Safety Analysis of Automotive Control Systems Using Multi-Modal Port-Hamiltonian Systems

Siyuan Dai
Institute for Software-Integrated Systems
Vanderbilt University
Nashville, TN, USA
siyuan.dai@vanderbilt.edu

Xenofon Koutsoukos
Institute for Software-Integrated Systems
Vanderbilt University
Nashville, TN, USA
xenofon.koutsoukos@vanderbilt.edu

ABSTRACT

Safety analysis is important when designing and developing cyber-physical systems (CPS). An autonomous vehicle can be described as a complex CPS where the physical dynamics of the vehicle interact with the control systems. The challenge is ensuring safety despite nonlinearities, hybrid dynamics, and disturbances as well as complex cyber-physical interactions. In this paper, we present an approach for the safety analysis of automotive control systems using multi-modal port-Hamiltonian systems (PHS). The approach uses the Hamiltonian function to represent the energy of the safe and unsafe states and employs passivity to prove that trajectories that begin in safe regions cannot enter unsafe regions. We first apply the approach to the safety analysis of a longitudinal vehicle dynamics composed with an adaptive cruise control (ACC) system. We then extend the results to the safety analysis of a combined longitudinal and lateral vehicle dynamics composed with an ACC and lane keeping control (LKC) system. Simulation results are presented to demonstrate the approach.

1. INTRODUCTION

An autonomous vehicle is an example of a complex cyber-physical system (CPS) containing physical dynamics and controllers controlling the speed and steering of the vehicle [17]. An adaptive cruise control (ACC) system controls the speed of the vehicle and is a hybrid system operating in two modes, throttle control mode where the throttle angle is determined and brake control mode where the brake pressure is determined. A lane keeping control (LKC) system controls the angle of the steering wheel in order to maintain a desired position on the road. Safe operation is an important requirement for a vehicle equipped with an ACC and LKC system.

The design of the ACC and LKC systems must ensure that the host vehicle can safely navigate roads. The appearance of a lead vehicle provides an additional constraint for the ACC in that the host vehicle maintains a desired speed depending on the behavior of the lead vehicle. A lead vehicle which suddenly decelerates creates a safety problem for the host vehicle. The ACC design on the host vehicle must guarantee that the distance between the lead and host vehicle stay above a minimum threshold. Turns and curves provide constraints for the LKC in that the host vehicle must maintain a position in the center of the road. Large road curvatures create skidding problems for the host vehicle. The ACC and LKC design on the host vehicle must guarantee that the lateral acceleration does not exceed a maximum threshold. The challenge considered in this paper is to prove the safety of an automotive control system consisting of ACC and LKC despite the nonlinearities, hybrid dynamics, and disturbances present in the system.

The contribution of this paper is an approach for the safety analysis of CPS such as automotive control systems. The dynamics of the vehicle and the control systems are described using port-Hamiltonian systems (PHS) which gives the approach the benefit of compositionality. Hybrid behavior is characterized using multi-modal PHS. The approach represents the safe states of the system using a bounded from above energy level of the Hamiltonian function. Similarly, the unsafe states of the system are represented using a bounded from below energy level of the Hamiltonian function. Passivity is used to prove that as long as the safe and unsafe energy regions do not overlap, trajectories that begin within a lower energy level (safe states) cannot terminate within a higher energy level (unsafe states). The approach can be applied to any system described as a multi-modal PHS.

We evaluate the approach by analyzing the safety conditions for two systems. First, we assume a straight road and consider the longitudinal dynamics and the ACC. We derive safety conditions for the ACC which ensure that the host vehicle does not collide with a lead vehicle. Second, we assume a curved road and consider the interactions between the longitudinal dynamics, lateral dynamics, ACC, and LKC. We derive safety conditions for the ACC and LKC which ensure that the host vehicle does not collide with a lead vehicle and skid off of the road. We use the vehicle parameters, disturbances, and safety conditions to select control parameters so that the closed-loop system is safe. In order to validate the approach, we present simulation results by implementing the closed-loop system using Simulink [9] and CarSim [2].

The rest of the paper is organized as follows. Section 2 presents the related work. Section 3 presents the energy-based safety analysis approach applied to multi-modal PHS. Section 4 applies the safety analysis approach to the longi-

HSCC'16, April 12-14, 2016, Vienna, Austria
© 2016 ACM. ISBN 978-1-4503-3955-1/16/04...$15.00
DOI: http://dx.doi.org/10.1145/2883817.2883845

tudinal dynamics of the vehicle composed with the ACC system. Section 5 extends the results of Section 4 by including the lateral dynamics and LKC system. Section 6 presents the simulation results which show that the closed-loop system is safe. The paper is concluded in Section 7.

2. RELATED WORK

The theory of PHS is presented in detail in [5]. A PHS consists of a set of ports (control, interaction, resistive, and storage) interconnected through a power-conserving Dirac structure [18]. PHS have significant implications for passivity, which has been studied extensively for control design and analysis of nonlinear systems [8]. An important property of PHS is compositionality, where component PHS compose with each other through the interaction ports of their respective Dirac structures. PHS provide a compositional framework for modeling complex physical lumped-parameter systems [3].

Barrier certificates, which are similar in structure to Lyapunov functions, are typically used for the purpose of validating nonlinear systems with uncertainties [10]. The use of barrier certificates allows for the validation of a larger class of continuous-time nonlinear models, including differential-algebraic systems with uncertain inputs [16]. Barrier certificates are functions which denote that there are no state trajectories starting from a given set of initial conditions that end up in an unsafe region [14].

Barrier certificates are also extended to guarantee safety of hybrid systems [11]. These barrier certificates are functions of both continuous and discrete states. To prove the safety of a hybrid system, a barrier certificate is constructed from a set of continuous state functions where each function corresponds to a discrete state. Each continuous state function needs to satisfy the barrier certificate inequalities in the invariant of the corresponding discrete mode in order to guarantee the safety of the hybrid system. The work presented in this paper is inspired by the concept of barrier certificates, using the Hamiltonian function as a barrier between safe and unsafe states. In contrast to a barrier certificate, the Hamiltonian function is derived from the model.

As the number of controllers added to automobiles increase, automotive CPS become more complex and rigorous engineering methods are needed to ensure safety [15]. Control barrier functions have been used in a control design approach demonstrated for ACC and place constraints on the host vehicle's acceleration and deceleration [1]. They balance the objectives of maintaining a desired host vehicle velocity and a relative distance above a minimum threshold.

The computation of barrier certificates is challenging and often computationally expensive [12]. If the dynamic equations of the system are described as polynomial functions, a sum of squares programming method can be used to approximate the barrier certificates by characterizing state regions as semi-algebraic sets and using semi-definite programming to obtain the optimal solution [13]. The method is restrictive because the dynamic equations of many physical systems cannot be described as polynomial functions.

The approach presented in this paper can be applied to systems with nonlinearities and hybrid dynamics because safety is characterized by the Hamiltonian function and the PHS structure. The inherent passive property of PHS yields the safety conditions and allows the Hamiltonian function to function as a barrier certificate.

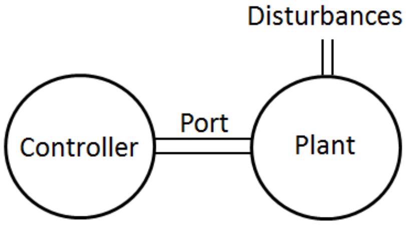

Figure 1: Generic plant system (with disturbances) and control system

3. SAFETY ANALYSIS APPROACH

The idea of the approach is to use the energy of the system as conditions and constraints in order to show the safety property of the system. We consider the plant and controller dynamics described by multi-modal PHS. We use the dynamic equations and Hamiltonian functions to derive the dynamic equations and Hamiltonian function of the closed-loop system. We characterize the initial and unsafe regions using the energy of the Hamiltonian function and show that the system trajectory cannot enter the unsafe region.

3.1 Multi-Modal PHS

Figure 1 provides a diagram of a generic multi-modal PHS of a plant system with disturbances connected to a control system via power ports. Given a plant system with a Hamiltonian function $H_p(x_p)$, continuous states $x_p \in X_p \subseteq \mathbb{R}^{n_p}$, discrete states $s_p \in S_p$, disturbances $\delta \in \mathbb{R}^o$, and a control system a Hamiltonian function $H_c(x_c)$, continuous states $x_c \in X_c \subseteq \mathbb{R}^{n_c}$, and discrete states $s_c \in S_c$, where $\{n_p, n_c, o\} \in \mathbb{N}^4$, we can write the set of dynamic equations of the closed-loop system as an input-state-output multi-modal PHS with Hamiltonian function $H(x) = H_p(x_p) + H_c(x_c)$, continuous states $x = \begin{bmatrix} x_p & x_c \end{bmatrix}^\mathsf{T} \in X = X_p \times X_c$, discrete states $s = \begin{bmatrix} s_p & s_c \end{bmatrix}^\mathsf{T} \in S = S_p \times S_c$, initial states $X_0 = X_{p0} \times S_{p0} \times X_{c0} \times S_{c0}$, and discrete transitions $\mathbb{T} \subseteq (X \times S) \to (X \times S)$:

$$\begin{cases} \dot{x} & = [J(x,s) - R(x,s)] \frac{\partial H}{\partial x} + \begin{bmatrix} L_p(x_p, s_p) \\ 0 \end{bmatrix} \delta \\ \zeta & = \begin{bmatrix} L_p^\mathsf{T}(x_p, s_p) & 0 \end{bmatrix} \frac{\partial H}{\partial x} \end{cases} \tag{1}$$

$$J(x,s) = \begin{bmatrix} J_p(x_p, s_p) & -G_p(x_p, s_p) G_c^\mathsf{T}(x_c, s_c) \\ G_c(x_c, s_c) G_p^\mathsf{T}(x_p, s_p) & J_c(x_c, s_c) \end{bmatrix},$$

$$R(x,s) = \begin{bmatrix} R_p(x_p, s_p) & 0 \\ 0 & R_c(x_c, s_c) \end{bmatrix},$$

where $J_p(x_p, s_p) \in \mathbb{R}^{n_p \times n_p}$ and $J_c(x_c, s_c) \in \mathbb{R}^{n_c \times n_c}$ are skew-symmetric interconnection matrices, $R_p(x_p, s_p) \in \mathbb{R}^{n_p \times n_p}$ and $R_c(x_c, s_c) \in \mathbb{R}^{n_c \times n_c}$ are symmetric positive semi-definite damping matrices, $G_p(x_p, s_p) \in \mathbb{R}^{n_p \times m}$, $G_c(x_c, s_c) \in \mathbb{R}^{n_c \times m}$, $L_p(x_p, s_p) \in \mathbb{R}^{n_p \times o}$, and (δ, ζ) are the input-output pairs corresponding to the disturbance port.

3.2 Safety Problem

Given a hybrid system represented as (1) with Hamiltonian function $H(x)$ and bounded disturbances, the safety problem is to show that there are no trajectories of the closed-loop system that reach an unsafe region of the state space.

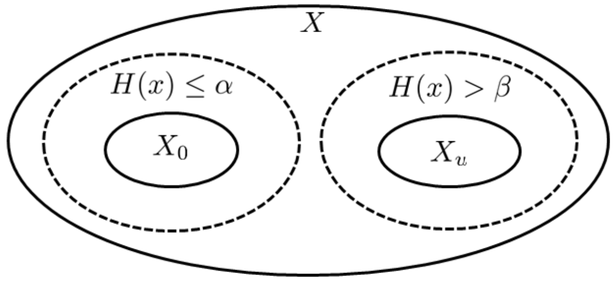

Figure 2: The Hamiltonian function prevents the trajectory from reaching the unsafe set X_u.

Definition 1. *Given a multi-modal PHS (1) and $H(x)$ with continuous states $X = X_p \times X_c \subseteq \mathbb{R}^{n_p+n_c}$, discrete states $S = S_p \times S_c$, initial states $X_{p0} \times X_{c0} \times S_{p0} \times S_{c0} \subseteq X \times S$, unsafe states $X_{pu} \times X_{cu} \times S_{pu} \times S_{cu} \subseteq X \times S$, and disturbances $\Delta \subset \mathbb{R}^o$, a system trajectory $\Gamma(x(t), s(t)) : [0, T] \to X \times S$ is unsafe if there exists a positive time instant T and a finite sequence of discrete transition times $0 \leq t_1 \leq \cdots \leq t_N \leq T$ such that $\Gamma(x(0), s(0)) \in X_{p0} \times X_{c0} \times S_{p0} \times S_{c0}$ and $\Gamma(x(T), s(T)) \in X_{pu} \times X_{cu} \times S_{pu} \times S_{cu}$. The system is safe if there are no unsafe state trajectories.*

3.3 Safety Analysis

We consider the following definitions for initial states, unsafe states, and guard conditions that specify discrete mode transitions. For each discrete state $s \in S$, the initial continuous states are defined as $\text{Init}(s) = \{x \in X : (x, s) \in X_{p0} \times X_{c0} \times S_{p0} \times S_{c0}\}$ and the unsafe continuous states are defined as $\text{Unsafe}(s) = \{x \in X : (x, s) \in X_{pu} \times X_{cu} \times S_{pu} \times S_{cu}\}$. Each transition of discrete states from $s \in S$ to $s' \in S$ is associated with the guard condition $\text{Guard}(s, s') = \{x, x' \in X : \{x, s\} \to \{x', s'\} \in \mathbb{T}\}$.

Similar to safety analysis using barrier certificates, the method in this paper shows that trajectories beginning from the safe region cannot reach the unsafe region. However, the barrier certificate typically separates the initial and unsafe states using its zero level set, while the Hamiltonian function characterizes the initial and unsafe states using two energy levels. A canonical coordinate transform Φ is needed to convert the dynamic equations and Hamiltonian function of the system into a form which shows the actual minimum energy. Technical details regarding canonical coordinate transformation of PHS can be found in [7]. The passivity condition prevents trajectories starting in the safe region from reaching the unsafe region. Figure 2 provides a visual illustration of the method.

Theorem 1. *A multi-modal PHS described by (1) and $H(x)$, with continuous states $x \in X$, discrete states $s \in S$, initial states $\text{Init}(s)$, unsafe states $\text{Unsafe}(s)$, and bounded disturbances $\delta \in \Delta$ is safe if the canonical coordinate transformation $\overline{x} = \Phi(x)$ and transformed Hamiltonian function $H(\Phi^{-1}(\overline{x}))$ satisfy the following four conditions with $\alpha \leq \beta$*

1. $H(\Phi^{-1}(\overline{x})) \leq \alpha, \forall x \in \text{Init}(s)$

2. $H(\Phi^{-1}(\overline{x})) > \beta, \forall x \in \text{Unsafe}(s)$

3. $\zeta^{\mathsf{T}}\delta \leq \frac{\partial H(\Phi^{-1}(\overline{x}))}{\partial \overline{x}}^{\mathsf{T}} \overline{R}(\overline{x}, s) \frac{\partial H(\Phi^{-1}(\overline{x}))}{\partial \overline{x}}, \forall \{x, \delta\} \in X \times \Delta$

4. $H(\Phi^{-1}(\overline{x})) \leq \alpha, \forall x \in \text{Guard}(s, s')$

Proof. Assuming that the Hamiltonian function $H(x)$ satisfy the four conditions in Theorem 1, yet there exists a time $T \geq 0$, an input δ, and initial states $\text{Init}(s)$, and a trajectory $\Gamma(x(t), s(t))$ such that $\Gamma(x(T), s(T)) \in \text{Unsafe}(s)$. We show that the Hamiltonian function cannot simultaneously satisfy the four condition and reach the unsafe region, thus proving safety by contradiction. The time derivative of the Hamiltonian functions $\frac{dH}{dt}$ can be written as:

$$\begin{aligned}
\frac{\partial H(x)}{\partial x}^{\mathsf{T}} \dot{x} &= \frac{\partial H(x)}{\partial x}^{\mathsf{T}} [J(x, s) - R(x, s)] \frac{\partial H(x)}{\partial x} \\
&\quad + \frac{\partial H(x)}{\partial x}^{\mathsf{T}} L(x, s)\delta \\
&= \frac{\partial H(\Phi^{-1}(\overline{x}))}{\partial \overline{x}}^{\mathsf{T}} [\overline{J}(\overline{x}, s) - \overline{R}(\overline{x}, s)] \frac{\partial H(\Phi^{-1}(\overline{x}))}{\partial \overline{x}} \\
&\quad + \frac{\partial H(\Phi^{-1}(\overline{x}))}{\partial \overline{x}}^{\mathsf{T}} \overline{L}(\overline{x}, s)\delta \\
&= -\frac{\partial H(\Phi^{-1}(\overline{x}))}{\partial \overline{x}}^{\mathsf{T}} \overline{R}(\overline{x}, s) \frac{\partial H(\Phi^{-1}(\overline{x}))}{\partial \overline{x}} + \zeta\delta
\end{aligned}$$

$$\overline{J}(\overline{x}, s) = \frac{\partial \Phi}{\partial x} J(x, s) \frac{\partial \Phi}{\partial x}^{\mathsf{T}} \Bigg|_{x = \Phi^{-1}(\overline{x})}$$

$$\overline{R}(\overline{x}, s) = \frac{\partial \Phi}{\partial x} R(x, s) \frac{\partial \Phi}{\partial x}^{\mathsf{T}} \Bigg|_{x = \Phi^{-1}(\overline{x})}$$

$$\overline{L}(\overline{x}, s) = \frac{\partial \Phi}{\partial x} L(x, s) \Bigg|_{x = \Phi^{-1}(\overline{x})}$$

Condition (3) shows that the system trajectory on the time interval of $[0, T]$ is non-increasing, which indicates that $H(x(T)) \leq H(x(0))$. Additionally, condition (4) asserts that during a discrete transition, the Hamiltonian function will not jump to an increasing value. These statements, however, contradict the original assumption that the system states start at $\text{Init}(s)$ and end at $\text{Unsafe}(s)$. As a result, we can conclude that the system is safe. □

4. COLLISION AVOIDANCE

In this section, we consider the safety analysis of a vehicle with ACC following a lead car and maintaining a safe distance between the vehicles. The goal for the ACC is to prevent the host car from colliding into the lead car in the event of rapid deceleration. For simplicity, we consider the case shown in Figure 3 in which the vehicles are driving on a straight road, which allows us to omit the lateral dynamics.

4.1 Multi-Modal PHS

Figure 4 shows the multi-modal PHS of the longitudinal vehicle dynamics connected to the ACC system via power ports. Disturbances from wind and slope of the road are modeled as ports attached to the longitudinal vehicle dynamics. The longitudinal dynamics contain state variables of longitudinal momentum p_x and longitudinal displacement q_x and two control ports (T_a, y_1) and (T_b, y_2). The longitudinal input force from the throttle, T_a, is a function of the throttle valve angle θ_a, $T_a = C_a\theta_a$, where C_a is the experimental throttle constant. The longitudinal input force from the brakes, T_b, is a function of the braking pressure P_b, $T_b = C_bP_b$, where C_b is the experimental braking constant. The outputs of the control ports y_1 and y_2 are V_x and $-V_x$, respectively. The longitudinal dynamics contain two disturbance ports whose inputs, δ_g and δ_{wx} are the disturbance

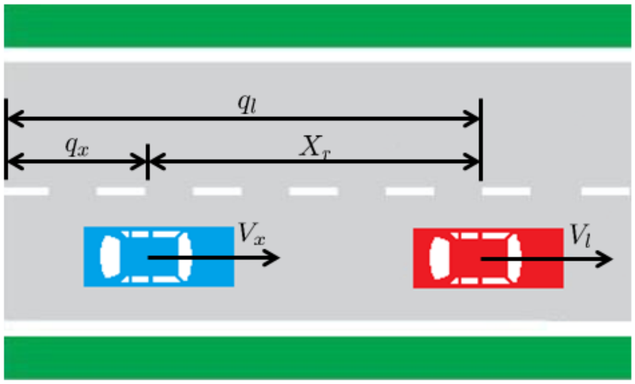

Figure 3: Lead vehicle and host vehicle on a straight road

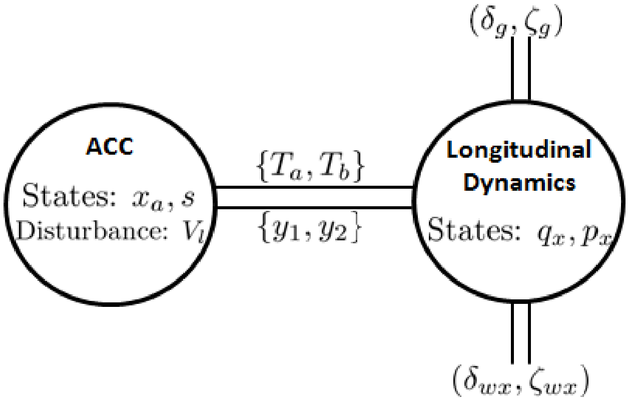

Figure 4: Longitudinal vehicle dynamics and ACC

forces resulting from the slope of the road and longitudinal wind, respectively. The outputs of the disturbance ports, ζ_g and ζ_{wx}, are the corresponding power conjugate values. The longitudinal dynamics has the following Hamiltonian function:

$$H_x(q_x, p_x) = \frac{1}{2m}p_x^2 + U_x(q_x),$$

where m represents the mass of the vehicle and $U_x(q_x)$ represents the potential energy. The longitudinal dynamics contain the continuous states $\{q_x, p_x\} \in X_k \subseteq \mathbb{R}^2$, initial states $X_{k0} \subseteq X_k$, inputs $\{T_a, T_b\}$, and disturbances $\{\delta_g, \delta_{wx}\}$.

$$\begin{cases} \begin{bmatrix} \dot{q}_x \\ \dot{p}_x \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ -1 & -R_x \end{bmatrix} \begin{bmatrix} \frac{\partial H_x}{\partial q_x} \\ \frac{\partial H_x}{\partial p_x} \end{bmatrix} + \begin{bmatrix} 0 \\ G_x \end{bmatrix} \begin{bmatrix} T_a \\ T_b \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \delta_g \\ \delta_{wx} \end{bmatrix} \\ \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} &= \begin{bmatrix} 0 & G_x^\mathsf{T} \end{bmatrix} \begin{bmatrix} \frac{\partial H_x}{\partial q_x} & \frac{\partial H_x}{\partial p_x} \end{bmatrix}^\mathsf{T} \\ \zeta_x &= \begin{bmatrix} 0 & L_x^\mathsf{T} \end{bmatrix} \begin{bmatrix} \frac{\partial H_x}{\partial q_x} & \frac{\partial H_x}{\partial p_x} \end{bmatrix} \end{cases} \tag{2}$$

where $G_x = \begin{bmatrix} 1 & -1 \end{bmatrix}$, $R_x = a + \frac{bp_x}{m} + \frac{cm}{p_x}$, a represents the tire rolling friction constant, b represents the air resistance constant, and c represents the static friction constant.

The ACC is connected to the longitudinal vehicle dynamics through the control ports and allows for autonomous driving by controlling T_a and T_b. The objective of the ACC is to maintain a desired speed depending on the lead vehicle velocity V_l, which is modeled as a disturbance. If a lead vehicle is not detected, the desired vehicle velocity is the driver's set speed which makes the system behave as a conventional cruise control system. Assuming that there is a lead vehicle, the host vehicle's radar system determines the speed of the lead vehicle. Figure 3 shows that the relative distance between the two vehicles is computed using the lead vehicle velocity, the host vehicle velocity, and the initial relative distance $X_r(0)$.

$$\begin{aligned} X_r(t) &= \int_0^t (V_l - V_x)d\tau + X_r(0) \\ &= \int_0^t \left(V_l(\tau) - \tfrac{1}{m}p_x(\tau)\right)d\tau + X_r(0). \end{aligned}$$

The state variables of the ACC are derived using the lead vehicle velocity and the desired relative distance $X_d = hV_l + S_0$, where h is the time headway and S_0 is the static distance constant. We compile the state variables into a vector $x_a = \begin{bmatrix} x_{at} & x_{ab} \end{bmatrix}^\mathsf{T}$, where $x_{at} = \int_0^t((1 + \gamma\frac{X_r - X_d}{X_d})V_l - V_x)d\tau$ and $x_{ab} = \int_0^t(V_x - (1 + \gamma\frac{X_r - X_d}{X_d})V_l)d\tau$ (γ is a constant).

The ACC has hybrid dynamics which is modeled using discrete variables s_t and s_b, where s_t is associated with the throttle control mode and s_b is associated with the brake control mode. The throttle control and brake control modes cannot be active simultaneously, which eliminates the case in which both s_t and s_b are active. We also make the assumption that the throttle control and brake control modes cannot be inactive simultaneously. The guards of the discrete transitions are defined in (3), where h_+ and h_- are hysteresis constants introduced to prevent the system from rapidly alternating between accelerating and decelerating:

$$\begin{cases} (s_t, s_b) = (1, 0) \text{ if } (1 + \gamma\frac{X_r - X_d}{X_d})V_l - V_x \geq 0, X_r \geq h_+ X_d \\ (s_t, s_b) = (0, 1) \text{ if } (1 + \gamma\frac{X_r - X_d}{X_d})V_l - V_x < 0, X_r < h_- X_d \end{cases} \tag{3}$$

We design the ACC to have the following Hamiltonian function:

$$H_a(x_a, s) = \frac{1}{2}(k_{ti}x_{at}^2 + k_{bi}x_{ab}^2),$$

where k_{ti} and k_{bi} are the gains of the Hamiltonian. The ACC system has continuous states $x_a \in X_a \subseteq \mathbb{R}^2$, discrete states $\{s_t, s_b\} \in S_a$, initial states $X_{a0} \times S_{a0} \subseteq X_a \times S_a$, and discrete transitions $\mathbb{T}_a \subseteq (X_a \times S_a) \to (X_a \times S_a)$. Its input-state-output PHS is described by:

$$\begin{cases} \dot{x}_a &= -R_a\frac{\partial H_a}{\partial x_a} + G_a u_a \\ y_a &= G_a^\mathsf{T}\frac{\partial H_a}{\partial x_a} + M_a u_a \end{cases} \tag{4}$$

where (u_a, y_a) are the input-output pairs corresponding to the control port. The parameter matrices are:

$$R_a = \begin{bmatrix} s_t k_t & 0 \\ 0 & s_b k_b \end{bmatrix}, G_a = \begin{bmatrix} s_t P & 0 \\ 0 & s_b \end{bmatrix},$$

$$M_a = \begin{bmatrix} s_t k_{td} & 0 \\ 0 & s_b k_{bd} \end{bmatrix}.$$

where k_t and k_{td} are throttle control gains, and k_b and k_{bd} are brake control gains. P is derived from the inverse engine map of the vehicle and is a mapping of the ratio of the acceleration force to V_x.

The standard feedback interconnection of the longitudinal vehicle dynamics with the ACC system is described using the power-conserving interconnection $u_x = -y_a$ and $y_x = u_a$.

The closed-loop system has a Hamiltonian function $H_k = H_a(x_a, s) + H_x(q_x, p_x)$, initial states $X_0 = X_{k0} \times X_{a0} \times S_{a0}$, discrete transitions $\mathbb{T}_k \subseteq (X \times S_a) \to (X \times S_a)$, and disturbances $\{\delta_g, \delta_{wx}\} \in \Delta_g \times \Delta_{wx}$. Its input-state-output PHS is described by:

$$\begin{cases} \begin{bmatrix} \dot{q}_x \\ \dot{p}_x \\ \dot{x}_{at} \\ \dot{x}_{ab} \end{bmatrix} = [\tilde{J}_x - \tilde{R}_x] \begin{bmatrix} \frac{\partial \tilde{H}_x}{\partial q_x} \\ \frac{\partial \tilde{H}_x}{\partial \hat{p}_x} \\ \frac{\partial \tilde{H}_x}{\partial x_{at}} \\ \frac{\partial \tilde{H}_x}{\partial x_{ab}} \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \delta_g \\ \delta_{wx} \end{bmatrix} \\ \begin{bmatrix} \zeta_g \\ \zeta_{wx} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \frac{\partial \tilde{H}_x}{\partial q_x} & \frac{\partial \tilde{H}_x}{\partial \hat{p}_x} & \frac{\partial \tilde{H}_x}{\partial x_{at}} & \frac{\partial \tilde{H}_x}{\partial x_{ab}} \end{bmatrix}^{\mathsf{T}} \end{cases} \tag{5}$$

$$\tilde{J}_x = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & -s_t P & s_b \\ 0 & s_t P & 0 & 0 \\ 0 & -s_b & 0 & 0 \end{bmatrix},$$

$$\tilde{R}_x = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & R_x + s_t k_{td} + s_b k_{bd} & 0 & 0 \\ 0 & 0 & s_t k_t & 0 \\ 0 & 0 & 0 & s_b k_b \end{bmatrix}.$$

4.2 Safety Problem

The control gains can be selected to stabilize the host vehicle velocity to $V_l + \gamma \frac{(X_r - X_d)V_l}{X_d}$ [4]. However, stability does not imply safety. We do not consider the scenario in which a lead vehicle appears in front of the host vehicle driving faster than or equal to the host vehicle set speed because the safety property is trivial since the controller stabilizes the host vehicle velocity to the set speed indicating that the relative distance between the two vehicles will not be less than the initial relative distance. We consider the scenario in which a lead vehicle appears in front of the host vehicle driving slower than the host vehicle set speed. In this scenario, the safety property needs to be validated because if the ACC does not react accordingly and slow the host vehicle to a reasonable speed, a collision may occur. The safety condition for the longitudinal dynamics asserts that the relative distance between the two vehicles will never reach a minimum distance q_m. We can represent the unsafe host vehicle displacement as the set of:

$$X_{ku} = \left\{ q_x \in \mathbb{R} : q_x \geq \int_0^t V_l d\tau + q_l(0) + q_m \right\}, \tag{6}$$

where $q_l(0)$ is the initial displacement value of the lead vehicle. Given (5), the safety condition for the longitudinal vehicle dynamics and ACC system states that that all possible trajectories cannot reach the unsafe region described by (6).

4.3 Safety Analysis

In order to show safety, we make some assumptions regarding the parameters of the lead and host vehicle. The first assumption is that the initial velocity of the lead vehicle is greater than a minimum velocity which depends on the deceleration of the lead vehicle (a_l) and the relative distance between the vehicles. The second assumption is that the initial relative distance between the vehicles is greater than a minimum distance which depends on the deceleration and velocity of the lead vehicle. If the initial velocity of the vehicle is high compared to the host vehicle velocity, then the initial relative displacement can be low because the host vehicle does not need a large distance to react to the lead vehicle velocity. However, if the initial velocity of the vehicle is low compared to the host vehicle velocity, then the initial relative displacement must be high because the host vehicle needs a larger distance to react to the low lead vehicle velocity. The relationship between the initial relative distance and the initial vehicle velocities is described in (7).

$$X_r(0) = \frac{V_l^2(0)}{2a_l} - \frac{V_x^2(0)}{2\dot{V}_x}. \tag{7}$$

We need the following definitions for initial states, unsafe states, and guard sets. For each discrete state $s_a \in S_a$, the initial continuous states are defined as $\text{Init}(s_a) = \{ (q_x, p_x, x_a) \in X : (q_x, p_x, x_a, s_a) \in X_0 \}$ and the unsafe continuous states are defined as $\text{Unsafe}(s_a) = \{ (q_x, p_x, x_a) \in X : q_x \in X_{ku} \}$. Each transition of discrete states from $s_a \in S_a$ to $s_a' \in S_a$ is defined using the guard condition Guard $(s_a, s_a') = \{ (q_x, p_x, x_a), (q_x, p_x, x_a)' \in X : (q_x, p_x, x_a, s_a) \to (q_x', p_x', x_a', s_a') \}$. Safety analysis of the longitudinal dynamics uses $\overline{p}_x = \Phi(p_x) = p_x - m(1 + \gamma \frac{X_r - X_d}{X_d})V_l$ as the canonical coordinate transformation on the longitudinal momentum.

We apply Theorem 1 to the composed longitudinal dynamics and ACC system. Given initial conditions $\text{Init}(s_a)$, we derive the energy bound α as a function of the initial host vehicle velocity $V_x(0)$, initial relative distance $X_r(0)$, and initial lead vehicle velocity $V_l(0)$. The initial relative distance must be greater than or equal to $\frac{V_l^2(0)}{2a_l} - \frac{V_x^2(0)}{2a_l}$ where a_l is the bounded lead vehicle deceleration. Consequently, we restate the first condition of Theorem 1 as $H_k(\Phi^{-1}(\overline{p}_x)) \leq \alpha, \forall x \in \text{Init}(s_a)$, where

$$\alpha = m \frac{k_{td} + k_{bd}}{2} (V_x(0) - (1 + \gamma \frac{X_r(0) - hV_l(0) - S_0}{hV_l(0) + S_0}) V_l(0))^2.$$

Given the unsafe states $\text{Unsafe}(s_a)$, we derive the energy bound β as a function of host vehicle velocity V_x and lead vehicle velocity V_l. The energy of the transformed Hamiltonian function has a maximum value which indicates that the minimum relative distance has been reached. Consequently, we restate the second condition of Theorem 1 as $H_k(\Phi^{-1}(\overline{p}_x)) > \beta, \forall x \in \text{Unsafe}(s_a)$, where

$$\beta = m \frac{k_{td} + k_{bd}}{2} (V_x - (1 - \gamma) V_l)^2.$$

Given an initial relative distance greater than q_m, α is less than β, which validates the first two conditions. Given the disturbances $\{\delta_g, \delta_{wx}\} \in \Delta$, we must guarantee that the system trajectory will never begin in $\text{Init}(s_a)$ and end in $\text{Unsafe}(s_a)$. Consequently, we restate the third condition of Theorem 1 as

$$\zeta_g \delta_g + \zeta_{wx} \delta_{wx} \leq$$

$$\frac{\partial H_k(\Phi^{-1}(\overline{p}_x))}{\partial \overline{p}_x}^{\mathsf{T}} \frac{\partial \Phi}{\partial p_x} R_x(\Phi^{-1}(\overline{p}_x)) \frac{\partial \Phi}{\partial p_x}^{\mathsf{T}} \frac{\partial H_k(\Phi^{-1}(\overline{p}_x))}{\partial \overline{p}_x}$$

$$\forall (q_x, p_x, x_a, \delta_g, \delta_{wx}) \in X \times \Delta.$$

Discrete transitions between the throttle and brake control mode must also be taken into account in order to guarantee that the system will not transition into Unsafe(s_a). We restate the fourth condition of Theorem 1 as $H_k(\Phi^{-1}(\overline{p}_x)) \leq \alpha$, $\forall (q_x, p_x, x_a) \in \text{Guard}(s_t, s_b)$. In Section 6, the ACC is designed by selecting control parameters that satisfy these safety conditions.

5. SKIDDING AVOIDANCE

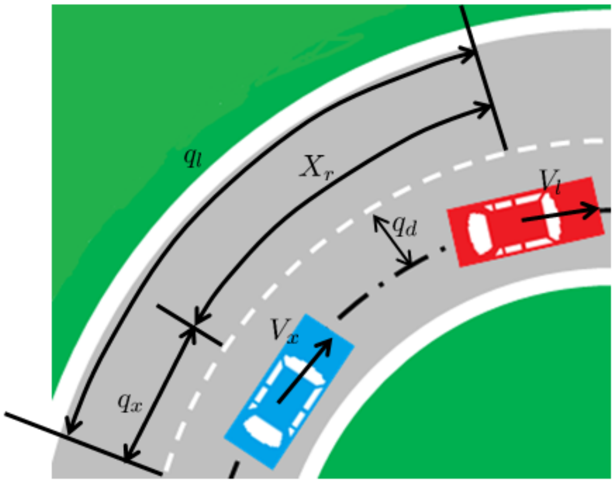

Figure 5: Diagram of lead vehicle and host vehicle on a curved road

In this section, we consider the safety problem of a vehicle with both ACC and LKC following a lead car around a curved road (Figure 5). In addition to maintaining a safe distance between the vehicles, the host car must also maintain a lateral acceleration as to not skid off the road. Interactions between the lateral and longitudinal dynamics, which can be characterized as an interaction structure, contribute to the lateral acceleration.

5.1 Multi-Modal PHS

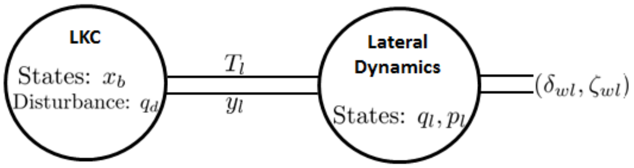

Figure 6: Lateral vehicle dynamics and LKC

Figure 6 shows the multi-modal PHS of the lateral vehicle dynamics connected to the LKC system via power ports. Disturbance from wind is modeled as a port attached to the lateral vehicle dynamics. The lateral dynamics contain state variables $q_l = \begin{bmatrix} q_y & q_r \end{bmatrix}^\mathsf{T}$ and $p_l = \begin{bmatrix} p_y & p_r \end{bmatrix}^\mathsf{T}$, where p_y is the lateral momentum, p_r is the angular momentum, q_y is the lateral displacement, and q_r is the angular displacement. The lateral dynamics contain a control port (T_l, y_l), where the output of the control port y_l is $V_y + l_f r$ (l_f represents the length of the vehicle center to the front wheels). The lateral input force from the steering, T_l, is a function of the steering angle θ_s, $T_l = 2C_f\theta_s$, where C_f is the cornering stiffness of the front wheels. The lateral dynamics contains a disturbance port whose input, δ_{wy}, represents a disturbance force resulting from lateral wind. The output of the disturbance ports, ζ_{wy}, is the corresponding power conjugate value. The lateral velocity, and yaw rate, are represented by V_x, V_y, and r, respectively. The lateral dynamics has the following Hamiltonian function:

$$H_l(q_y, q_r, p_y, p_r) = \frac{1}{2m}p_y^2 + \frac{1}{2I}p_r^2 + U_l(q_y, q_r),$$

where I represents the moment of inertia of the vehicle and $U_l(q_y, q_r)$ represents the potential energy. The lateral dynamics contain the continuous states $\{q_l, p_l\} \in X_l \subseteq \mathbb{R}^4$, initial states $X_{l0} \subseteq X_l$, input T_l, and disturbance δ_{wy}.

$$\begin{cases} \begin{bmatrix} \dot{q}_l \\ \dot{p}_l \end{bmatrix} = \begin{bmatrix} 0 & I \\ -I & -R_l \end{bmatrix} \begin{bmatrix} \frac{\partial H_l}{\partial q_l} \\ \frac{\partial H_l}{\partial p_l} \end{bmatrix} + \begin{bmatrix} 0 \\ G_l \end{bmatrix} T_l + \begin{bmatrix} 0 \\ L_l \end{bmatrix} \delta_{wl} \\ y_l = \begin{bmatrix} 0 & G_l^\mathsf{T} \end{bmatrix} \begin{bmatrix} \frac{\partial H_l}{\partial q_l} & \frac{\partial H_l}{\partial p_l} \end{bmatrix}^\mathsf{T} \\ \zeta_{wl} = \begin{bmatrix} 0 & L_l^\mathsf{T} \end{bmatrix} \begin{bmatrix} \frac{\partial H_l}{\partial q_l} & \frac{\partial H_l}{\partial p_l} \end{bmatrix}^\mathsf{T} \end{cases} \tag{8}$$

$$R_l = \begin{bmatrix} \frac{W_1}{V_x} & \frac{W_2}{V_x} \\ \frac{W_2}{V_x} & \frac{W_3}{V_x} \end{bmatrix},$$

where $G_l = \begin{bmatrix} 1 & l_f \end{bmatrix}^\mathsf{T}$ and $L_l = \begin{bmatrix} 1 & 0 \end{bmatrix}^\mathsf{T}$. The parameter constants of R_l are $W_1 = 2C_f + 2C_r$, $W_2 = 2C_f l_f - 2C_r l_r$, and $W_3 = 2C_f l_f^2 + 2C_r l_r^2$, where C_r is the cornering stiffness of the rear wheels, l_f is the length of the vehicle center to the front wheels, and l_r is the length of the vehicle center to the rear wheels.

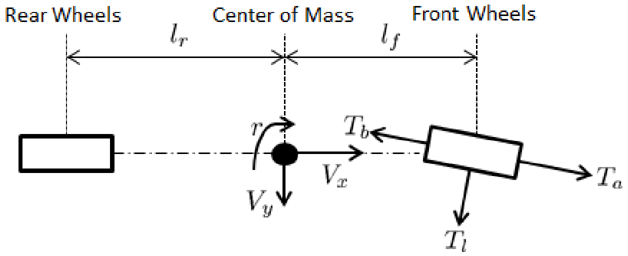

Figure 7: Free-body diagram of the vehicle dynamics

Interactions between the longitudinal and lateral dynamics are a result of the vehicle heading angle being affected by longitudinal velocity and can be derived by analysis of the free-body diagram in Figure 7 [15]. The x-component of the lateral force affecting the longitudinal motion is represented by d_x and its power-conjugate velocity is represented by z_x. The y-component of the longitudinal force affecting the lateral motion is represented by d_l and its power-conjugate velocity is represented by z_l.

Figure 8 shows a diagram of the interacting vehicle dynamics and the two control systems. The altered equations (2) and (8), which include the interaction ports (d_x, z_x) and

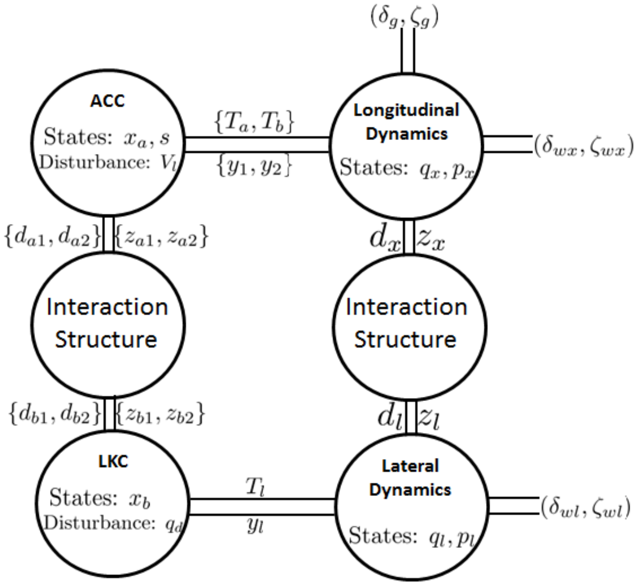

Figure 8: Closed-loop system

(d_l, z_l), are described by:

$$\left\{\begin{aligned} \begin{bmatrix}\dot{q}_x\\ \dot{p}_x\end{bmatrix} &= \begin{bmatrix}0 & 1\\ -1 & -R_x\end{bmatrix}\begin{bmatrix}\frac{\partial H_x}{\partial q_x}\\ \frac{\partial H_x}{\partial p_x}\end{bmatrix} + \begin{bmatrix}0\\ G_x\end{bmatrix} u_x + \begin{bmatrix}0\\ 1\end{bmatrix} d_x \\ &\quad + \begin{bmatrix}\delta_g\\ \delta_{wx}\end{bmatrix} \\ y_x &= \begin{bmatrix}0 & G_x^{\mathsf{T}}\end{bmatrix}\begin{bmatrix}\frac{\partial H_x}{\partial q_x} & \frac{\partial H_x}{\partial p_x}\end{bmatrix}^{\mathsf{T}} \\ z_x &= \begin{bmatrix}0 & 1\end{bmatrix}\begin{bmatrix}\frac{\partial H_x}{\partial q_x} & \frac{\partial H_x}{\partial p_x}\end{bmatrix}^{\mathsf{T}} \\ \begin{bmatrix}\zeta_g\\ \zeta_{wx}\end{bmatrix} &= \begin{bmatrix}0 & L_x^{\mathsf{T}}\end{bmatrix}\begin{bmatrix}\frac{\partial H_x}{\partial q_x} & \frac{\partial H_x}{\partial p_x}\end{bmatrix}^{\mathsf{T}} \end{aligned}\right. \tag{9}$$

$$\left\{\begin{aligned} \begin{bmatrix}\dot{q}_l\\ \dot{p}_l\end{bmatrix} &= \begin{bmatrix}0 & I\\ -I & -R_l\end{bmatrix}\begin{bmatrix}\frac{\partial H_l}{\partial q_l}\\ \frac{\partial H_l}{\partial p_l}\end{bmatrix} + \begin{bmatrix}0\\ G_l\end{bmatrix} T_l + \begin{bmatrix}0\\ K_l\end{bmatrix} d_l \\ &\quad + \begin{bmatrix}0\\ L_l\end{bmatrix} \delta_{wl} \\ y_l &= \begin{bmatrix}0 & G_l^{\mathsf{T}}\end{bmatrix}\begin{bmatrix}\frac{\partial H_l}{\partial q_l} & \frac{\partial H_l}{\partial p_l}\end{bmatrix}^{\mathsf{T}} \\ z_l &= \begin{bmatrix}0 & K_l^{\mathsf{T}}\end{bmatrix}\begin{bmatrix}\frac{\partial H_l}{\partial q_l} & \frac{\partial H_l}{\partial p_l}\end{bmatrix}^{\mathsf{T}} \\ \zeta_{wl} &= \begin{bmatrix}0 & L_l^{\mathsf{T}}\end{bmatrix}\begin{bmatrix}\frac{\partial H_l}{\partial q_l} & \frac{\partial H_l}{\partial p_l}\end{bmatrix}^{\mathsf{T}} \end{aligned}\right. \tag{10}$$

where $K_l = \begin{bmatrix}1 & 0\end{bmatrix}^{\mathsf{T}}$. The interaction between the longitudinal and lateral dynamics is a mapping of velocity to force, which indicates a gyrator relationship. The gyrator ratio has units of kg/s which is represented by multiplying the mass of the vehicle with the yaw rate. The interaction structure is modeled as a Dirac structure modulated by the yaw momentum p_r:

$$\begin{bmatrix}d_x\\ d_l\end{bmatrix} = \begin{bmatrix}0 & -\frac{mp_r}{I}\\ \frac{mp_r}{I} & 0\end{bmatrix}\begin{bmatrix}z_x\\ z_l\end{bmatrix}. \tag{11}$$

The LKC connects with the lateral vehicle dynamics via the control ports and allows for autonomous driving by controlling T_l. The objective of the LKC is to maintain a desired lateral displacement q_d. The control system consists of ACC, LKC, and an interaction structure. The LKC shares the control port with the lateral dynamics and its state variable $x_b = q_y - q_d$ is derived using the desired lateral displacement. We design the LKC to have the following Hamiltonian function:

$$H_b(x_b) = \frac{1}{2} k_{si} x_b^2,$$

where k_{si} is the gain associated with the integrator. The LKC system has continuous states $x_b \in X_b \subseteq \mathbb{R}$ and initial states X_{b0}, with dynamic equations as an input-state-output PHS with direct-feedthrough:

$$\left\{\begin{aligned} \dot{x}_b &= u_b \\ y_b &= \frac{\partial H_b}{\partial x_b} + k_{sd} u_b, \end{aligned}\right. \tag{12}$$

where (u_b, y_b) are the input-output pairs corresponding to the control port and k_{sd} is the gain associated with the steering control. We connect the ACC and LKC using an interaction structure, which alters (4) and (12), so that the state variables and outputs of the speed control are affected by the state variable of the steering control, and vice versa. The purpose of the interaction structure is to lower the speed of the vehicle in the event of a turn by transferring energy from the ACC to the LKC.

$$\left\{\begin{aligned} \dot{x}_a &= -R_a \frac{\partial H_a}{\partial x_a} + G_a y_x + K_{a1} d_{a1} \\ u_x &= G_a^{\mathsf{T}} \frac{\partial H_a}{\partial x_a} + M_a y_x + K_{a2} d_{a2} \\ \begin{bmatrix}z_{a1}\\ z_{a2}\end{bmatrix} &= \begin{bmatrix}K_{a1}^{\mathsf{T}} & 0\\ 0 & K_{a2}^{\mathsf{T}}\end{bmatrix}\begin{bmatrix}\frac{\partial H_a}{\partial x_a}\\ y_x\end{bmatrix} \end{aligned}\right. \tag{13}$$

$$\left\{\begin{aligned} \dot{x}_b &= y_l + d_{b1} \\ T_l &= \frac{\partial H_b}{\partial x_b} + k_{sd} y_l + d_{b2} \\ \begin{bmatrix}z_{b1}\\ z_{b2}\end{bmatrix} &= \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}\frac{\partial H_b}{\partial x_b}\\ y_l\end{bmatrix} \end{aligned}\right. \tag{14}$$

The interaction structure of the control system is represented by the following Dirac structure:

$$\begin{bmatrix}d_{a1}\\ d_{a2}\\ d_{b1}\\ d_{b2}\end{bmatrix} = \begin{bmatrix}0 & 0 & J_c & 0\\ 0 & 0 & 0 & M_c\\ -J_c^{\mathsf{T}} & 0 & 0 & 0\\ 0 & -M_c^{\mathsf{T}} & 0 & 0\end{bmatrix}\begin{bmatrix}z_{a1}\\ z_{a2}\\ z_{b1}\\ z_{b2}\end{bmatrix}. \tag{15}$$

The parameters J_c and M_c define how the speed control and the steering control interact. In order to derive the closed-loop system, we define the variables $q = \begin{bmatrix}q_x & q_l\end{bmatrix}^{\mathsf{T}}$, $p = \begin{bmatrix}p_x & p_l\end{bmatrix}^{\mathsf{T}}$, $x = \begin{bmatrix}x_{at} & x_{ab} & x_b\end{bmatrix}^{\mathsf{T}}$, $\delta = \begin{bmatrix}\delta_g & \delta_{wx} & \delta_l\end{bmatrix}^{\mathsf{T}}$, and $\zeta = \begin{bmatrix}\zeta_g & \zeta_{wx} & \zeta_l\end{bmatrix}^{\mathsf{T}}$. The closed-loop system has a Hamiltonian function $\tilde{H}(q, p, z) = H_x + H_l + H_a + H_b$, continuous states $\{q, p, x\} \in \tilde{X}$, initial states $\tilde{X}_0 = \tilde{X}_{p0} \times \tilde{X}_{c0} \times S_a$, discrete transitions $\tilde{\mathbb{T}} \subseteq (\tilde{X} \times S_a) \to (\tilde{X} \times S_a)$, and disturbances $\delta = \{\delta_g, \delta_{wx}, \delta_{wy}\} \in \Delta_g \times \Delta_{wx} \times \Delta_{wy}$.

$$\left\{\begin{aligned} \begin{bmatrix}\dot{q}\\ \dot{p}\\ \dot{x}\end{bmatrix} &= \begin{bmatrix}0 & I & 0\\ -I & \tilde{J} - \tilde{R} & \tilde{K}\\ 0 & -\tilde{K}^{\mathsf{T}} & -\tilde{Q}\end{bmatrix}\begin{bmatrix}\frac{\partial \tilde{H}}{\partial q}\\ \frac{\partial \tilde{H}}{\partial p}\\ \frac{\partial \tilde{H}}{\partial x}\end{bmatrix} + \begin{bmatrix}0\\ \tilde{L}\\ 0\end{bmatrix} \delta \\ \zeta &= \begin{bmatrix}0 & \tilde{L} & 0\end{bmatrix}\begin{bmatrix}\frac{\partial \tilde{H}}{\partial q} & \frac{\partial \tilde{H}}{\partial p} & \frac{\partial \tilde{H}}{\partial x}\end{bmatrix}^{\mathsf{T}} \end{aligned}\right. \tag{16}$$

where $\tilde{J}$, $\tilde{L}$, $\tilde{R}$, $\tilde{K}$, and $\tilde{Q}$ are defined as:

$$\tilde{J} = \begin{bmatrix} 0 & \frac{mp_r}{I} - M_c & -l_f M_c \\ -\frac{mp_r}{I} + M_c & 0 & 0 \\ l_f M_c & 0 & 0 \end{bmatrix}, \tilde{L} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

$$\tilde{R} = \begin{bmatrix} R_x + s_t k_{td} + s_b k_{bd} & 0 & 0 \\ 0 & \frac{mW_1}{p_x} + k_{sd} & \frac{mW_2}{p_x} + l_f k_{sd} \\ 0 & \frac{mW_2}{p_x} + l_f k_{sd} & \frac{mW_3}{p_x} + l_f^2 k_{sd} \end{bmatrix},$$

$$\tilde{K} = \begin{bmatrix} s_t P & s_b & 0 \\ 0 & 0 & -1 \\ 0 & 0 & -l_f \end{bmatrix}, \tilde{Q} = \begin{bmatrix} s_t k_t & 0 & -J_c \\ 0 & s_b k_b & 0 \\ J_c & 0 & 0 \end{bmatrix}.$$

5.2 Safety Problem

The control gains can be selected to stabilize the host vehicle velocity to $V_l + \gamma\frac{(X_r - X_d)V_l}{X_d}$ and the lateral displacement to q_d [4]. However, stability does not imply safety. The unsafe states for the lateral momentum are related to that of the longitudinal momentum because of the interactions between the longitudinal and lateral dynamics. The inputs to the longitudinal dynamics (T_a and T_b) affect the lateral dynamics. Similarly, the input to the lateral dynamics (T_l) affects the longitudinal dynamics. This introduces an additional safety constraint on the system. In order for the vehicle to operate safely on the road, its lateral acceleration must not exceed a maximum value A_m. If the lateral acceleration exceeds A_m, the vehicle will skid. This lateral acceleration value of the vehicle is affected by the yaw rate and longitudinal velocity of the vehicle. This interaction between lateral and longitudinal motion results in an unsafe region characterized by a set defined as:

$$X_{lu} = \{p_x \in \mathbb{R}, p_r \in \mathbb{R} : p_x p_r \geq m^2 I A_m\}. \qquad (17)$$

This safety condition indicates that longitudinal and lateral motion are bounded by a hyperbolic relationship. A large longitudinal momentum results in a lower bound for the lateral and yaw momentum, and a large lateral and yaw momentum results in a lower bound for the longitudinal momentum. Using this safety constraint we must verify that the product of longitudinal momentum and yaw rate does not exceed a maximum threshold. Given (16) and $\tilde{H}(q, p, z)$, the safety condition for the vehicle dynamics, ACC system, and LKC system states that that all possible trajectories cannot reach the unsafe region described by (6) and (17).

5.3 Safety Analysis

A road can be divided into segments consisting of four types of road profiles: straight road, decreasing curvature, constant curvature, and increasing curvature. Of the four cases the lateral acceleration safety problem is trivial for the straight road and decreasing curvature cases. A straight road nullifies the unsafe state set X_{lu} and a decreasing road curvature relaxes the safety condition. In order to safely navigate a curved section of the road, the vehicle must avoid the unsafe regions of X_{ku} and X_{lu}. Given a road curvature of ρ, the yaw momentum required is calculated as $p_r = \frac{Ip_x}{m}\rho$, which shows the direct relationship between the yaw momentum and the longitudinal momentum. Additionally, the road curvature is related to the vehicle slip angle ω and steering angle θ_s:

$$\rho = \frac{\cos(\omega)\tan(\theta_s)}{l_f + l_r},$$

$$\omega = \arctan(\frac{l_r}{l_f + l_r}\tan(\theta_s)).$$

The lateral momentum depends on the longitudinal momentum, the yaw momentum, and the vehicle slip angle:

$$p_y = p_x \sin(\frac{p_r}{I} + \omega).$$

Given that ω and p_r are directly proportional to ρ, we can represent the state variable p_y as a function directly proportional to p_x and ρ. We need the following definitions for initial states, unsafe states, and guard sets. For each discrete state $s_a \in S_a$, the initial continuous states are defined as $\overline{\mathrm{Init}}(s_a) = \{(q, p, x) \in \tilde{X} : (q, p, x, s_a) \in \tilde{X}_0\}$ and the unsafe continuous states are defined as $\overline{\mathrm{Unsafe}}(s_a) = \{(q, p, x) \in \tilde{X} : (q_x, p_x, p_r) \in X_{ku} \times X_{lu}$. Each transition of discrete states from $s_a \in S_a$ to $s'_a \in S_a$ is associated with the guard set $\overline{\mathrm{Guard}}(s_a, s'_a) = \{(q, p, x), (q, p, x)' \in \tilde{X} : (q, p, x, s_a) \to (q', p', x', s'_a)\}$. Safety analysis of the vehicle dynamics uses $\tilde{\Phi}$ as the canonical coordinate transformation for the momentum variables.

$$\begin{bmatrix} \overline{p}_x \\ \overline{p}_y \\ \overline{p}_r \end{bmatrix} = \begin{bmatrix} \tilde{\Phi}_x(p_x) \\ \tilde{\Phi}_y(p_y) \\ \tilde{\Phi}_r(p_r) \end{bmatrix} = \begin{bmatrix} p_x - m(1 + \gamma\frac{X_r - X_d}{X_d})V_l - M_c x_b \\ p_y + k_{si}(q_y - q_d) + M_c(x_{at} + x_{ab}) \\ p_r + k_{si}(q_r - \frac{q_d}{l_f}) + M_c\frac{x_{at} + x_{ab}}{l_f} \end{bmatrix}.$$

We apply Theorem 1 to the composed longitudinal dynamics, lateral dynamics, ACC, and LKC system. Given initial conditions $\overline{\mathrm{Init}}(s_a)$, we derive the energy bound $\tilde{\alpha}$ as a function of the initial host vehicle velocity $V_x(0)$, initial relative distance $X_r(0)$, initial lead vehicle velocity $V_l(0)$, and initial road curvature $\rho(0)$. Consequently, we restate the first condition of Theorem 1 as $\tilde{H}(\tilde{\Phi}^{-1}(\overline{p})) \leq \tilde{\alpha}, \forall(q, p, x) \in \overline{\mathrm{Init}}(s_a)$, where

$$\begin{aligned} \tilde{\alpha} \ &= \ m\tfrac{k_{td} + k_{bd}}{2}(V_x(0) - (1 + \gamma\tfrac{X_r(0) - hV_l(0) - S_0}{hV_l(0) + S_0})V_l(0))^2 \\ &\quad + \tfrac{m}{2}V_x^2(0)\sin^2(\rho(0)V_x(0) + \omega(0)) + \tfrac{I}{2}\rho^2(0)V_x^2(0). \end{aligned}$$

Given the unsafe states $\overline{\mathrm{Unsafe}}(s_a)$, we derive the energy bound $\tilde{\beta}$ as a function of host vehicle velocity V_x, relative distance X_r, lead vehicle velocity V_l, and road curvature ρ. The energy of the transformed Hamiltonian function has a maximum value which indicates that the maximum lateral acceleration has been reached. Consequently, we restate the second condition of Theorem 1 as $\tilde{H}(\tilde{\Phi}^{-1}(\overline{p})) > \tilde{\beta}, \forall(q, p, x) \in \overline{\mathrm{Unsafe}}(s_a)$, where

$$\begin{aligned} \tilde{\beta} \ &= \ m\tfrac{k_{td} + k_{bd}}{2}(V_x - (1 - \gamma)V_l - \tfrac{M_c}{m}(q_y - q_d))^2 \\ &\quad + \tfrac{m}{2}(V_x \sin(\rho V_x + \omega) + k_{si}(q_y - q_d))^2 \\ &\quad + \tfrac{I}{2}(\rho V_x + k_{si}(q_y - \tfrac{q_d}{l_f}))^2. \end{aligned}$$

Given the disturbances $\{\delta_g, \delta_{wx}, \delta_{wy}\} \in \Delta$, we must guarantee that the system trajectory will never begin in $\overline{\mathrm{Init}}(s_a)$ and end in $\overline{\mathrm{Unsafe}}(s_a)$. Consequently, we restate the third condition of Theorem 1 as

$$\zeta_g \delta_g + \zeta_{wx}\delta_{wx} + \zeta_{wy}\delta_{wy} \leq$$

$$\frac{\partial\tilde{H}(\tilde{\Phi}^{-1}(\overline{p}))}{\partial(q, \overline{p})}^{\mathsf{T}} \frac{\partial\tilde{\Phi}}{\partial p}\tilde{R}(\tilde{\Phi}^{-1}(\overline{p}))\frac{\partial\tilde{\Phi}}{\partial p}^{\mathsf{T}} \frac{\partial\tilde{H}(\tilde{\Phi}^{-1}(\overline{p}))}{\partial(q, \overline{p})},$$

$$\forall(q,p,x,\delta_g,\delta_{wx},\delta_{wy}) \in \tilde{X} \times \tilde{\Delta}.$$

Discrete transitions between throttle and brake control mode must also be taken into account in order to guarantee that the system will not transition into $\overline{\text{Unsafe}}(s_a)$. Consequently, we restate the fourth condition of Theorem 1 as $\tilde{H}(\tilde{\Phi}^{-1}(\overline{p})) \leq \tilde{\alpha}, \forall(q,p,x) \in \overline{\text{Guard}}(s_t,s_b) \cup \overline{\text{Guard}}(s_b,s_t)$. In Section 6, the ACC and LKC are designed by selecting control parameters that satisfy these safety conditions.

6. SIMULATION RESULTS

In this section, we present simulation results to illustrate the approach. For validation of the PHS model we use a standard E-class sedan model in CarSim as a reference [2]. We select parameters for the vehicle dynamics so that its passivity index values match that of the CarSim model [19]. We determine that the parameters of the vehicle dynamics are $a = 0.1$ s^{-1}, $b = 0.06$ m^{-1}, $c = 10$ m/s^2, $C_f = 300$ N, $l_f = 1.4$ m, $C_r = 200$ N, $l_r = 1.4$ m, $m = 1650$ kg, and $I = 3234$ kg m^2 [4]. The inverse engine map of the vehicle, P, can be found in [6]. We then use the vehicle dynamics parameters along with the safety conditions to choose control parameters (Table 1) so that the vehicle dynamics will not reach the unsafe regions (6) and (17). The safety conditions derived in Sections 4 and 5 are valid for vehicle velocities given a maximum road decline angle of 15 degrees which corresponds to $\delta_g = 4200$ N and a maximum lead vehicle deceleration of 5 m/s^2 which corresponds to a braking distance of 50 m from 80 km/hr to 0 km/hr.

Table 1: Table of controller gains

k_{ti}	k_{bi}	k_t	k_{td}	k_b
0.05	0.01	0.1	0.02	0.2
k_{bd}	k_{si}	k_{sd}	J_c	M_c
0.02	40	15	0.2	0.5

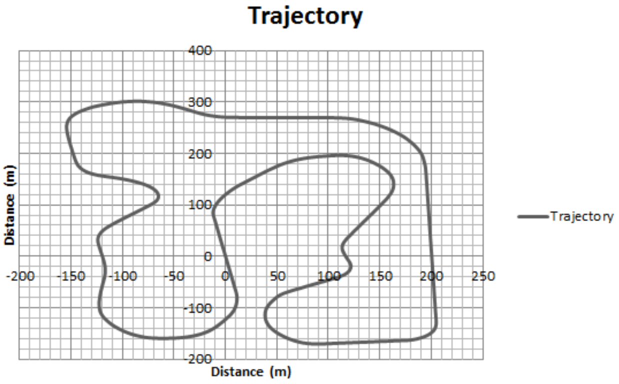

Figure 9: Road trajectory

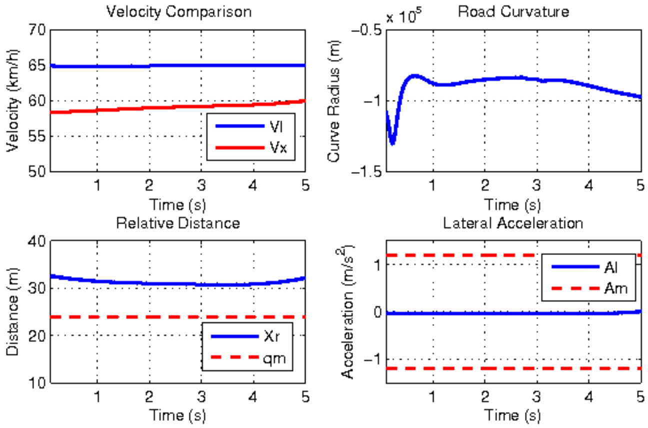

Figure 10: Zero degree decline and straight road

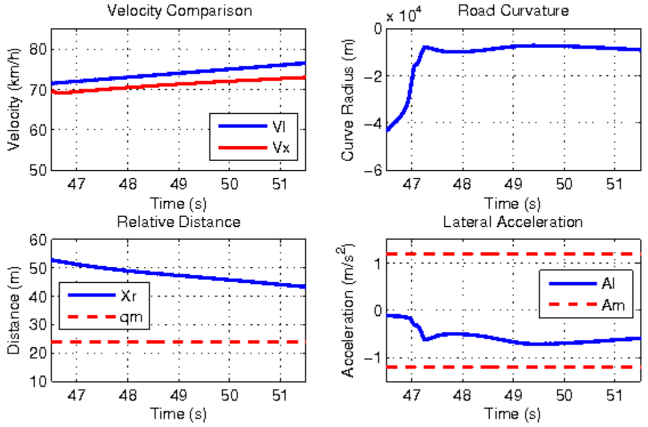

Figure 11: Zero degree decline and curved road

Simulation of the closed-loop system consists of two minutes of running time in which the host vehicle follows a lead vehicle on the road featured in Figure 9. Figure 10 shows the time range of 0 to 5 s, which is a straight segment of the road with a zero degree decline. The simulation results show that the system is safe since the relative distance is greater than $q_m = 24$ m. The curve radius is large because the road is relatively straight, so the lateral acceleration is near zero. Figure 11 shows the time range of 46.5 to 51.5 s, which is a curved segment of the road with a zero degree decline. The curve radius during this time period decreases, which corresponds to a non-zero lateral acceleration value. Safety is ensured because the lateral acceleration is bounded by $A_m = 1.2$ m/s^2.

Figure 12 shows the time range of 54 to 58 s, which is a straight segment of the road with a fifteen degree decline. The control parameters of the ACC system are designed to compensate for disturbances such as road decline, and the system is safe since the relative distance is greater than q_m. Similar to the time range of 0 to 5 s, the curve radius is large because the road is relatively straight, so the lateral acceleration is near zero. Figure 13 shows the time range of 70 to 75 s, which is a curved segment of the road with a fifteen degree decline. The simulation results show that safety conditions are satisfied.

7. CONCLUSION

The approach in this paper addresses the safety problem for multi-modal PHS given complex interactions, nonlinearities, and hybrid dynamics. The approach ensures the safety of the system by characterizing safe and unsafe regions using

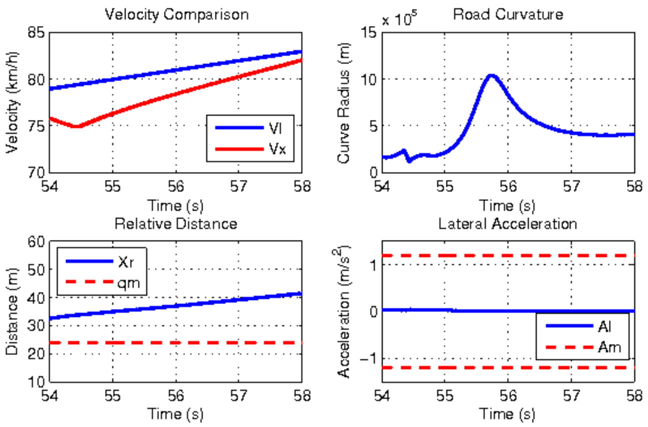

Figure 12: Fifteen degree decline and straight road

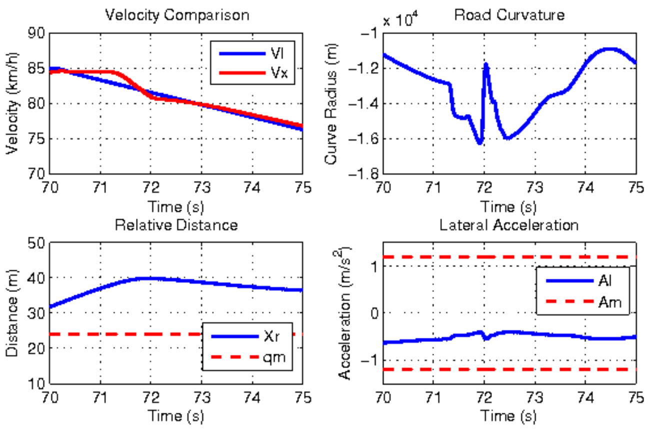

Figure 13: Fifteen degree decline and curved road

energy levels of the Hamiltonian function and deriving conditions on model and control parameters. We demonstrate the approach by analyzing the safety conditions of an automotive control system to prevent collision and skidding. Simulation results from an automotive control system are recorded and show the effectiveness of the safety analysis approach.

ACKNOWLEDGEMENT

This work is supported in part by the National Science Foundation (CNS-1035655).

8. REFERENCES

[1] A. Ames, J. Grizzle, and P. Tabuada. Control barrier function based quadratic programs with application to adaptive cruise control. In *Proceedings of the 53rd IEEE Conference of Decision and Control*, Los Angeles, CA, USA, December 2014.

[2] CarSim. *http://www.carsim.com*. Mechanical Simulation Corporation, Ann Arbor, MI, USA, 2013.

[3] J. Cervera, A. van der Schaft, and A. Banos. Interconnection of port-hamiltonian systems and composition of dirac structures. *Automatica*, 43(2), February 2007.

[4] S. Dai and X. Koutsoukos. Model-based automotive control design using port-hamiltonian systems. In *International Conference on Complex Systems Engineering*, Storrs, CT, USA, November 2015.

[5] V. Duindam, A. Macchelli, S. Stramigioli, and H. Bruyninckx. *Modeling and Control of Complex Physical Systems: The Port-Hamiltonian Approach*. Springer, New York, NY, 2009.

[6] E. Eyisi, Z. Zhang, X. Koutsoukos, J. Porter, G. Karsai, and J. Sztipanovits. Model-based control design and integration of cyberphysical system: An adaptive cruise control case study. *Journal of Control Science and Engineering, Special Issue on Embedded Model-Based Control*, 2013.

[7] K. Fujimoto and T. Sugie. Canonical transformation and stabilization of generalized hamiltonian systems. *Systems and Control Letters*, 42:217–227, 2001.

[8] H. Khalil. *Nonlinear Systems, 3rd Edition*. Prentice Hall, Upper Saddle River, NJ, 2002.

[9] MATLAB. *Version R2012a, http://www.mathworks.com*. The Mathworks, Inc., Natick, MA, USA, 2012.

[10] S. Prajna. Barrier certificates for nonlinear model validation. *Automatica*, 42:117–126, 2006.

[11] S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *Hybrid Systems Computation and Control*, pages 477–492, Philadelphia, PA, USA, 2004. Springer-Verlag.

[12] S. Prajna, A. Jadbabaie, and G. Pappas. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8):1415–1428, August 2007.

[13] S. Prajna, A. Papachristodoulou, and P. Parrilo. Introducing sostools: A general purpose sum of squares programming solver. In *Proceedings of the IEEE Conference on Decision and Control*, Las Vegas, NV, USA, 2002.

[14] S. Prajna and A. Rantzer. Primal-dual tests for safety and reachability. In *Hybrid Systems Computation and Control*, pages 542–556, Zurich, Switzerland, 2005. Springer-Verlag.

[15] R. Rajamani. *Vehicle Dynamics and Control*. Springer, New York, NY, 2006.

[16] C. Sloth, G. Pappas, and R. Wisniewski. Compositional safety analysis using barrier certificates. In *Hybrid System Computation and Control*, Beijing, China, April 2012.

[17] J. Sztipanovits, X. Koutsoukos, G. Karsai, N. Kottenstette, P. Antsaklis, V. Gupta, B. Goodwine, J. Baras, and S. Wang. Toward a science of cyber-physical system integration. *Proceedings of IEEE*, 100:29–44, January 2012.

[18] A. van der Schaft. Port-hamiltonian systems: Network modeling and control of nonlinear physical systems. In *Advanced Dynamics and Control of Structures and Machines. CISM Courses and Lectures No. 444, CISM International Centre for Mechanical Sciences*, pages 127–168, New York, NY, USA, 2004. Springer.

[19] P. Wu, M. McCourt, and P. Antsaklis. Experimentally determining passivity indices: Theory and simulation. In *ISIS Technical Report ISIS-2013-002*, University of Notre Dame, April 2013.