figure 4 runs online to keep the vehicle in the lane. In the following we provide details on the implementation of these two parts.

A. Safety supervisor

The logic diagram of the full algorithm is depicted in Figure 4. Here we focus on the implementation of the safety supervisor block, that is, on the implementation of the feedback strategy given in Theorem 3.1. For the purpose of discretization we use a fixed step size $\Delta t>0$ and perform a forward Euler approximation in order to compute the state that would result by applying the driver input (τ_w^d,δ_f^d). Checking whether this state is in $\mathcal{W}_+\cap\mathcal{W}_-$ is simply done by integration. Pseudo code is provided in Algorithm 1. Notice that in Algorithm 1 we abbreviate (1) by $\dot{x}=f(x,\tau_w,\delta_f)$.

B. Design parameter verification

As discussed in detail in Section III-C, the parameter verification requires to find an over approximation of the reachable set $\mathcal{R}(\tilde{V},\tilde{r})$ and the solution of the optimization problems (5) and (7). There exist already many tools for these tasks. We would however like to stress that in order to have safety guarantees, one needs to use tools with guaranteed accuracy. To be precise, for the reachable set we need a guaranteed over approximation. For a freely available software tool that allows to compute this, see for instance [2]. Similarly, for the optimization problems we need to find a guaranteed lower bound of the values $\mathcal{V}_1$ and $\mathcal{V}_2$. Such bounds can be provided by global optimization algorithms, see for instance [5] and [18] for the corresponding software.

Algorithm 1: Safety supervisor

Input: Current state x and driver input (τ_w^d,δ_f^d)
Output: Wheel torque and front wheel steering angle (τ_w,δ_f)

```
(τ_w, δ_f) ← (τ_w^d, δ_f^d);
x^pred ← x + Δt f(x, τ_w^d, δ_f^d);
x ← x^pred;
while x_4 ≤ ψ̃ do
    if x_6 < 0 then
        (τ_w, δ_f) ← (τ_w^s, δ̄_f); BREAK;
    else
        x ← x + Δt f(x, τ_w^s, δ̄_f);
    end if
end while
x ← x^pred;
while x_4 ≥ −ψ̃ do
    if x_5 < 0 then
        (τ_w, δ_f) ← (τ_w^s, −δ̄_f); BREAK;
    else
        x ← x + Δt f(x, τ_w^s, −δ̄_f);
    end if
end while
return (τ_w, δ_f);
```

C. Simulations

We implemented Algorithm 1 in Matlab and used it to prevent lane departures of a simulated driver with a tendency to drift to the right. The result of the simulation is shown in Figure 9. In the simulation we represent the center of gravity of the car by a red circle and its heading by a black arrow. The safety supervisor keeps the center of gravity between the solid blue lines. At 3.15s the driver is overridden to avoid a lane departure. When the danger is averted control is given back to the driver.

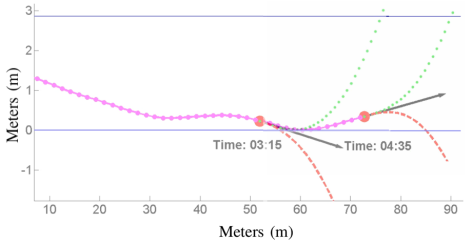

Fig. 9. Result of the simulation described in Section IV-C. The dashed-dotted line represents the actual vehicle trajectory. The dashed trajectory and the dotted trajectory correspond to right and left steering respectively.

V. Conclusions

We used a formal approach to design a semi-autonomous lane departure warning system. The core of this system is a safety supervisor that uses the controlled invariant safe set to determine when to act. This guarantees both safety and that the driver is overridden only when necessary. Moreover, the supervisor is computationally efficient and easy to implement. The design of the supervisor is based on a number of parameters that have to be verified before safety can be guaranteed. It was shown that this verification can be done algorithmically. When the system is operational,

an initialization check is performed when the driver switches the system on. This test ensures that the LDAS is enabled only under conditions for which safety can be guaranteed. If the initialization check is successful, the safety supervisor is enabled and guarantees that the vehicle stays in the lane at all time.

The most restrictive assumption that we made is that the lane is straight. In future work this assumption should be relaxed. In addition, it was assumed that the system dynamics could be modeled accurately. As in practice these dynamics are subject to uncertainties and disturbances, the design should be extended to accommodate bounded uncertainties. Finally, it would be desirable to have an algorithm that allows to revise the parameter choice automatically when the parameter verification fails.

APPENDIX

a) Derivation of differential equation for d_l: In order to derive a differential equation for d_l, we first notice that the following two equations have to be satisfied, see Figure 1.

$$\frac{d}{dt}\left[d_l\vec{j}\right] = \dot{d}_l\vec{j} + d_l\dot{\vec{j}} = \dot{d}_l\vec{j} - d_l r\vec{i},$$
$$\frac{d}{dt}\left[d_l\vec{j}\right] = \tau\begin{pmatrix}\cos(\psi)\\ -\sin(\psi)\end{pmatrix} - \begin{pmatrix}U\\ V\end{pmatrix},$$

where τ is a parameter representing the velocity of the projection onto the left lane boundary. Solving this system of equations for τ and $\dot{d}_l$ we find that

$$\tau = \frac{U - d_l r}{\cos(\psi)} \quad \text{and} \quad \dot{d}_l = (d_l r - U)\tan(\psi) - V.$$

b) Proof of Theorem 3.1: We provide here a sketch of the proof. Full details can be found in [15].

We start by fixing $x^0 \in X$ as in the statement of the theorem. It suffices to show that $\hat{\mathbf{x}}(t;\pi^s,x^0) \in \mathcal{W}_+ \cap \mathcal{W}_-$ and $\hat{\mathbf{x}}_4(t;\pi^s,x^0) \in]-\tilde{\psi},\tilde{\psi}[$ for all $t \in \mathbb{R}_+$ such that

$$\mathbf{x}_1(s;\pi^s,x^0) \in [U_{min},U_{max}] \quad \forall s \in [0,t]. \tag{9}$$

It will be convenient to denote the set of all times $t \in \mathbb{R}_+$ for which (9) is satisfied by T.

Step 1: Show that $\hat{\mathbf{x}}(t;\pi^s,x^0) \in \mathcal{W}_+$ for all $t \in T$. This can be done by contradiction, assuming that there exists $t \in T$ such that $\hat{\mathbf{x}}(t;\pi^s,x^0) \notin \mathcal{W}_+$. The contradiction follows readily from the definition of π^s and $\mathcal{W}_+$.

Step 2: Set $t^* := \inf\{t \in T \mid \hat{\mathbf{x}}_4(t;\pi^s,x^0) \in \{-\tilde{\psi},\tilde{\psi}\}\}$, where $t^* = \infty$ if this set is empty. Then show that $\hat{\mathbf{x}}(t;\pi^s,x^0) \in \mathcal{W}_-$ for all $t \in T \cap [0,t^*[$. This is again done by a contradiction argument and uses the conclusion of Step 1 and Condition 2.

Step 3: Show that $t^* = \infty$. This follows once more by contradiction. Indeed, from Step 1 and 2 we know that $\hat{\mathbf{x}}(t;\pi^s,x^0) \in \mathcal{W}_+ \cap \mathcal{W}_-$ for all $t \in [0,t^*[$. Since one can show that the set $\mathcal{W}_+ \cap \mathcal{W}_-$ is closed, it follows that if $t^* < \infty$ then also $\hat{\mathbf{x}}(t^*;\pi^s,x^0) \in \mathcal{W}_+ \cap \mathcal{W}_-$. This however is by Condition 3 impossible. ■

REFERENCES

[1] J. Ackermann, A. Bartlett, D. Kaesbauer, W. Sienel, and R. Steinhauser, *Robust control*. Springer Berlin, 1993.

[2] M. Althoff, *CORA 2015 Manual*, TU Munich, 85748 Garching, Germany, 2015.

[3] M. Althoff and J. M. Dolan, "Online verification of automated road vehicles using reachability analysis," *IEEE Transactions on Robotics*, vol. 30, pp. 903–918, 2014.

[4] M. Althoff, O. Stursberg, and M. Buss, "Reachability analysis of nonlinear systems with uncertain parameters using conservative linearization," in *Conference on Decision and Control*, 2008, pp. 4042–4048.

[5] I. P. Androulakis, C. D. Marnas, and C. A. Floudas, "αBB: A global optimization method for general constrained nonconvex problems," *J. Global Optim.*, vol. 7, pp. 337–363, 1995.

[6] R. Baier and M. Gerdts, "A computational method for non-convex reachable sets using optimal control," in *European Control Conference*, 2009, pp. 97–102.

[7] M. Campbell, M. Egerstedt, J. P. How, and R. M. Murray, "Autonomous driving in urban environments: approaches, lessons and challenges," *Phil. Trans. Soc. A*, vol. 368, pp. 4649–4672, 2010.

[8] J. M. Clanton, D. M. Bevly, and A. S. Hodel, "A low-cost solution for an integrated multisensor lane departure warning system," *IEEE Trans. Intell. Transp. Syst.*, vol. 10, pp. 47–59, 2009.

[9] V. R. Desaraju, H. C. Ro, M. Yang, E. Tay, S. Roth, and D. Del Vecchio, "Partial order techniques for vehicle collision avoidance: Application to an autonomous roundabout test-bed," in *Robotics and Automation, IEEE International Conference on*, 2009, pp. 82–87.

[10] J. Ding, J. Sprinkle, C. J. Tomlin, S. S. Sastry, and J. L. Paunicka, "Reachability calculations for vehicle safety during manned/unmanned vehicle interaction," *J. Guidance, Control and Dynamics*, vol. 35, pp. 138–152, 2012.

[11] T. Fujioka, Y. Shirano, and A. Matsushita, "Driver's behavior under steering assist control system," in *IEEE Intell. Transp. Syst.*, 1999, pp. 246–251.

[12] J. Guldner, H.-S. Tan, and S. Patwardhan, "Analysis of automatic steering control for highway vehicles with look-down lateral reference systems," *Vehicle System Dynamics*, vol. 26, pp. 243–269, 1996.

[13] A. Hac and M. D. Simpson, "Estimation of vehicle side slip angle and yaw rate," SAE Technical Paper 2000-010696, Tech. Rep., 2000.

[14] M. Hafner, D. Cunningham, L. Caminiti, and D. Del Vecchio, "Cooperative collision avoidance at intersections: Algorithms and experiments," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, pp. 1162–1175, 2013.

[15] D. Hoehener, G. Huang, and D. Del Vecchio, "Design of a lane departure driver-assist system under safety specifications: theorems and proofs," Massachusetts Institute of Technology, Tech. Rep., 2016.

[16] C. R. Jung and C. R. Kelber, "A lane departure warning system using lateral offset with uncalibrated camera," in *IEEE Intell. Transp. Syst.*, 2005, pp. 348–353.

[17] D. Karnopp, *Vehicle Stability*. CRC Press, 2004.

[18] R. Misener and C. A. Floudas, "ANTIGONE: Algorithms for continuous / integer global optimization of nonlinear equations," *Journal of Global Optimization*, vol. 59, pp. 503–526, 2014.

[19] I. Mitchell and C. J. Tomlin, "Overapproximating reachable sets by Hamilton-Jacobi projections," *J. Sci Comput*, vol. 19, pp. 323–346, 2003.

[20] Fatality analysis reporting system. National Highway Traffic Safety Administration NHTSA. [Online]. Available: http://www.nhtsa.gov/FARS

[21] R. Rajamani, *Vehicle Dynamics and Control*. Springer Verlag, 2012.

[22] E. J. Rosetter and J. C. Gerdes, "Lyapunov based performance guarantees for a the potential field lane-keeping assistance system," *IEEE Trans. ASME*, vol. 128, pp. 510–522, 2006.

[23] S. G. S. Mammar and M. Netto, "Time to line crossing for lane departure avoidance: A theoretical study and an experimental settting," in *IEEE Intell. Transp. Syst.*, 2006, pp. 226–241.

[24] Y. S. Son, W. Kim, S.-H. Lee, and C. C. Chung, "Robust multirate control scheme with predictive virtual lane for lane-keeping system of autonomous highway driving," *IEEE Trans. Vehicular Technology*, vol. 64, pp. 3378–3391, 2015.

[25] T. Weiskircher and B. Ayalew, "Frameworks for interfacing trajectory tracking with predictive trajectory guidance for autonomous road vehicles," in *American Control Conference*, 2015.