Safety Verification Using Barrier Certificates with Application to Double Integrator with Input Saturation and Zero-Order Hold *

Azad Ghaffari, Imoleayo Abel, Daniel Ricketts, Sorin Lerner, and Miroslav Krstić

***Abstract*— It is desirable to increase the control sample period in cyber-physical systems such that the available processing power and data transfer are minimized. In this paper, a safety verification technique is proposed which allows a trade-off between the size of the sample period and the convergence rate. The proposed technique is applied to a double integrator with input saturation and zero-order hold. An expression for the control law and an explicit relationship between sample period and control parameters are presented. It is shown that the proposed control law drives all state trajectories initiated in the safe set to the origin without violating safety criteria as long as the sample period remains sufficiently small. Moreover, if the control signal is bounded between the proposed limits, it is shown analytically that a pilot-based configuration also remains in the safe set. The effectiveness of the proposed technique is verified using numerical simulations.**

I. Introduction

Barrier certificate functions (BCFs) are commonly used in the safety verification of cyber-physical systems [4], [6], [8], [9], [14]. Also, barrier Lyapunov functions have been extensively used to design controllers to enforce state constraints on a given system [7], [11]. Recently, control barrier functions have been used along with control Lyapunov functions in the quadratic programming of safety-critical systems [1], [2] and constrained stabilization of nonlinear systems [5]. The existing methods are developed for continuous time controllers. Moreover, the formulation of the barrier Lyapunov functions and control barrier functions creates complexity in deriving an explicit control law, even in low-order systems.

In this paper, we focus on developing a minimal safety verification technique for a general nonlinear system where the control input has a zero-order hold (ZOH) unit. The proposed technique is an extended version of the continuous time safety verification technique. We then use the proposed technique as a building block to verify safety of a quadcopter which operates inside a geofence. Movement of the quadcopter in each dimension can be simplified as a double integrator. It is desirable to control the system such that a specific position barrier such as an altitude limit is not violated while the control input is subject to saturation and has a ZOH unit. In other words, the system is allowed to move freely farther away from the barrier but must stop smoothly at the barrier without violating the safety criteria.

Azad Ghaffari, Imoleayo Abel, and Miroslav Krstić are with the Department of Mechanical and Aerospace Engineering, University of California, San Diego, CA 92093-0411, USA, aghaffari@ucsd.edu, iabel@ucsd.edu, and krstic@ucsd.edu.

Daniel Ricketts and Sorin Lerner are with the Department of Computer Science and Engineering, University of California, San Diego, CA 92093-0411, USA, daricket@ucsd.edu and lerner@ucsd.edu.

* This research was supported in part by the National Science Foundation through grant 1544757

Safety verification techniques have been implemented in physical systems with digital controllers [13], [3] with state-of-the-art hardware where computational resources are in abundance. In real-world applications, because of augmentation of cloud computing in smart networks, it is desirable to conserve the computational resources and reduce the traffic of communication lines. So, the sample period of the ZOH unit can be tuned to minimize the network load while the safe operation of the system is guaranteed. Our extension of the continuous time safety verification technique provides a simple analytic tool that is easy to implement and accommodates the effect of sampling. We enforce exponential decay on the BCF to compensate the effect of sampling. Hence, the proposed modification ensures that the time derivative of the BCF changes by no more than a state-independent constant in between sample instants. This additional condition allows us to compute bounds on the control input as a function of the sample period and system parameters to guarantee the forward invariance of the safe set.

The contributions of this paper are twofold. First, we propose a modified version of the BCF-based safety verification technique suitable for general nonlinear systems with a ZOH unit in the input, where the ZOH sample period may be larger than the response time of the plant dynamics. Second, we apply the results of the first step to a double integrator with input saturation and ZOH. The proposed technique enforces an upper bound on the growth rate of the BCF, so the effect of the ZOH unit can be compensated. We provide explicit relationships between the control law, ZOH sample period, input saturation level, and the BCF such that the safe set is forward invariant. Two control goals are achieved for the double integrator. First, the proposed control law drives every initial condition in the safe set toward the origin without violating safety criteria. Second, when a pilot is in charge, the modified control law guarantees the safety of the system. In other words, the system stays in the safe set as long as the pilot does not violate the safety criteria. The system will stop at the origin if the pilot wants to violate the safety criteria.

The rest of this paper is organized as follows: We introduce BCFs with exponential decay rate in Section II and describe necessary properties of the BCFs to accommodate the effect of the ZOH. In Section III, we develop a BCF for the double integrator with input saturation and ZOH. Section IV proposes safety verification and convergence results for the double integrator. Section V provides numerical simulations to show the effectiveness of the proposed technique. Section VI concludes the paper.

II. Barrier Certificate Functions

A dynamic system is given in the following

$$\frac{d}{dt}z = f(z,u) \tag{1}$$

where $z \in \mathcal{Z} \subseteq \mathbb{R}^n$, and $u \in \mathcal{U} \subseteq \mathbb{R}$. In safety verification applications, it is desirable not only to drive the system to the origin but also to contain the system trajectory in a predefined region of the state domain. So, a barrier certificate function (BCF) with exponential decay rate is introduced to ensure the operation of the system in the safe domain.

Definition 1 (Kong et al. [6]): a function $B(z) : \mathcal{Z} \to \mathbb{R}$ is a barrier certificate of system (1) if it is differentiable with respect to its argument and satisfies the following conditions:

1) $B(z_0) \leq 0$ where z_0 is the initial condition
2) $(\partial B(z)/\partial z)\, f(z,u) \leq -\alpha B(z)$, where u is an input and α is an arbitrary constant.

Remark 1: Barrier Lyapunov functions [7], [11], control barrier functions [1], [2], [8], and nested saturation controllers [12] have been widely used to enforce state constraints when a reference state trajectory is tracked. In this work, however, we are not concerned about tracking a reference state trajectory. Instead, we focus on avoiding a barrier whose shape is enforced by the input saturation. We have found BCFs with exponential decay rate sufficiently flexible to study the problem in hand. Please refer to Ricketts [10] for a detailed comparison between different forms of barrier certificates.

If there exists a BCF for the system (1), then it is straightforward to prove the safety of system (1) using the following lemma.

Lemma 1 (Kong et al. [6]): Assume that $B(z)$ is a BCF of the system (1). Then the safety of the system is guaranteed for $B(z)$, i.e., $B(z(t)) \leq 0$ for all $t \geq 0$.

A proof is obtained by converting the second condition of the BCF to the following equality:

$$\frac{d}{dt}B(z(t)) + \alpha B(z(t)) - g(t) = 0, \tag{2}$$

where $g(t) \leq 0$ and $B(z(0)) \leq 0$. The solution of (2) gives $B(z(t)) \leq 0$ for all $t \geq 0$.

In a real-world application, however, the control is implemented using a digital processing unit which includes a ZOH unit. So, it is desirable to extend the results of Lemma 1 to continuous time systems with a ZOH unit in the input

$$\frac{d}{dt}z = f(z,u_k), \tag{3}$$

where $u_k \in U \subset \mathcal{U}$. Control input u_k has a constant value for all $t \in [t_k, t_k + T)$, where T is the sample period and $k = 0, 1, 2, \cdots$. Also, the sampled state at time t_k is shown as $z_k = z(t_k)$. The sampled data version of Lemma 1 is proposed in the following.

Theorem 2 (Barrier Certificate for General Systems with ZOH): Consider system (3) and a differentiable function $B : \mathcal{Z} \to \mathbb{R}$. Let $\alpha \in \mathbb{R}^+$ denote a constant and, given $k \in \mathbb{N}$ and $z_k \in \mathcal{Z}$, let $U \subset \mathcal{U}$ denote a set of inputs u_k such that

$$\frac{\partial B(z_k)}{\partial z} f(z_k, u_k) \leq -\alpha B(z_k). \tag{4}$$

Furthermore, let there exist $\beta \in \mathbb{R}$ such that the solution $z(t)$ of (3) for the initial condition $z_k \in \mathcal{Z}$ and $u_k \in U$ satisfy

$$\frac{\partial B(z(t))}{\partial z} f(z(t), u_k) - \frac{\partial B(z_k)}{\partial z} f(z_k, u_k) \leq \beta \tag{5}$$

for all $t \in [t_k, t_k + 1/\alpha)$. If

$$B(z_k) \leq \frac{\beta}{\alpha} \triangleq c, \tag{6}$$

then

$$B(z(t)) \leq c \tag{7}$$

for all $t \in [t_k, t_k + 1/\alpha)$. Moreover if conditions (4)–(6) are satisfied with β independent of k, (7) holds for all $t \geq t_0$.

Proof: Since $B(z)$ is a differentiable function for $t \in [t_k, t + T)$, we have

$$B(z) - B(z_k) = \int_{t_k}^{t} \frac{d}{d\tau} B(z(\tau)) d\tau \tag{8}$$

$$= \int_{t_k}^{t} \frac{\partial B(z(\tau))}{\partial z} f(z(\tau), u_k) d\tau. \tag{9}$$

From (5) we get

$$B(z) - B(z_k) \leq \int_{t_k}^{t} \frac{\partial B(z_k)}{\partial z} f(z_k, u_k) + \beta d\tau \tag{10}$$

$$\leq \frac{\partial B(z_k)}{\partial z} f(z_k, u_k)\delta + \beta\delta, \tag{11}$$

where $\delta = t - t_k$. Using (4) we get

$$B(z) - B(z_k) \leq -\alpha\delta B(z_k) + \alpha\delta c \tag{12}$$

$$B(z) \leq (1 - \alpha\delta) B(z_k) + \alpha\delta c \tag{13}$$

$$B(z) - c \leq (1 - \alpha\delta)\,(B(z_k) - c) \tag{14}$$

From (6) we obtain $B(z_k) - c \leq 0$. Also, $\delta \leq 1/\alpha$, thus $(1 - \alpha\delta) \geq 0$, therefore $B(z) \leq c$ for $t \in [t_k, t_k + 1/\alpha)$. Using induction, one can show that $B(z) \leq c$ for all $t \geq t_0$. ∎

We presented Theorem 2 to investigate the safety of continuous time systems with a ZOH unit at the input. So, the control signal is only updated at sampling instants. In between sampling instants, there is no control over the evolution of the system (and consequently, the rate of change of $\mathcal{B}(x,v)$). Thus, condition (5) of Theorem 2 enforces an upper bound on the rate of time variation of $\mathcal{B}(x,v)$ along the system dynamics in between samples.

Remark 2: While Definition 1 uses an arbitrary constant α, Theorem 2 requires the constant α to be positive. In additon, the solution of the system (3) is required to evaluate condition (5) which may restrict the application of Theorem 2. It is possible, however, to present a less conservative form of Theorem 2 by relaxing condition (5) by enforcing Lipschitz continuity

$$\frac{\left\| \frac{\partial B(z)}{\partial z} f(z, u_k) - \frac{\partial B(z_k)}{\partial z} f(z_k, u_k) \right\|}{\|z - z_k\|} \leq \beta. \tag{15}$$

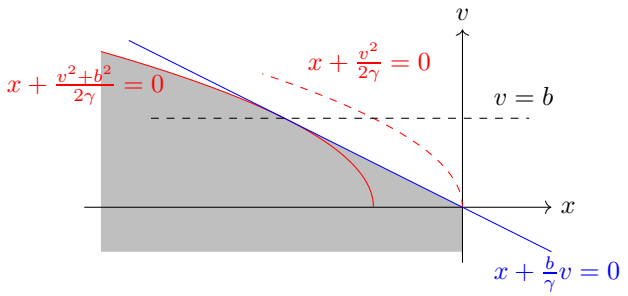

Fig. 1: Shaded area shows the safe set of the second order system.

Furthermore, one has to assume that $\|f(z, u_k)\|$ is bounded to proceed with the proof of Theorem 2.

III. Barrier Certificate of Double Integrator with Input Saturation and ZOH

Consider the following double integrator

$$\frac{d}{dt}x = v \tag{16}$$

$$\frac{d}{dt}v = u_k, \qquad -\mu \leq u_k \leq \mu, \tag{17}$$

where x is position and v is velocity. It is assumed that the initial position satisfies $x_0 \leq 0$. The goal of the control design is to maintain $x \leq 0$ for all $t \geq 0$.

In addition to sample period, T, the physical limitation of the control input, $-\mu \leq u_k \leq \mu$, plays a vital role in safety verification of the system (16)–(17). Consider the braking command $u_k = -\gamma$, where $0 < \gamma < \mu$. The state trajectory associated with $u_k = -\gamma$ with initial condition $(x_0 < 0, v_0 > 0)$ and final condition $(0, 0)$ is expressed as $x_0 + v_0^2/(2\gamma) = 0$ which its plot for $v > 0$ is shown in Fig. 1. The initial conditions between the vertical axis and $x_0 + v_0^2/(2\gamma) = 0$ require braking command of $u_k < -\gamma$ to guarantee $x \leq 0$. Otherwise, the state trajectories cross the vertical axis. As shown in Fig. 1, we select the following safety barrier for the system (16)–(17)

$$\hat{\mathcal{B}}(x, v) = x + \frac{1}{2\gamma}v^2. \tag{18}$$

We argued that $\hat{\mathcal{B}}(x, v) = 0$ defines a safety barrier of the system under control input $-\gamma \leq u_k \leq \mu$. However, the state trajectories that arrive on the safety barrier (18) do not stop at the origin. To ensure that the system stops at the origin we introduce a safety barrier that is quadratic away from the origin (similar to (18)) but linear close to the origin as shown in Fig. 1. The modified barrier function is introduced as the following

$$\mathcal{B}(x, v) = \begin{cases} x + \frac{1}{2\gamma}(v^2 + b^2), & v \geq b \\ x + \frac{b}{\gamma}v, & v < b, \end{cases} \tag{19}$$

where $b > 0$. When the state trajectory arrives on the linear segment, we get $dx/dt = -(\gamma/b)x$ and $dv/dt = -(\gamma/b)v_k$. Thus, the system will stop at the origin.

Note that the linear segment of the barrier function is tangent to the quadratic segment at $v = b$, making the barrier function continuously differentiable. The linear segment of the safety barrier permits a decreasing braking command as the system approaches the origin, enabling the system to settle smoothly at the origin. For notational simplicity, we combine the two cases of (19) into the following

$$\mathcal{B}(x, v) = x + \frac{h(v-b)}{2\gamma}\left(v^2 + b^2\right) + \left(1 - h(v-b)\right)\frac{b}{\gamma}v, \tag{20}$$

where

$$h(\theta) = \begin{cases} 1, & \theta \geq 0 \\ 0, & \theta < 0. \end{cases} \tag{21}$$

We emphasize the usage of the function $h(\cdot)$ solely for simplicity and as such $h(\cdot)$ is ignored in all subsequent computations involving time derivatives.

IV. Safety Verification of Double Integrator with Input Saturation and ZOH

We use (20) to verify the safety of the system (16)–(17). Conditions (4) and (5) of Theorem 2 are first satisfied in the following two lemmas respectively.

Lemma 3: If the control signal satisfies

$$u_k \leq \gamma \frac{\left(-v_k - \alpha\mathcal{B}(x_k, v_k)\right)}{h(v_k - b)v_k + (1 - h(v_k - b))b}, \tag{22}$$

for some $\alpha \in \mathbb{R}^+$, then the condition (4), namely,

$$\begin{bmatrix} \frac{\partial\mathcal{B}(x_k,v_k)}{\partial x} & \frac{\partial\mathcal{B}(x_k,v_k)}{\partial v} \end{bmatrix} \begin{bmatrix} v_k \\ u_k \end{bmatrix} \leq -\alpha\mathcal{B}(x_k, v_k) \tag{23}$$

is satisfied for the system (16)–(17) with barrier function (20).

Proof: Note that $h(v_k - b)v_k + (1 - h(v_k - b))b \geq 0$. So, (22) can be rewritten as the following

$$v_k + \left(\frac{h(v_k - b)}{\gamma}v_k + (1 - h(v_k - b))\frac{b}{\gamma}\right)u_k \leq -\alpha\mathcal{B}(x_k, v_k). \tag{24}$$

With further simplification one arrives at (23) which concludes the proof. ■

Lemma 4: The following holds for the system (16)–(17) and barrier function (20) for $u_k \leq \mu$

$$\begin{bmatrix} \frac{\partial\mathcal{B}(x,v)}{\partial x} & \frac{\partial\mathcal{B}(x,v)}{\partial v} \end{bmatrix} \begin{bmatrix} v \\ u_k \end{bmatrix} \leq \begin{bmatrix} \frac{\partial\mathcal{B}(x_k,v_k)}{\partial x} & \frac{\partial\mathcal{B}(x_k,v_k)}{\partial v} \end{bmatrix} \begin{bmatrix} v_k \\ u_k \end{bmatrix} + \\ + \mu T\left(1 + \frac{\mu}{\gamma}\right), \qquad t \in [t_k, t_k + T), \tag{25}$$

namely, (5) is satisfied with

$$\beta = \mu T\left(1 + \frac{\mu}{\gamma}\right). \tag{26}$$

Proof: Denote $\delta = t - t_k$. From (16)–(17) and (20) and by using $v = v_k + u_k\delta$ we get

$$\begin{bmatrix} \frac{\partial\mathcal{B}(x,v)}{\partial x} & \frac{\partial\mathcal{B}(x,v)}{\partial v} \end{bmatrix} \begin{bmatrix} v \\ u_k \end{bmatrix} = \\ = v + \frac{h(v-b)}{\gamma}vu_k + (1 - h(v-b))\frac{b}{\gamma}u_k \\ \leq \begin{bmatrix} \frac{\partial\mathcal{B}(x_k,v_k)}{\partial x} & \frac{\partial\mathcal{B}(x_k,v_k)}{\partial v} \end{bmatrix} \begin{bmatrix} v_k \\ u_k \end{bmatrix} + \delta u_k + \frac{\delta}{\gamma}u_k^2. \tag{27}$$

Inequality (27) is valid for all v and v_k. Note that $0 \leq \delta \leq T$ and since $u_k \leq \mu$, (25) is satisfied. Also, comparing (25) with condition (5) of Theorem 2, we get (26). ■

Recall the definition $c \triangleq \beta/\alpha$ from (6). The following sets represent the safe set and safety buffer, respectively.

$$\Phi_c = \{(x,v) \in \mathbb{R}^2 : x \leq c \ \cap \ \mathcal{B}(x,v) \leq c\} \tag{28}$$

$$\Psi_c = \{(x,v) \in \mathbb{R}^2 : 0 < x \leq c \cap 0 < \mathcal{B}(x,v) \leq c\} \tag{29}$$

We summarize the safety verification of the double integrator in the following.

Theorem 5 (Double Integrator with Input Saturation and ZOH): Consider the system (16)-(17) with $0 < T \leq 1/\alpha$ and the input with saturation and ZOH, $-\mu \leq u_k \leq \mu$, where $\alpha > 0$ and $\mu > 0$. The barrier function is (20), with

$$\gamma \leq \mu \frac{b - \mu T}{b + \mu T}, \tag{30}$$

and $b > \mu T$. If the conditions of Lemmas 3 and 4 are satisfied, i.e. if u_k satisfies

$$u_k \leq \min \left\{ \mu, -\gamma \frac{\big(v_k + \alpha \mathcal{B}(x_k, v_k)\big)}{h(v_k - b)v_k + (1 - h(v_k - b))b} \right\}. \tag{31}$$

for all $(x_k, v_k) \in \Phi_c$ for all $k = 0, 1, 2, \cdots$, then $(x(t), v(t)) \in \Phi_c$ for all $t \geq t_0$.

Proof: Following the footsteps of Theorem 2, it is straightforward to show that $\mathcal{B}(x,v) \leq c$ for all $t \geq t_0$. Moreover, when $v \leq b$ then

$$\frac{d}{dt}(x - c) \leq -\frac{\gamma}{b}(x - c). \tag{32}$$

Since $x_k \leq c$ then Lemma 1 guarantees that $x(t) \leq c$ for all $t \geq t_k$, and by induction $x(t) \leq c$ for all $t \geq t_0$.

Moreover, it is necessary to show that the control signal does not violate $-\mu \leq u_k \leq \mu$. Rearranging (30), and using (26) gives the following

$$\gamma \left(1 + \frac{\mu T}{b}\left(1 + \frac{\mu}{\gamma}\right)\right) \leq \mu$$

$$\gamma \left(1 + \frac{\alpha c}{b}\right) \leq \mu. \tag{33}$$

From (21), it can be verified that the following inequalities hold

$$\frac{v_k}{h(v_k - b)v_k + (1 - h(v_k - b))b} \leq 1 \tag{34}$$

$$\frac{1}{h(v_k - b)v_k + (1 - h(v_k - b))b} \leq \frac{1}{b}, \tag{35}$$

thus (33) gives

$$\gamma \left(\frac{v_k + \alpha c}{h(v_k - b)v_k + (1 - h(v_k - b))b} \right) \leq \mu. \tag{36}$$

Since $\mathcal{B}(x_k, v_k) \leq c$, (36) thus gives

$$-\mu \leq -\gamma \frac{(v_k + \alpha \mathcal{B}(x_k, v_k))}{h(v_k - b)v_k + (1 - h(v_k - b))b} \tag{37}$$

which shows that $-\mu \leq u_k \leq \mu$. Hence, the system is maintained in the safe set without violating the control limits. ■

The convergence of the state trajectories to the origin is proven in the following theorem.

Theorem 6 (Convergence of the Double Integrator): Let $b > \mu T$, $\alpha \gg T$, and $c = \beta/\alpha$, where β is defined in (26). Let γ be defined as in (30). Then for all $(x_0, v_0) \in \Phi_c$, the feedback law

$$u_k = \min \left\{ \mu, -\gamma \frac{\big(v_k + \alpha \mathcal{B}(x_k, v_k)\big)}{h(v_k - b)v_k + (1 - h(v_k - b))b} \right\} \tag{38}$$

guarantees that the system trajectories of (16)–(17) converge to the origin without leaving the safe set, Φ_c.

Proof: Since the control signal is saturated in a subset of Φ_c, the proof is developed in two main steps. First, we determine the set where the control is saturated at μ. Using (38) we get

$$-\gamma \frac{\big(v_k + \alpha \mathcal{B}(x_k, v_k)\big)}{h(v_k - b)v_k + (1 - h(v_k - b))b} \geq \mu \tag{39}$$

Note that $h(v_k - b)v_k + (1 - h(v_k - b))b \geq 0$. Thus, inequality (39) gives $S(x_k, v_k) \leq 0$, where

$$S(x,v) = \alpha\gamma \mathcal{B}(x,v) + (\gamma + \mu h(v - b))\, v + \\ + (1 - h(v - b))\, \mu b. \tag{40}$$

Note that

$$(\gamma + \mu h(v_k - b))\, v_k + (1 - h(v_k - b))\, \mu b \geq 0. \tag{41}$$

Thus, $S(x_k, v_k) \leq 0$ always satisfies $\mathcal{B}(x_k, v_k) \leq 0$ which means that the following set

$$\Omega = \left\{ (x,v) \in \mathbb{R}^2 : x \leq 0 \ \cap \ S(x,v) \leq 0 \right\} \tag{42}$$

is a subset of Φ_c. Moreover, $S(x,v)$ shows the distance from the border of Ω. Consider the time derivative of $S(x,v)$ along (16)–(17) for $u_k = \mu$

$$\frac{d}{dt}S(x,v) = \gamma\mu + \alpha\gamma v + \left(\alpha\mu v + \mu^2\right) h(v - b) + \\ + \alpha b \mu (1 - h(v - b)). \tag{43}$$

The following holds

$$\frac{d}{dt}S(x,v) = \begin{cases} \alpha\mu(\frac{\gamma}{\mu} + 1)v + \gamma\mu + \mu^2 & v \geq b \\ \alpha\mu(\frac{\gamma}{\mu}\frac{v}{b} + 1)b + \gamma\mu & v < b \end{cases}. \tag{44}$$

The time derivative of $S(x,v)$ is always positive in Ω. Also, Theorem 5 shows that the state trajectory remains in Φ_c. Thus, the state trajectory moves toward $S(x,v) = 0$ until it reaches the following set

$$\Pi = \big\{(x,v) \in \mathbb{R}^2 : \\ x \leq c \ \cap \ \mathcal{B}(x,v) \leq c \ \ \cap \ S(x,v) \geq 0\big\}, \tag{45}$$

where the control input is no longer saturated. In the set Π the control law is given as

$$u_k = -\gamma \frac{\big(v_k + \alpha \mathcal{B}(x_k, v_k)\big)}{h(v_k - b)v_k + (1 - h(v_k - b))b}. \tag{46}$$

In the subsequent analysis we show that $\mathcal{B}(x,v) = 0$ attracts the state trajectories in Π. It is also shown that the state

trajectories converge to the origin. The convergence proof covers the quadratic and linear segments of the barrier certificate.

1) Quadratic segment: The system dynamics for $v_k \geq b$ become

$$\frac{d}{dt}x = v \tag{47}$$

$$\frac{d}{dt}v = -\gamma - \frac{\gamma\alpha}{v_k}\mathcal{B}(x_k, v_k). \tag{48}$$

Note that $v = v_k + u_k\delta \geq b - \mu T > 0$. The time derivative of $\mathcal{B}(x, v)$ for all $t \in [t_k, t_k + T)$ along (47)–(48) equals

$$\begin{aligned}\frac{d}{dt}\mathcal{B}(x, v) &= v\left(1 + \frac{u_k}{\gamma}\right) \\ &= -\alpha\frac{v}{v_k}\mathcal{B}(x_k, v_k)\end{aligned} \tag{49}$$

which shows that $\mathcal{B}(x_k, v_k)$ and its time derivative have different signs. Thus, Theorem 5 and (49) guarantee that the state trajectory moves toward $\mathcal{B}(x, v)=0$ without leaving Φ_c.

If $\mathcal{B}(x_k, v_k) \simeq 0$, then (47)–(48) is simplified to

$$\frac{d}{dt}x = v \tag{50}$$

$$\frac{d}{dt}v = -\gamma. \tag{51}$$

Introduce the following Lyapunov function

$$W = \frac{\gamma}{2}x^2 + \frac{c+1}{2}v^2, \tag{52}$$

where the time derivative of W along (50)–(51) is obtained as

$$\frac{dW}{dt} = (x - c - 1)\gamma v \tag{53}$$

which is negative definite for $v \geq b$ and $x \leq c$. Thus, the state trajectory moves toward the origin in a narrow band around $\mathcal{B}(x, v) = 0$.

2) Linear segment: The system dynamics for $v_k < b$ are given in the following

$$\frac{d}{dt}x = v \tag{54}$$

$$\frac{d}{dt}v = -\frac{\alpha\gamma}{b}S_1(x_k, v_k), \tag{55}$$

where

$$S_1(x_k, v_k) = x_k + \left(\frac{b}{\gamma} + \frac{1}{\alpha}\right)v_k. \tag{56}$$

Consider the following set

$$\begin{aligned}\Sigma = \Big\{&(x, v) \in \mathbb{R}^2 : \\ &S(x, v) > 0 \cap S_1(x, v) < 0 \cap v < b \cap x < 0\Big\}\end{aligned} \tag{57}$$

which is shown in Fig. 2. We have

$$\frac{d}{dt}\mathcal{B}(x, v) = v - v_k - \alpha\mathcal{B}(x_k, v_k), \quad v < b. \tag{58}$$

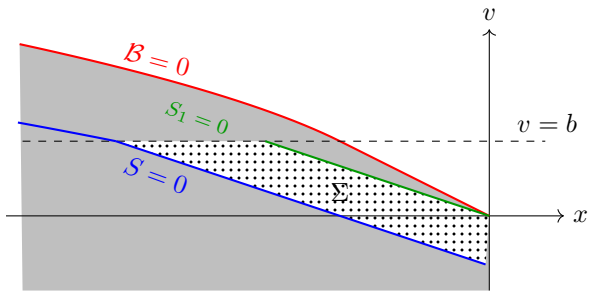

Fig. 2: Barrier certificate is $\mathcal{B} = 0$. The control input saturates in the area below $S = 0$. The dotted area represents the set Σ.

If $(x_k, v_k) \in \Sigma$, then $S_1(x_k, v_k) < 0$ and (55) shows that $v > v_k$. Thus, the time derivative of $\mathcal{B}(x, v)$ is positive which shows that the state trajectory moves toward the barrier.

As the last step, we investigate the evolution of the state trajectories in the triangular area between $S_1(x, v) = 0$, $\mathcal{B}(x, v) = 0$, and $v = b$. Solution of (55) for $t \in [t_k, t_k + T)$ is given as

$$v = v_k - \frac{\alpha\gamma\delta}{b}S_1(x_k, v_k). \tag{59}$$

So, the time derivative of $\mathcal{B}(x, v)$ along (54)–(55) is obtained as

$$\frac{d}{dt}\mathcal{B}(x, v) = -\frac{\alpha(\eta + \delta)}{\eta}S_2(\delta, x_k, v_k), \tag{60}$$

where

$$S_2(\delta, x, v) = x + \left(\eta + \frac{\delta}{\alpha(\eta + \delta)}\right)v, \tag{61}$$

where $\eta = b/\gamma$ and $0 \leq \delta < T$. Also, the following inequality is valid

$$\eta \leq \eta + \frac{\delta}{\alpha(\eta + \delta)} < \eta + \frac{1}{\alpha}. \tag{62}$$

Thus, $S_2(\delta, x, v) = 0$ falls between $S_1(x, v) = 0$ and $\mathcal{B}(x, v) = 0$. Using $b > \mu T$ we get $\eta > (\mu/\gamma)T > T$. Also, assuming that $\alpha \gg T$, $S_2(\delta, x, v) = 0$ is almost identical to $\mathcal{B}(x, v) = 0$. Furthermore, $S_2(\delta, x, v) < 0$ in the triangular area between $v = b$, $S_1(x, v) = 0$, and $\mathcal{B}(x, v) = 0$. Thus, (60) shows that the time derivative of $\mathcal{B}(x, v)$ is positive, meaning that the state trajectory moves toward the barrier. So, $\mathcal{B}(x_k, v_k) \simeq 0$ which implies that $S_1(x_k, v_k) \geq 0$, and thus, (59) shows that $v < v_k$. Hence, the state trajectory moves toward the origin in a narrow band around $x + (b/\gamma)v = 0$ which means that

$$\frac{d}{dt}x = -\frac{\gamma}{b}x, \tag{63}$$

so the position also moves toward the origin. Since the barrier meets $S_1(x, v) = 0$ at the origin, at some point $S_1(x_k, v_k) = 0$ and the system dynamics (54)–(55) show that velocity arrives at zero. Because $S_1(x_k, 0) = x_k$, then position also arrives at zero.

We have shown that within every sample period the state trajectory moves toward the barrier $\mathcal{B}(x, v) = 0$. Thus, as the time progresses, the state trajectories are absorbed by the barrier and afterward converge to the origin. ■

Reducing the sample rate results in increasing γ and expanding the safety region. If the switching point, b, is chosen very close to μT, then γ becomes very close to zero. So, the nonlinear part of $\mathcal{B}(x,v)$ shifts toward the horizontal axis meaning that the safety region is at its minimum size. In contrast, the upper bound of γ increases toward μ as the value of b increases in comparison to μT. Thus, we suggest selecting $b \gg \mu T$. So, $\gamma \simeq \mu$ and the size of the safety region is maximized.

Moreover, α enforces the convergence rate of the system. A combination of a small α and a large μT leads to a large c which results in a large safety buffer. So, the results of Theorem 5 become very conservative. Thus, we suggest the following

$$T \leq \min\left\{\frac{1}{\alpha}, \frac{\alpha}{\mu}\right\} \tag{64}$$

to tune T which guarantees a reasonably small safety buffer.

V. Simulation Results

The safety verification is designed for pilot-based operations. The pilot is allowed to send a command $-\mu \leq u_p \leq \mu$ to the system. It is the responsibility of the safety verification algorithm to guarantee that the system trajectory never leaves the safe set. Thus, the control input is implemented as the following

$$u_k = \max\left\{-\mu, \right.$$
$$\left. \min\left\{u_p, \mu, \frac{-\gamma\big(v_k + \alpha\mathcal{B}(x_k, v_k)\big)}{h(v_k - b)v_k + (1 - h(v_k - b))b}\right\}\right\}. \tag{65}$$

We conduct simulations to show the effectiveness of the proposed safety verification technique with the system parameters designed as the following: $\mu = 2$, $\alpha = 1$, $T = 100$ ms, $b = 2$, and $\gamma = 1.63$.

The pilot generates a state feedback within the allowed control limits to drive the system to the state $(x, v) = (5, 0)$ thereby violating the boundary $x \leq 0$. We run simulations for two scenarios with and without the safety verification (65). When (65) is not in place, the control signal applied to the system equals $\max\{-\mu, \min\{u_p, \mu\}\}$. In the case where the barrier certificate is in place, the control law (65) guarantees that all the initial conditions in Φ_c, where c is given as (26), remain in the safe set. Moreover, all the state trajectories converge to the origin. The phase portrait of the system in both scenarios is shown in Fig. 3. Also, the control signal satisfies $-2 \leq u_k \leq 2$.

VI. Conclusions

We proposed a safety verification technique for systems with input saturation. The results were used to design safety barriers of a double integrator with input saturation and ZOH. The maximum braking power enforces the shape of the barrier. Also, the shape of the barrier and the rate of its variation determine the size of the safety buffer around the safe set. If the sample period is chosen within the prescribed limits, the state trajectories converge to the origin. Moreover,

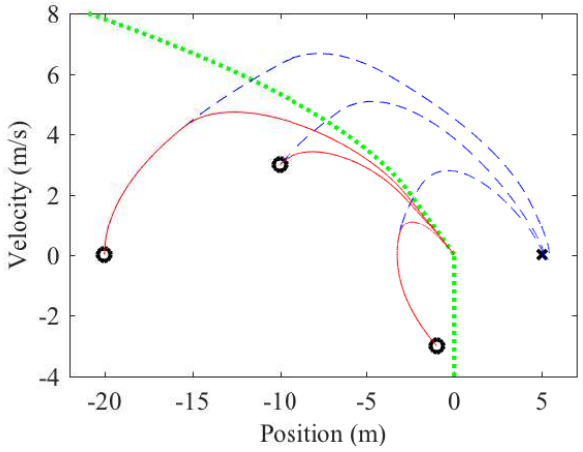

Fig. 3: (dotted green) Barrier certificate. State trajectories with the pilot (dashed blue) without and (solid red) with the safety verification.

we showed that when a pilot is present, the proposed safety verification technique guarantees that the system never leaves the safe set. Two sets of simulations verified the effectiveness of the proposed technique, especially for the case of pilot-based operation.

References

[1] A. D. Ames, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs with application to adaptive cruise control," in *IEEE Conference on Decision and Control*, 2014, pp. 6271–6278.

[2] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, vol. 62, pp. 3861–3876, 2017.

[3] U. Borrmann, L. Wang, A. D. Ames, and M. Egerstedt, "Control barrier certificates for safe swarm behavior," *IFAC-PapersOnLine*, vol. 48, no. 27, pp. 68 – 73, 2015.

[4] K. Ghorbal, A. Sogokon, and A. Platzer, "A hierarchy of proof rules for checking positive invariance of algebraic and semi-algebraic sets," *Computer Languages, Systems & Structures*, vol. 48, pp. 19–43, 2017.

[5] M. Jankovic, "Combining control Lyapunov and barrier functions for constrained stabilization of nonlinear systems," in *American Control Conference*, 2017, pp. 1916–1922.

[6] H. Kong, F. He, X. Song, W. N. N. Hung, and M. Gu, "Exponential-Condition-Based Barrier Certificate Generation for Safety Verification of Hybrid Systems," *ArXiv e-prints*, Mar. 2013.

[7] Y.-J. Liu and S. Tong, "Barrier Lyapunov functions-based adaptive control for a class of nonlinear pure-feedback systems with full state constraints," *Automatica*, vol. 64, pp. 70–75, 2016.

[8] Q. Nguyen and K. Sreenath, "Exponential control barrier functions for enforcing high relative-degree safety-critical constraints," in *American Control Conference*, 2016, pp. 322–328.

[9] S. Prajna and A. Jadbabaie, *Safety Verification of Hybrid Systems Using Barrier Certificates*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 477–492.

[10] D. Ricketts, "Verification of sampled-data systems using Coq," Ph.D. dissertation, University of California, San Diego, 2017.

[11] K. P. Tee, S. S. Ge, and E. H. Tay, "Barrier Lyapunov functions for the control of output-constrained nonlinear systems," *Automatica*, vol. 45, pp. 918–927, 2009.

[12] A. R. Teel, "Global stabilization and restricted tracking for multiple integrators with bounded controls," *Syst. Control Lett.*, vol. 18, no. 3, pp. 165–171, Mar. 1992.

[13] L. Wang, A. Ames, and M. Egerstedt, "Safety barrier certificates for heterogeneous multi-robot systems," in *American Control Conference*, 2016, pp. 5213–5218.

[14] X. Xu, "Control sharing barrier functions with application to constrained control," in *IEEE Conference on Decision and Control*, 2016, pp. 4880–4885.