2017 American Control Conference
Sheraton Seattle Hotel
May 24–26, 2017, Seattle, USA

Safety Analysis of Integrated Adaptive Cruise Control and Lane Keeping Control using Discrete-Time Models of Port-Hamiltonian Systems

Siyuan Dai[1] and Xenofon Koutsoukos[2]

Abstract— **For continuous-time port-Hamiltonian systems (PHS), safety can be shown using the Hamiltonian function as a barrier between the safe and unsafe states. However, the safety property may not be preserved when the system is discretized. This paper presents a safety analysis approach for discrete-time models of PHS using conservative time-discretization and applies the approach to the design of a safe integrated adaptive cruise control (ACC) and lane keeping control (LKC) system. Instead of performing safety analysis in continuous-time and then imposing conditions so that safety is preserved after discretization, safety conditions are developed for a discrete-time model. The approach is applied to the safety analysis of a vehicle dynamics composed with an ACC and a LKC. A hardware-in-the-loop simulation platform is used to evaluate the approach.**

I. Introduction

Port-Hamiltonian systems (PHS) provide a compositional framework for the modeling and design of control systems [6]. They also provide advantages for the analysis of cyber-physical systems (CPS) such as automotive control systems that are composed of multiple subsystems [5]. Safety analysis is important when designing such systems. For example, a vehicle operating in an autonomous manner can be described as a CPS where the physical dynamics of the vehicle interact with an adaptive cruise controller (ACC) and a lane keeping controller (LKC). The ACC controls the speed of the vehicle in response to a detected lead vehicle or a desired speed set by the driver. The LKC controls the angle of the steering wheel in order to maintain a desired lateral position on the road. Safety analysis of the overall system must ensure that the vehicle can operate safely and avoid collisions and skidding.

In our previous work, we have developed an approach for the safety analysis of multi-modal PHS and applied the approach to the safety analysis of a vehicle equipped with an ACC and LKC [5]. The main idea is to use the Hamiltonian function as a barrier between the safe and unsafe states and provide conditions that do not allow the system trajectories to enter the unsafe regions of the state space. The approach has been developed for continuous-time models of PHS, however, implementation of the control system requires discretization. The safety conditions are based on the notion of passivity, and it is well-known that when a passive system is discretized, its passivity is no longer guaranteed [13] [3]. One way to address this problem is to impose conditions on the discretization method and the sampling rate of the system. Further, the design may be conservative, since some "extra" passivity will need to be built into the original system in order to address the impact of discretization (see [23] for more information on passivity indexes). Alternatively, the system model can be discretized and the safety analysis can be performed using a discrete-time model of the system. This paper considers the safety problem using discrete-time models of PHS and its application to integrated speed and steering control.

The theory of PHS is presented in detail in [6]. A PHS consists of a set of ports (control, interaction, resistive, and storage) interconnected through a power-conserving Dirac structure [21]. PHS provide a compositional framework for modeling complex physical lumped-parameter systems [2]. PHS have significant implications for passivity, which has been studied extensively for control design and analysis of nonlinear systems [10]. PHS can be used to describe hybrid systems using a framework known as multi-modal PHS [22]. Discrete-time models of PHS have been presented in [18]. We consider these discretization methods in order to formulate the safety problem for discrete-time multi-modal PHS.

Our safety analysis approach employs a canonical coordinate transform. The canonical coordinate transform method is used extensively in classical mechanics for analyzing the dynamical equations of physical systems. Technical details regarding canonical coordinate transformation of PHS can be found in [8]. The main idea of the proposed approach is to use the Hamiltonian as a barrier certificate to show safety. Barrier certificates are functions which show that there are no state trajectories starting from a given set of states that end up in an unsafe region [15]. They are similar in structure to Lyapunov functions and are typically used for the purpose of validating nonlinear systems with uncertainties [14]. The use of barrier certificates allows analysis of a large class of continuous-time nonlinear models, including differential-algebraic systems with uncertain inputs [17].

The contributions of the paper are a safety analysis approach for discrete-time multi-modal PHS and its application to an integrated adaptive cruise control (ACC) and lane keeping control (LKC) system. Instead of performing safety analysis in the continuous-time domain and then discretizing the controllers for implementation purposes, we model and

[1]Siyuan Dai is with Toyota InfoTechnology Center, 465 Bernardo Ave, Mountain View, CA 94043, USA sdai@us.toyota-itc.com

[2]Xenofon Koutsoukos is with the Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN 37235, USA xenofon.koutsoukos@vanderbilt.edu

design the system in discrete-time [9]. The dynamics of the plant and the control systems are described using conservative time-discretized PHS models, which enable the system to retain passivity [11] [19]. We then 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). We apply the approach for designing an integrated ACC and LKC system and we derive safety conditions which ensure that the host vehicle does not collide with a lead vehicle or skid off of the road. Finally, we evaluate the approach by implementing the control design in a hardware-in-the-loop simulation platform.

The rest of the paper is organized as follows. Section II presents the energy-based safety analysis approach applied to discrete-time multi-modal PHS. Section III applies the safety analysis approach to a vehicle dynamics model composed with an ACC and LKC system described by discrete-time PHS. Section IV describes the evaluation of the discrete-time implementation of the controllers onto a HIL platform. The paper is concluded in Section V.

II. Safety Analysis for Discrete-Time PHS

An appropriate discrete-time model is required for representing PHS [18]. Our approach is based on the conservative time-discretization for PHS, which is presented in [11].

A. Safety Problem

Given a discrete-time PHS with Hamiltonian function H 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.

Definition 1: Given a discrete-time multi-modal PHS and $H(x_k)$ with sampled states $x_k \in X$, initial states $x_0 \in X_0 \subseteq X$, unsafe state space $X_u \subseteq X$, and sampled disturbances $\Delta(k)$, a system trajectory, where k is an integer, $\Gamma(x(kt_s), s(kt_s)) : [0, Nt_s] \rightarrow X$ is unsafe if there exists $N > 0$ and a finite sequence $0 \leq k_1 t_s \leq \cdots \leq k_{N-1} t_s \leq Nt_s$ such that $\Gamma(x_0) \in X_0$ and $\Gamma(x_k) \in X_u$. The system is safe if there are no unsafe state trajectories.

A canonical coordinate transform Φ is needed to convert the dynamic equations and Hamiltonian function of the system into a form which allows to represent the minimum energy. Typically, the canonical coordinate transform method is used for analyzing the dynamics of PHS and there are many possible choices for the coordinate transformations [8]. In this paper, we assume that there exists a coordinate transformation $\overline{x}_k = \Phi(x_k)$ for a d iscrete-time PHS. Then, the dynamic equations of the PHS can be written as:

$$\begin{cases} \frac{\overline{x}_{k+1}-\overline{x}_k}{t_s} &= [\overline{J}(\hat{\overline{x}}_k, s)) - \overline{R}(\hat{\overline{x}}_k, s)] \frac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}(\hat{\overline{x}}_k) \\ & \quad -\overline{J}(\hat{\overline{x}}_k, s))\overline{H}^g(k) \frac{\overline{x}_{k+1}-\overline{x}_k}{\overline{Q}(k)} \\ & \quad + \begin{bmatrix} \overline{L}(\hat{\overline{x}}_k, s) \\ 0 \end{bmatrix} \delta(k) \\ \zeta(k) &= \begin{bmatrix} \overline{L}^{\mathsf{T}}(\hat{\overline{x}}_k, s) & 0 \end{bmatrix} \frac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}(\hat{\overline{x}}_k) \end{cases} \quad (1)$$

$$\begin{aligned} \overline{H}^g(k) &= H(\Phi^{-1}(\overline{x}_{k+1})) - H(\Phi^{-1}(\overline{x}_k)) \\ &\quad + \langle \tfrac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}(\hat{\overline{x}}_k), \overline{J}^g(k) \rangle \\ \overline{J}^g(k) &= \overline{J}^+(\overline{x}_k, s)\overline{J}(\overline{x}_k, s)(x_{k+1} - x_k) \\ \overline{Q}(k) &= (x_{k+1} - x_k)^{\mathsf{T}} \overline{J}^g(k) \end{aligned}$$

where $x_k \equiv x(kt_s)$ are the discrete samples of the continuous state variables (k is a non-negative integer and t_s is the sampling period), $\hat{x}_k = \frac{x_{k+1}+x_k}{2}$, and J^+ is the Moore-Penrose pseudo-inverse matrix of J.

B. Safety Analysis of Discrete-Time Multi-Modal Port-Hamiltonian Systems

We consider the following definitions for initial states, unsafe states, and guard conditions that specify mode transitions. For each discrete mode $s \in S$, the initial states are defined as $\text{Init}(s) = \{x_k \in X : (x_k, s) \in X_0 \times S_0\}$ and the unsafe states are defined as $\text{Unsafe}(s) = \{x_k \in X : (x_k, s) \in X_u \times S_u\}$. Each mode transition $s \rightarrow s'$ is associated with the guard condition $\text{Guard}(s, s') = \{x_k, x'_k \in X : \{x, s\} \rightarrow \{x', s'\} \in \mathbb{T}\}$.

Theorem 1: A multi-modal PHS described by (1) and $H(\Phi^{-1}(\overline{x}_k))$, with states $x_k \in X$, initial states $\text{Init}(s)$, unsafe states $\text{Unsafe}(s)$, and bounded disturbances $\delta(k) \in \Delta(k)$ is safe if the transformed Hamiltonian function $H(\Phi^{-1}(\overline{x}_k))$ satisfies the following conditions with $\alpha \leq \beta$

1) $H(\Phi^{-1}(\overline{x}_k)) \leq \alpha, \forall x \in \text{Init}(s)$
2) $H(\Phi^{-1}(\overline{x}_k)) > \beta, \forall x \in \text{Unsafe}(s)$
3) $\zeta(k)^{\mathsf{T}}\delta(k) \leq \frac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}^{\mathsf{T}} \overline{R}(\overline{x}_k, s) \frac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}$, $\forall \{x_k, \delta\} \in X \times \Delta$
4) $H(\Phi^{-1}(\overline{x}_k)) \leq \alpha, \forall x_k \in \text{Guard}(s, s')$

Proof: Assuming that the Hamiltonian function $H(\Phi^{-1}(\overline{x}_k))$ satisfies 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 $\Gamma(x_0))$ such that $\Gamma(x_T) \in \text{Unsafe}(s)$. We show that the Hamiltonian function cannot simultaneously satisfy the four condition and reach the unsafe region, thus proving safety by contradiction. The time difference of the Hamiltonian functions, $\frac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}(\hat{\overline{x}}_k)^{\mathsf{T}} \frac{\overline{x}_{k+1}-\overline{x}_k}{t_s}$, can be written as:

$$\begin{aligned} &= \tfrac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}(\hat{\overline{x}}_k)^{\mathsf{T}} [\overline{J}(\hat{\overline{x}}_k, s) - \overline{R}(\hat{\overline{x}}_k, s)] \tfrac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}(\hat{\overline{x}}_k) \\ &- \tfrac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}(\hat{\overline{x}}_k)^{\mathsf{T}} \overline{J}(\hat{\overline{x}}_k, s) \overline{H}^g(k) \tfrac{\overline{x}_{k+1}-\overline{x}_k}{\overline{Q}(k)} \\ &+ \tfrac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}(\hat{\overline{x}}_k)^{\mathsf{T}} \begin{bmatrix} \overline{L}(\hat{\overline{x}}_k, s) \\ 0 \end{bmatrix} \delta(k) \end{aligned}$$

The important part of the proof is showing that the interaction structure $\overline{J}$ and the conservative Hamiltonian structure $\overline{J}(\hat{\overline{x}}_k, s))\overline{H}^g(k) \frac{\overline{x}_{k+1}-\overline{x}_k}{\overline{Q}(k)}$ contribute zero energy. As a result of the skew symmetric nature of $\overline{J}$ and the third term of the conservative Hamiltonian structure, we can conclude that:

$$\frac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}(\hat{\overline{x}}_k)^{\mathsf{T}} \overline{J}(\hat{\overline{x}}_k, s) \frac{\partial H(\Phi^{-1}(\overline{x}_k))}{\partial \overline{x}_k}(\hat{\overline{x}}_k) = 0$$

The sum of the remaining two terms of the conservative Hamiltonian structure can be simplified to zero as well.

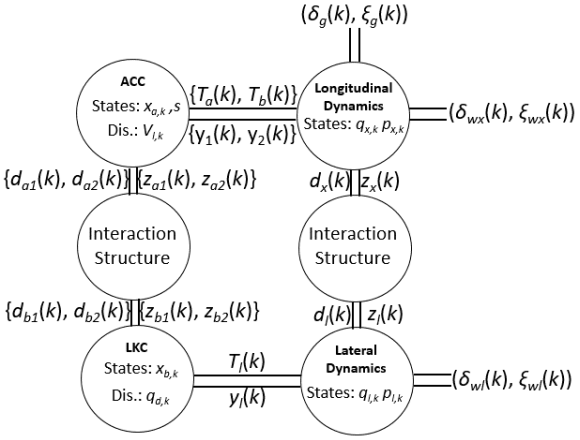

Fig. 1. Closed-loop system

Condition (3) shows that the system trajectory on the 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 Init(s) and end at Unsafe(s). As a result, we can conclude that the system is safe. ■

III. Safety Analysis of Integrated ACC and LKC

We consider the safety problem of a vehicle equipped with both an ACC and a LKC system following a lead car. Figure 1 shows the multi-modal PHS of the vehicle dynamics connected to the ACC and LKC systems via power ports. Disturbances from wind are modeled as ports attached to the longitudinal and lateral vehicle dynamics, while disturbance from the slope of the road is modeled as a port attached to the longitudinal vehicle dynamics.

A. PHS Representation of the System Model

We derived the discrete-time PHS representation of the system model from the continuous-time PHS presented in [5]. For length considerations, we will omit detailed explanations of the variables that can be found in [5].

1) Vehicle Longitudinal Dynamics: The longitudinal dynamics has the following Hamiltonian function:

$$H_x(q_{x,k}, p_{x,k}) = \frac{1}{2m} p_{x,k}^2 + U_x(q_{x,k}),$$

and it is modeled as:

$$\begin{cases} \begin{bmatrix} \frac{q_{x,k+1}-q_{x,k}}{t_s} \\ \frac{p_{x,k+1}-p_{x,k}}{t_s} \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ -1 & -R_{x,k} \end{bmatrix} \begin{bmatrix} \frac{\partial H_x}{\partial q_{x,k}} \\ \frac{\partial H_x}{\partial p_{x,k}} \end{bmatrix} + Q_x(p_{x,k}) \\ & \quad + \begin{bmatrix} 0 \\ G_x \end{bmatrix} u_x(k) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} d_x(k) + \begin{bmatrix} \delta_g(k) \\ \delta_{wx}(k) \end{bmatrix} \\ y_x(k) &= \begin{bmatrix} 0 & G_x^\mathsf{T} \end{bmatrix} \begin{bmatrix} \frac{\partial H_x}{\partial q_{x,k}} & \frac{\partial H_x}{\partial p_{x,k}} \end{bmatrix}^\mathsf{T} \\ z_x(k) &= \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{\partial H_x}{\partial q_{x,k}} & \frac{\partial H_x}{\partial p_{x,k}} \end{bmatrix}^\mathsf{T} \\ \begin{bmatrix} \zeta_g(k) \\ \zeta_{wx}(k) \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{\partial H_x}{\partial q_x} & \frac{\partial H_x}{\partial p_x} \end{bmatrix}^\mathsf{T}, \end{cases} \tag{2}$$

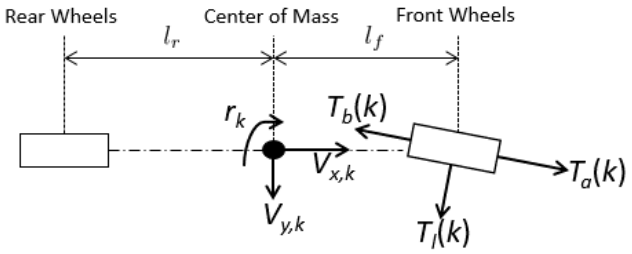

Fig. 2. Free-body diagram of the vehicle dynamics

$$Q_x(p_{x,k}) = \begin{bmatrix} 0 & \frac{1}{2m}p_{x,k+1}^2 - \frac{1}{2m}p_{x,k}^2 \\ \frac{1}{2m}p_{x,k}^2 - \frac{1}{2m}p_{x,k+1}^2 & 0 \end{bmatrix}$$

2) Vehicle Lateral Dynamics: The lateral dynamics has the following Hamiltonian function:

$$H_l(q_{y,k}, q_{r,k}, p_{y,k}, p_{r,k}) = \frac{1}{2m}p_{y,k}^2 + \frac{1}{2I}p_{r,k}^2 + U_l(q_{y,k}, q_{r,k}),$$

and it is modeled as:

$$\begin{cases} \begin{bmatrix} \frac{q_{l,k+1}-q_{l,k}}{t_s} \\ \frac{p_{l,k+1}-p_{l,k}}{t_s} \end{bmatrix} &= \begin{bmatrix} 0 & E \\ -E & -R_{l,k} \end{bmatrix} \begin{bmatrix} \frac{\partial H_l}{\partial q_{l,k}} \\ \frac{\partial H_l}{\partial p_{l,k}} \end{bmatrix} + Q_l(p_{l,k}) \\ & \quad + \begin{bmatrix} 0 \\ G_l \end{bmatrix} T_l(k) + \begin{bmatrix} 0 \\ K_l \end{bmatrix} d_l(k) + \begin{bmatrix} 0 \\ L_l \end{bmatrix} \delta_{wl}(k) \\ y_l(k) &= \begin{bmatrix} 0 & G_l^\mathsf{T} \end{bmatrix} \begin{bmatrix} \frac{\partial H_l}{\partial q_{l,k}} & \frac{\partial H_l}{\partial p_{l,k}} \end{bmatrix}^\mathsf{T} \\ z_l(k) &= \begin{bmatrix} 0 & K_l^\mathsf{T} \end{bmatrix} \begin{bmatrix} \frac{\partial H_l}{\partial q_{l,k}} & \frac{\partial H_l}{\partial p_{l,k}} \end{bmatrix}^\mathsf{T} \\ \zeta_{wl}(k) &= \begin{bmatrix} 0 & L_l^\mathsf{T} \end{bmatrix} \begin{bmatrix} \frac{\partial H_l}{\partial q_l} & \frac{\partial H_l}{\partial p_l} \end{bmatrix}^\mathsf{T}, \end{cases} \tag{3}$$

$$R_{l,k} = \begin{bmatrix} \frac{W_1}{V_{x,k}} & \frac{W_2}{V_{x,k}} \\ \frac{W_2}{V_{x,k}} & \frac{W_3}{V_{x,k}} \end{bmatrix},$$

$$Q_l(p_{l,k})[i,j] = \begin{cases} \frac{1}{2m}p_{y,k+1}^2 - \frac{1}{2m}p_{y,k}^2, & \text{if } (i,j) = (1,3) \\ \frac{1}{2I}p_{r,k+1}^2 - \frac{1}{2I}p_{r,k}^2, & \text{if } (i,j) = (2,4) \\ \frac{1}{2m}p_{y,k}^2 - \frac{1}{2m}p_{y,k+1}^2, & \text{if } (i,j) = (3,1) \\ \frac{1}{2I}p_{r,k}^2 - \frac{1}{2I}p_{r,k+1}^2, & \text{if } (i,j) = (4,2) \\ 0, & \text{if } (i,j) = \text{ any other pair} \end{cases}$$

3) Interaction Between Longitudinal and Lateral 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 2 [16]. Composition of the longitudinal and lateral dynamics is modeled through the interaction structure of (4) modulated by the sampled angular momentum $p_{r,k}$:

$$\begin{bmatrix} d_x(k) \\ d_l(k) \end{bmatrix} = \begin{bmatrix} 0 & -\frac{mp_{r,k}}{I} \\ -\frac{mp_{r,k}}{I} & 0 \end{bmatrix} \begin{bmatrix} z_x(k) \\ z_l(k) \end{bmatrix}. \tag{4}$$

4) Adaptive Cruise Control Design: The ACC is connected to the longitudinal vehicle dynamics through the control ports of $T_a(k)$ and $T_b(k)$. The ACC has the following Hamiltonian function:

$$H_a(x_{a,k}) = \frac{1}{2}(s_t k_{ti} x_{at,k}^2 + s_b k_{bi} x_{ab,k}^2),$$

and it is represented by the following discrete-time model:

$$\begin{cases} \frac{x_{a,k+1}-x_{a,k}}{t_s} & = -R_a \frac{\partial H_a}{\partial x_{a,k}} + G_a y_x(k) + K_{a1} d_{a1}(k) \\ u_x(k) & = G_a^{\mathsf{T}} \frac{\partial H_a}{\partial x_{a,k}} + S_a y_x(k) + K_{a2} d_{a2}(k) \\ \begin{bmatrix} z_{a1}(k) \\ z_{a2}(k) \end{bmatrix} & = \begin{bmatrix} K_{a1}^{\mathsf{T}} & 0 \\ 0 & K_{a2}^{\mathsf{T}} \end{bmatrix} \begin{bmatrix} \frac{\partial H_a}{\partial x_{a,k}} \\ y_x(k) \end{bmatrix}. \end{cases} \tag{5}$$

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

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

5) Lane Keeping Control Design: The LKC connects with the lateral vehicle dynamics through the control port of T_l. The LKC has the following Hamiltonian function:

$$H_b(x_{b,k}) = \frac{1}{2} k_{si} x_{b,k}^2,$$

and it is represented by the following discrete-time model:

$$\begin{cases} \frac{x_{b,k+1}-x_{b,k}}{t_s} & = y_l(k) + d_{b1}(k) \\ T_l(k) & = \frac{\partial H_b}{\partial x_{b,k}} + k_{sd} y_l(k) + d_{b2}(k) \\ \begin{bmatrix} z_{b1}(k) \\ z_{b2}(k) \end{bmatrix} & = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{\partial H_b}{\partial x_{b,k}} \\ y_l(k) \end{bmatrix}. \end{cases} \tag{6}$$

6) Interaction Between the Controllers: We connect the ACC and LKC using the following interaction structure, so that the state variables and outputs of the ACC are affected by the state variable of the LKC, and vice versa.

$$\begin{bmatrix} d_{a1}(k) \\ d_{a2}(k) \\ d_{b1}(k) \\ d_{b2}(k) \end{bmatrix} = \begin{bmatrix} 0 & 0 & J_c & 0 \\ 0 & 0 & 0 & M_c \\ -J_c^{\mathsf{T}} & 0 & 0 & 0 \\ 0 & -M_c^{\mathsf{T}} & 0 & 0 \end{bmatrix} \begin{bmatrix} z_{a1}(k) \\ z_{a2}(k) \\ z_{b1}(k) \\ z_{b2}(k) \end{bmatrix}, \tag{7}$$

where the parameters J_c and M_c define how the speed control and the steering control interact. 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.

7) Closed-Loop System: The closed-loop system, composed from (2), (3), (4), (5), (6), and (7), has a Hamiltonian function $\tilde{H}(q_k, p_k, z_k) = H_x + H_l + H_a + H_b$, sampled continuous states $\{q_k, p_k, x_k\} \in \tilde{X}$, 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 $\delta(k) = \{\delta_g(k), \delta_{wx}(k), \delta_{wy}(k)\} \in \Delta_g(k) \times \Delta_{wx}(k) \times \Delta_{wy}(k)$.

$$\begin{cases} \begin{bmatrix} \frac{q_{k+1}-q_k}{t_s} \\ \frac{p_{k+1}-p_k}{t_s} \\ \frac{x_{k+1}-x_k}{t_s} \end{bmatrix} & = \begin{bmatrix} 0 & I & 0 \\ -I & \tilde{J}_k - \tilde{R}_k & \tilde{K} \\ 0 & -\tilde{K}^{\mathsf{T}} & -\tilde{Q} \end{bmatrix} \begin{bmatrix} \frac{\partial \tilde{H}}{\partial q_k} \\ \frac{\partial \tilde{H}}{\partial p_k} \\ \frac{\partial \tilde{H}}{\partial x_k} \end{bmatrix} \\ & \quad + \begin{bmatrix} 0 \\ \tilde{L} \\ 0 \end{bmatrix} \delta(k) \\ \zeta(k) & = \begin{bmatrix} 0 & \tilde{L} & 0 \end{bmatrix} \begin{bmatrix} \frac{\partial \tilde{H}}{\partial q_k} & \frac{\partial \tilde{H}}{\partial p_k} & \frac{\partial \tilde{H}}{\partial x_k} \end{bmatrix}^{\mathsf{T}} \end{cases} \tag{8}$$

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

$$\tilde{J}_k = \begin{bmatrix} 0 & \frac{m p_{r,k}}{I} - M_c & -l_f M_c \\ -\frac{m p_{r,k}}{I} + M_c & 0 & 0 \\ l_f M_c & 0 & 0 \end{bmatrix},$$

$$\tilde{R}_k = \begin{bmatrix} R_{x,k} & 0 & 0 \\ 0 & \frac{mW_1}{p_{x,k}} + k_{sd} & \frac{mW_2}{p_{x,k}} + l_f k_{sd} \\ 0 & \frac{mW_2}{p_{x,k}} + l_f k_{sd} & \frac{mW_3}{p_{x,k}} + l_f^2 k_{sd} \end{bmatrix},$$

$$\tilde{K} = \begin{bmatrix} s_t P & s_b & 0 \\ 0 & 0 & -1 \\ 0 & 0 & -l_f \end{bmatrix}, \tilde{L} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

$$\tilde{Q} = \begin{bmatrix} s_t k_t & 0 & -J_c \\ 0 & s_b k_b & 0 \\ J_c & 0 & 0 \end{bmatrix}.$$

B. Safety Problem

The safety condition for the longitudinal dynamics asserts that the relative distance between the two vehicles will fall below a minimum distance q_m.

$$X_{ku} = \left\{ q_{x,k} \in \mathbb{R} : q_{x,k} \geq \sum_{i=0}^{k} t_s V_{l,i} + q_l(0) + q_m \right\}, \tag{9}$$

where $q_l(0)$ is the initial displacement value of the lead vehicle. The unsafe set states that the system is unsafe if the displacement of the host vehicle exceeds that of the lead vehicle extended by q_m, which is indicative of an impending collision. Given (8), the safety condition for the closed-loop system states that that all possible trajectories cannot reach the unsafe region described by (9).

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.

$$X_{lu} = \{ p_{x_k} \in \mathbb{R}, p_{r_k} \in \mathbb{R} : p_x p_r \geq m^2 I A_m \}. \tag{10}$$

This safety condition indicates that longitudinal and lateral motion are bounded by a hyperbolic relationship. Using this safety constraint we must verify that the product of longitudinal momentum and yaw rate does not exceed a maximum threshold. Given (8) 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 (9) and (10).

C. Safety Analysis

The initial states are defined as $\overline{\text{Init}}(s_a) = \{(q_k, p_k, x_k) \in \tilde{X} : (q_k, p_k, x_k, s_a) \in \tilde{X}_0\}$ and the unsafe states are defined as $\overline{\text{Unsafe}}(s_a) = \{(q_k, p_k, x_k) \in \tilde{X} : (q_{x,k}, p_{x,k}, p_{r,k}) \in X_{ku} \times X_{lu}$. Each transition from $s_a \in S_a$ to $s_a' \in S_a$ is associated with the guard set $\overline{\text{Guard}}(s_a, s_a') = \{(q_k, p_k, x_k), (q_k, p_k, x_k)' \in \tilde{X} : (q_k, p_k, x_k, s_a) \to (q_k', p_k', x_k', s_a')\}$. Using similar assumptions as in the continuous-time case [5], we can prove that

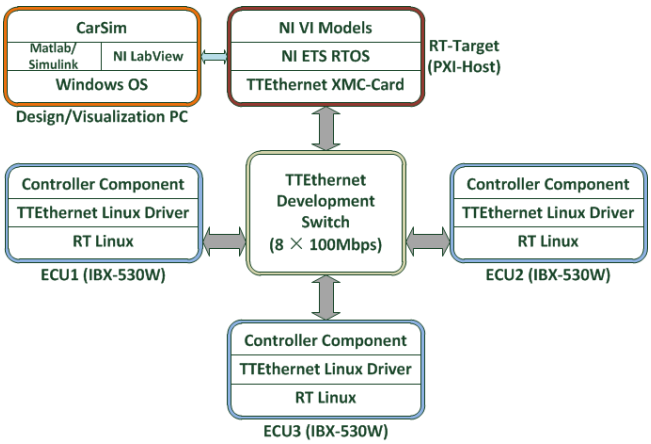

Fig. 3. HIL simulator architecture [7]

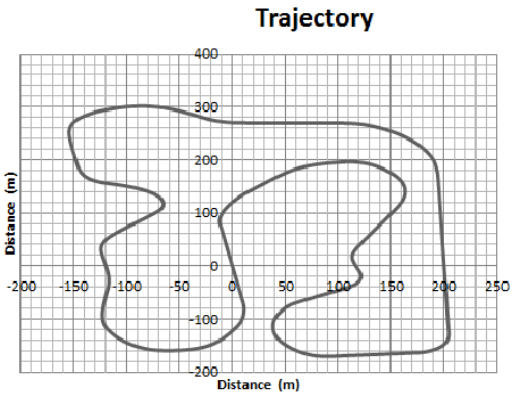

Fig. 4. Trajectory of the road

(8) is guaranteed to be safe, given the following coordinate transformation $\tilde{\Phi}_k = \begin{bmatrix}\tilde{\Phi}_{x,k} & \tilde{\Phi}_{y,k} & \tilde{\Phi}_{r,k}\end{bmatrix}^{\mathsf{T}}$:

$$\begin{bmatrix}\overline{p}_{x,k}\\ \overline{p}_{y,k}\\ \overline{p}_{r,k}\end{bmatrix} = \begin{bmatrix}\tilde{\Phi}_{x,k}(p_{x,k})\\ \tilde{\Phi}_{y,k}(p_{y,k})\\ \tilde{\Phi}_{r,k}(p_{r,k})\end{bmatrix} = \begin{bmatrix} p_{x,k} - m(1+\gamma\frac{X_r - X_d}{X_d})V_l - M_c x_{b,k} \\ p_{y,k} + k_{si}(q_{y,k} - q_d) + M_c(x_{at,k} + x_{ab,k}) \\ p_{r,k} + k_{si}(q_{r,k} - \frac{q_d}{l_f}) + M_c\frac{x_{at,k}+x_{ab,k}}{l_f}\end{bmatrix}.$$

We restate the first condition of Theorem 1 as $\tilde{H}(\tilde{\Phi}_k^{-1}(\overline{p}_k)) \leq \tilde{\alpha}_k, \forall (q_k, p_k, x_k) \in \overline{\text{Init}}(s_a)$, where

$$\begin{aligned}\tilde{\alpha} &= m\tfrac{k_{td}+k_{bd}}{2}(V_{x,0} - (1+\gamma\tfrac{X_{r,0} - hV_{l,k} - S_0}{hV_{l,0}+S_0})V_{l,0})^2 \\ &\quad + \tfrac{m}{2}V_{x,0}^2\sin^2(\rho(0)V_{x,0} + \omega(0)) + \tfrac{I}{2}\rho^2(0)V_{x,0}^2.\end{aligned}$$

We restate the second condition of Theorem 1 as $\tilde{H}(\tilde{\Phi}_k^{-1}(\overline{p}_k)) > \tilde{\beta}_k, \forall (q_k, p_k, x_k) \in \overline{\text{Unsafe}}(s_a)$, where

$$\begin{aligned}\tilde{\beta} &= m\tfrac{k_{td}+k_{bd}}{2}(V_{x,k} - (1-\gamma)V_{l,k} - \tfrac{M_c}{m}(q_{y,k} - q_d))^2 \\ &\quad + \tfrac{m}{2}(V_{x,k}\sin(\rho V_{x,k} + \omega) + k_{si}(q_{y,k} - q_d))^2 \\ &\quad + \tfrac{I}{2}(\rho V_{x,k} + k_{si}(q_{y,k} - \tfrac{q_d}{l_f}))^2.\end{aligned}$$

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

$$\begin{aligned}&\zeta_g(k)\delta_g(k) + \zeta_{wx}(k)\delta_{wx}(k) + \zeta_{wy}(k)\delta_{wy}(k) \\ &\leq \frac{\partial\tilde{H}(\tilde{\Phi}_k^{-1}(\overline{p}_k))}{\partial(q_k,\overline{p}_k)}^{\mathsf{T}}\frac{\partial\tilde{\Phi}_k}{\partial p_k}\tilde{R}(\tilde{\Phi}_k^{-1}(\overline{p}_k))\frac{\partial\tilde{\Phi}_k}{\partial p_k}^{\mathsf{T}}\frac{\partial\tilde{H}(\tilde{\Phi}_k^{-1}(\overline{p}_k))}{\partial(q_k,\overline{p}_k)}.\end{aligned}$$

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 $\overline{\text{Unsafe}}(s_a)$. We restate the fourth condition of Theorem 1 as $\tilde{H}(\tilde{\Phi}_k^{-1}(\overline{p}_k)) \leq \tilde{\alpha}_k, \forall (q_k, p_k, x_k) \in \overline{\text{Guard}}(s_t, s_b) \cup \overline{\text{Guard}}(s_b, s_t)$.

IV. Evaluation and Validation

Our objective is to implement the proposed control design into a hardware-in-the-loop (HIL) simulation platform and ensure that the system is safe. The HIL platform, shown in Figure 3 and detailed in [7], provides a realistic environment for validating automotive control software. The physical dynamics of the vehicle is modeled in CarSim [1] and is simulated in real-time. The vehicle simulation interfaces with three electronic control units (ECUs) that form a time-triggered network (100Mbps TTEthernet developed by TTTech [20]). We selected the control parameters (from Table I) using the method presented in [4]. We used a sampling period of 10 ms. We quantized the controllers using Simulink's Fixed-Point Toolbox, which allows us to set the word lengths as 32-bit fixed point data. The safety analysis method of this paper ensures that the control parameters will result in a safe closed-loop system.

TABLE I
Table of Controller Gains

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

In this section we present simulation results to validate the safety analysis approach and to compare them to the continuous-time results presented in [5]. 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 on a trajectory (Figure 4). The safety conditions derived in Section III 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.

Figure 5 shows the relative distance between the two vehicles for the continuous-time case and the conservative time-discretization case. Figure 6 shows the lateral acceleration of the host vehicles for the continuous-time case and the conservative time-discretization case. The continuous-time results are derived from simulations using only Simulink [12] and CarSim [1] [5]. The conservative time-discretization results indicate that the system behaves in a safe manner. One of the main goals of using this discretization method is for the discrete-time results to match the continuous-time

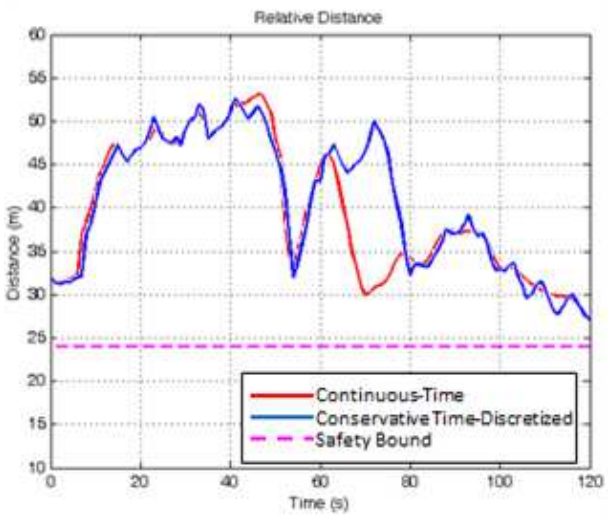

Fig. 5. Relative distance comparison

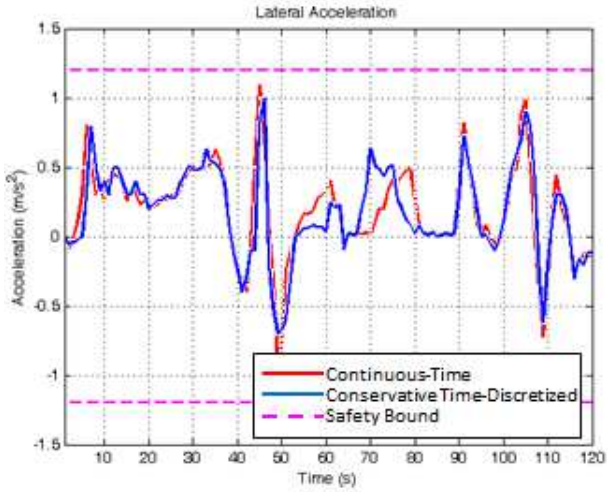

Fig. 6. Lateral acceleration comparison

results. Figures 5 and 6 indicate that the continuous-time and discrete-time results mostly match.

V. Conclusion

This paper considers the safety problem of PHS and its application to adaptive cruise control and lane keeping control. Safety analysis can be performed using continuous-time models and passivity but implementation of the control system may not preserve passivity because of the fact that passivity degrades during discretization. Our objective is to perform safety analysis using discrete-time models, so that we can use the results to reason about safety of the implementation of the control system in a realistic setting. We developed a safety analysis method using conservative time-discretization and we presented a case study for the safety analysis of a automotive control systems that shows collision and skidding avoidance. The method is evaluated by implementing the control design in a HIL simulation platform and comparing the results with simulations of the continuous-time design.

Acknowledgement

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

References

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

[2] J. Cervera, A. J. van der Schaft, and A. Baños. Interconnection of port-hamiltonian systems and composition of dirac structures. *Automatica*, 43:214–217, February 2007.

[3] R. Costa-Castello and E. Fossas. On preserving passivity in sampled-data linear systems. *Proceedings of the 2006 American Control Conference*, pages 4373–4378, June 2006.

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

[5] S. Dai and X. Koutsoukos. Safety analysis of automotive control systems using multi-modal port-hamiltonian systems. *19th ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2016)*, April 2016.

[6] 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.

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

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

[9] O. Gonzalez. Time integration and discrete hamiltonian systems. *Journal of Nonlinear Science*, 6:449–467, 1996.

[10] H. Khalil. *Nonlinear Systems*. Prentice-Hall, Inc., Upper Saddle River, NJ, 2002.

[11] D. S. Laila and A. Astolfi. Construction of discrete-time models for port-hamiltonian systems with applications. *Systems and Control Letters*, 55:673–680, 2006.

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

[13] Y. Oishi. Passivity degradation under the discretization with the zero-order hold and the ideal sampler. *49th IEEE Conference on Decision and Control*, December 2010.

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

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

[16] R. Rajamani. *Vehicle Dynamics and Control*. Mechanical Engineering Series, 2012.

[17] C. Sloth, G. J. Pappas, and R. Wisniewski. Compositional safety analysis using barrier certificates. *2012 Conference on Hybrid Systems Computation and Control*, April 2012.

[18] O. J. Staffans. Passive linear discrete time-invariant systems. *Proceedings of the International Congress of Mathematicians*, 2006.

[19] S. Stramigioli, C. Secchi, A. J. van der Schaft, and C. Fantuzzi. Sampled data systems passivity and discrete port-hamiltonian systems. *IEEE Transactions on Robotics*, 21(4):574–587, 2005.

[20] TTEthernet. *http://www.tttech.com/en/products/ttethernet/*. TTTech Computertechnik AG, Vienna, Austria, 2013.

[21] A. van der Schaft. Port-hamiltonian systems: Network modeling and control of nonlinear physical systems. *Advanced Dynamics and Control of Structures*, 2004.

[22] A. van der Schaft. Port-hamiltonian systems: An introductory survey. *Proceedings of the International Congress of Mathematicians*, 2006.

[23] H. Yu and P. Antsaklis. A passivity measure of systems in cascade based on passivity indices. *49th IEEE Conference on Decision and Control*, December 2010.