Control Barrier Functions for Stochastic Systems

Andrew Clark

Abstract

Control Barrier Functions (CBFs) aim to ensure safety by constraining the control input at each time step so that the system state remains within a desired safe region. This paper presents a framework for CBFs in stochastic systems in the presence of Gaussian process and measurement noise. We first consider the case where the system state is known at each time step, and present reciprocal and zero CBF constructions that guarantee safety with probability 1. We extend our results to high relative degree systems with linear dynamics and affine safety constraints. We then develop CBFs for incomplete state information environments, in which the state must be estimated using sensors that are corrupted by Gaussian noise. We prove that our proposed CBF ensures safety with probability 1 when the state estimate is within a given bound of the true state, which can be achieved using an Extended Kalman Filter when the system is linear or the process and measurement noise are sufficiently small. We propose control policies that combine these CBFs with Control Lyapunov Functions in order to jointly ensure safety and stochastic stability. Our results are validated via numerical study on an adaptive cruise control example.

Key words: Safe control; stochastic control; stochastic differential equations.

1 Introduction

Safety, defined as ensuring that the state of a control system remains within a particular region, is an essential property in applications including transportation, medicine, and energy. The need for safety has motivated extensive research into synthesizing and verifying controllers to satisfy safety requirements. Widely-studied methodologies include barrier methods [19], discrete approximations [6,20,15], and reachable set computation [9,1].

Recently, Control Barrier Functions (CBFs) have emerged as a promising approach to ensure safety while maintaining computational tractability [4]. A CBF is a function that either decays to zero (Zero CBF, or ZCBF) or diverges to infinity (Reciprocal CBF, or RCBF) as the state trajectory approaches the boundary of the safe region. Safety of the system can be guaranteed by adding a constraint to the control input, which ensures that the CBF remains finite in the case of RCBF and positive in the case of ZCBF. The CBF approach has been successfully applied to bipedal locomotion [10,17], automotive control [14,5], and UAVs [27]. Furthermore, by composing a CBF with a Control Lyapunov Function (CLF), optimization-based control policies with joint guarantees on safety and stability can be designed.

Existing CBF techniques are applicable to deterministic systems with exact observation of the system state. Many control systems, however, operate in the presence of noise in both the system dynamics and sensor measurements. A CBF framework for stochastic systems would enable computationally tractable control with probabilistic guarantees on safety by making the CBF method applicable to a broader class of systems.

In this paper, we generalize CBF to stochastic systems. We consider complete information systems, in which the exact state is known at each time, as well as incomplete information systems in which only noisy measurements of the state are available. For both cases, we formulate stochastic versions of ZCBF and RCBF, and show that a linear constraint on the control at each time step results in provable safety guarantees. We make the following specific contributions:

• In the complete information case, we formulate ZCBFs and RCBFs and derive sufficient conditions for the system to satisfy safety with probability 1.
• In the incomplete information case, we consider a class of controllers in which the state estimate is obtained via Extended Kalman Filter (EKF). We derive bounds on the probability of violating the safety constraints...
as a function of the estimation error of the filter.

• We derive sufficient conditions for constructing ZCBFs for high relative degree linear systems with affine safety constraints and complete state information.

• We construct optimization-based controllers that integrate stochastic CLFs with CBFs to ensure safety and performance. The controllers solve quadratic programs at each time step and thus can be implemented on embedded systems.

• We evaluate our approach via numerical study on an adaptive cruise control system. We find that both ZCBF and RCBF ensure safety, albeit by following different controller trajectories.

The rest of the paper is organized as follows. Section 3 presents needed background. Section 4 presents CBF constructions in the complete information case. Section 5 considers the incomplete information case. Section 6 presents control policy constructions via stochastic CBFs. Section 7 contains numerical results. Section 8 concludes the paper.

2 Related Work

The CBF method for synthesizing safe controllers was proposed in [3,4]. For a comprehensive survey of recent work on CBFs, see [2]. Composition of CBFs with CLFs for guaranteed safety and stability was proposed in [23]. CBFs have been proposed for input-constrained systems [21], systems with delays [11], self-triggered systems [29], and linearizable systems [28]. Extensions to incorporate signal temporal logic constraints were developed in [13]. A framework for exponential CBFs that enable safety guarantees in high relative-degree systems was proposed in [16]. While the present paper also considers high relative-degree systems, we propose a different approach and, moreover, consider the problem in a stochastic setting.

The problem of verifying safety of a given system and controller has been studied extensively over the past several decades [6,20,8,25,26]. In the verification literature, the approach that is closest to the present work is the barrier function method [18,19]. Barrier certificates provide provable guarantees that a system with given controller does not enter an unsafe region. More recently, a tighter barrier function construction that enables controller synthesis for stochastic systems was proposed in [24].

The preliminary conference version of this paper [7] introduced CBFs for stochastic systems, including what this paper refers to as reciprocal CBFs. The present paper introduces the additional notion of zero CBFs for stochastic systems, as well as methodologies for computing CBFs for high relative degree systems.

3 Background

This section provides background on martingales and stochastic differential equations (SDEs). In what follows, we let \( + = \max \{ \cdot, 0 \} \), \( - = \min \{ \cdot, 0 \} \), \( E(\cdot) \) denote expectation, and \( \text{tr}(\cdot) \) denote the trace operator.

We consider stochastic processes with respect to a probability space \((\Omega, \mathcal{F}, Pr)\), where \(\Omega\) is a sample space, \(\mathcal{F}\) is a \(\sigma\)-field over \(\Omega\), and \(Pr: \mathcal{F} \to [0,1]\) is a probability measure. A filtration \(\{\mathcal{F}_t: t \geq 0\}\) is a collection of sub-\(\sigma\)-fields with \(\mathcal{F}_s \subseteq \mathcal{F}_t \subseteq \mathcal{F}\) for \(0 \leq s < t < \infty\). A stochastic process is adapted to filtration \(\{\mathcal{F}_t\}\) if, for each \(t \geq 0\), \(X_t\) is an \(\mathcal{F}_t\)-measurable random variable.

Definition 1 The random process \(x_t\) is a martingale if \(E(x_t|x_s) = x_s\) for all \(t \geq s\), a submartingale if \(E(x_t|x_s) \geq x_s\) for all \(t \geq s\), and a supermartingale if \(E(x_t|x_s) \leq x_s\) for all \(t \geq s\).

A stopping time is defined as follows.

Definition 2 A random time \(\tau\) is a stopping time of a filtration \(\mathcal{F}_t\) if the event \(\{\tau \leq t\}\) belongs to the \(\sigma\)-field \(\mathcal{F}_t\) for all \(t \geq 0\).

Let \(x_t\) be a submartingale (resp. supermartingale) and let \(\tau\) be a stopping time. If \(t \wedge \tau\) denotes the minimum of \(t\) and \(\tau\), then \(x_{t \wedge \tau}\) is a submartingale (resp. supermartingale), i.e., stopped martingales are martingales. The following result gives bounds on the maximum value of a submartingale.

Theorem 1 (Doob’s Martingale Inequality [12]) Let \(x_t\) be a submartingale, \([t_0, t_1]\) a subinterval of \([0, \infty)\), and \(\lambda > 0\). Then

\[
\lambda Pr \left( \sup_{t_0 \leq t \leq t_1} x_t \geq \lambda \right) \leq E(x_{t_1}^+). \quad (1)
\]

The following result follows directly from Doob’s Martingale Inequality.

Corollary 1 Let \(x_t\) be a supermartingale, \([t_0, t_1]\) a subinterval of \([0, \infty)\), and \(\lambda > 0\). Then

\[
\lambda Pr \left( \inf_{t \in [t_0, t_1]} x_t \leq -\lambda \right) \leq E(x_{t_1}^-) - E(x_{t_0}). \quad (2)
\]

We next define a semimartingale and give a composition result on semimartingales.

Definition 3 A continuous semimartingale \(x_t\) is a stochastic process which has decomposition \(x_t = x_0 + M_t + B_t\) with probability 1, where \(M_t\) is a martingale and \(B_t\) is the difference between two continuous, nondecreasing, adapted processes.
For any stopping time $\tau$ and semimartingale $x_t$, $x_{t\wedge \tau}$ is a semimartingale. The following lemma gives a composition rule for semimartingales.

**Lemma 1 (Itô’s Lemma [12])** Let $f(x, t)$ be a twice-differentiable function and let $x_1$ be a semimartingale. Then $f(x_1)$ is a semimartingale that satisfies

$$f(x_t) = f(x_0) + \int_0^t f'(x_s) \, dM_s + \int_0^t f'(x_s) \, dB_s + \frac{1}{2} \int_0^t f''(x_s) \, d<M>_s$$

with probability 1 for all $t$, where $<M>_s$ denotes the quadratic variation of $M$ at time $s$.

A stochastic differential equation (SDE) in Itô form is defined by

$$dx_t = a(x, t) \, dt + \sigma(x, t) \, dW_t$$

(3)

where $a(x, t)$ and $\sigma(x, t)$ are continuous functions and $W_t$ is a Brownian motion. The dimension of $x_t$ is equal to $n$, while the dimension of $W_t$ is equal to $r$. A strong solution to an SDE is defined as follows.

**Definition 4** A strong solution of SDE (3) with respect to Brownian motion $W_t$ and initial condition $\chi$ is a process $\{x_t \in [0, \infty)\}$ with continuous sample paths and the following properties:

(i) $Pr(x_0 = \chi) = 1$

(ii) For every $1 \leq i \leq n$, $1 \leq j \leq r$, and $t \in [0, \infty)$,

$$Pr \left( \int_0^t |a_i(x_\tau, \tau)| + \sigma_{ij}^2(x_\tau, \tau) \, d\tau \right) = 1.$$

(iii) The integral equation

$$x_t = x_0 + \int_0^t a(x, \tau) \, d\tau + \int_0^t \sigma(x, \tau) \, dW_\tau,$$

where the latter term is a stochastic integral with respect to the Brownian motion $W_t$, holds with probability 1.

Any strong solution of an SDE is a semimartingale. For such strong solutions, if $f(x, t)$ is a twice differentiable function, then Itô’s Lemma reduces to

$$dx_t = \left( \frac{\partial f}{\partial t} + \frac{\partial f}{\partial x} a(x, t) + \frac{1}{2} \text{tr} \left( \sigma(x, t)^T \frac{\partial^2 f}{\partial x^2} \sigma(x, t) \right) \right) \, dt$$

$$+ \left( \frac{\partial f}{\partial x} \sigma(x, t) \right) \, dW_t$$

(4)

## 4 Complete-Information CBFs

This section presents our construction of control barrier functions for stochastic systems where the controller has complete state information. We first present the problem statement, followed by constructions of reciprocal and zero CBFs.

### 4.1 Problem Statement

We consider a system with time-varying state $x_t \in \mathbb{R}^n$ and control input $u_t \in \mathbb{R}^m$. The state $x_t$ follows the SDE

$$dx_t = (f(x_t) + g(x_t)u_t) \, dt + \sigma(x_t) \, dW_t$$

(5)

where $f : \mathbb{R}^n \to \mathbb{R}^n$, $g : \mathbb{R}^n \to \mathbb{R}^{n \times m}$, and $\sigma : \mathbb{R}^n \to \mathbb{R}^n$ are locally Lipschitz continuous functions and $W_t$ is a Brownian motion. We assume that (5) has a strong solution for any control signal $u_t$.

The system is required to satisfy a safety constraint for all time $t$, which is expressed as $x_t \in \mathcal{C}$ for all $t$ where $\mathcal{C}$ is a safe operating region. The set $\mathcal{C}$ is defined by a locally Lipschitz function $h : \mathbb{R}^n \to \mathbb{R}$ as

$$\mathcal{C} = \{ x : h(x) \geq 0 \}, \quad \partial \mathcal{C} = \{ x : h(x) = 0 \}.$$

**Problem studied:** How to design a control policy that maps the sequence $\{x_t \in [0, t]\}$ to an input $u_t$ such that $x_t \in \mathcal{C}$ for all $t$ with maximal probability?

### 4.2 Reciprocal Control Barrier Function Construction

We present our first stochastic CBF construction, which is a reciprocal CBF (RCBF) analogous to [4].

**Definition 5** Let $x_t$ be a stochastic process described by (5). A reciprocal CBF is a function $\alpha : \mathbb{R}^n \to \mathbb{R}$ that is locally Lipschitz, twice differentiable on $\text{int}(\mathcal{C})$, and satisfies the following properties:

1. There exist class-K functions $\alpha_1$ and $\alpha_2$ such that

$$\frac{1}{\alpha_1(h(x))} \leq B(x) \leq \frac{1}{\alpha_2(h(x))}$$

(6)

for all $x \in \text{int}(\mathcal{C})$.

2. For all $x \in \text{int}(\mathcal{C})$, there exists $u \in \mathbb{R}^m$ such that

$$\frac{\partial B}{\partial x} (f(x) + g(x)u) + \frac{1}{2} \text{tr} \left( \sigma(x)^T \frac{\partial^2 B}{\partial x^2} \sigma(x) \right) \leq \alpha_3(h(x))$$

(7)
In the deterministic case [4], the reciprocal CBF construction ensures that $B(x) \sim \frac{1}{x^\tau}$, and hence $B(x)$ tends to infinity as the system state approaches the boundary of the safe region $C$. Definition 5 extends this approach to the stochastic case by providing sufficient conditions for the system to remain bounded in expectation, and hence almost surely finite, as shown by the following theorem.

**Theorem 2** Suppose that there exists an RCBF $B$ for a controlled stochastic process $x_t$ described by (5), and at each time $t$, $u_t$ satisfies (7). Then for all $t$, $Pr(x_t \in C) = 1$, provided that $x_0 \in C$.

**Proof:** Let $B$ be a RCBF and define $B_t = B(x_t)$. Since each sample path of $x_t$ is continuous, each sample path of $B_t$ is continuous. Hence, if $x_t \notin C$ for some $t$, then there exists $t' < t$ such that $h(x_{t'}) = 0$ and thus $B_t \to \infty$ by (6). As a result, if for all $t > 0$ and for all $\delta \in (0,1)$, we have

$$Pr\left(\sup_{t < t'} B_t = \infty\right) < \delta,$$

then $Pr(x_t \in C) = 1$ for all $t$. Equivalently, $Pr(x_t \in C) = 1$ for all $t$ if, for all $t > 0$ and $\delta \in (0,1)$, we can construct $K$ such that $Pr(\sup_{t < t'} B_t \to \infty \leq Pr(\sup_{t < t'} B_t > K) < \delta$.

We construct such a $K$ as follows. Let $L = B_0$, and choose $K$ such that

$$K > \frac{L + t\alpha_3(\alpha_2^{-1}\left(\frac{1}{L}\right))}{\delta}.$$

Define stopping time $\beta$ as $\beta = \inf\{t : B_t = 2K\}$. We have that $x_{t\wedge \beta}$ is a semimartingale and $x_{t\wedge \beta} \in \text{int}(C)$ for all $t$. The function $B(x)$ is twice differentiable on int$(C)$, and therefore for any $x$ in a sample path of $x_{t\wedge \beta}$. Hence we can apply Itô’s Lemma to obtain

$$B_{t\wedge \beta} = B_0 + \int_0^{t\wedge \beta} \left[\frac{\partial B}{\partial x}(f(x_\tau) + g(x_\tau)u_\tau) + \frac{1}{2}\text{tr}\left(\sigma(x_\tau)^T\frac{\partial^2 B}{\partial x^2}\sigma(x_\tau)\right)\right] d\tau + \int_0^{t\wedge \beta} \frac{\partial B}{\partial x}\sigma(x_\tau) dW_\tau$$

with probability 1. We construct a sequence of stopping times $\eta_i$ and $\zeta_i$ as

$$\eta_0 = 0, \zeta_0 = \inf\{t : B_t < L\}$$

$$\eta_i = \inf\{t : B_t > L, t > \zeta_{i-1}\}, i = 1, 2, \ldots$$

$$\zeta_i = \inf\{t : B_t < L, t > \eta_i\}, i = 1, 2, \ldots$$

The times $\eta_i$ and $\zeta_i$ are the up- and down-crossings of $B_t$ over $L$. Define a random process $\tilde{B}_t$ by

$$\tilde{B}_t = L + \sum_{i=0}^{\infty} \left[\int_{\eta_i}^{\zeta_i} \alpha_3(\alpha_2^{-1}\left(\frac{1}{L}\right)) d\tau + \int_{\eta_i}^{\zeta_i} \frac{\partial B}{\partial x}\sigma(x_\tau) dW_\tau\right]$$

We will show that, for any sample path where (9) holds, we have $B_{t\wedge \beta} \leq \tilde{B}_{t\wedge \beta}$, or equivalently, $B_{t\wedge \beta} \leq \tilde{B}_{t\wedge \beta}$ with probability 1. The proof is by induction. At time $t = 0$, $B_0 = \tilde{B}_0 = L$. For $t \in [\eta_i, \zeta_i]$,

$$B_t = B_{\eta_i} + \int_{\eta_i}^{t} \left[\frac{\partial B}{\partial x}(f(x_\tau) + g(x_\tau)u_\tau) + \frac{1}{2}\text{tr}\left(\sigma(x_\tau)^T\frac{\partial^2 B}{\partial x^2}\sigma(x_\tau)\right)\right] d\tau + \int_{\eta_i}^{t} \frac{\partial B}{\partial x}\sigma(x_\tau) dW_\tau$$

(12)

By induction, $B_{\eta_i} \leq \tilde{B}_{\eta_i}$. The third terms of (12) and (13) are equal. It remains to show that the second term of (12) is a lower bound on the second term of (13). By definition of $\eta_i$, $B_{\eta_i} \geq L$ for all $\tau \in [\eta_i, t]$, or equivalently, $\frac{1}{B_{\eta_i}} \leq \frac{1}{B_t}$. By Eq. (6), $B_t \leq \frac{1}{\alpha_2(h(x_\tau))}$, and hence $\alpha_2(h(x_\tau)) \leq \frac{1}{B_t}$ and $h(x_\tau) \leq \alpha_2^{-1}\left(\frac{1}{B_t}\right)$. Thus $h(x_\tau) \leq \alpha_2^{-1}\left(\frac{1}{L}\right)$ and $\alpha_3(h(x_\tau)) \leq \alpha_3(\alpha_2^{-1}\left(\frac{1}{L}\right))$. Combining these inequalities with (7), we obtain

$$\frac{\partial B}{\partial x}(f(x_\tau) + g(x_\tau)u_\tau) + \frac{1}{2}\text{tr}\left(\sigma(x_\tau)^T\frac{\partial^2 B}{\partial x^2}\sigma(x_\tau)\right) \leq \alpha_3\left(\alpha_2^{-1}\left(\frac{1}{L}\right)\right),$$

and therefore the integrand of the second term of (12) is a lower bound on the integrand of the second term of (13). In particular, $L = B_{\zeta_i} \leq \tilde{B}_{\zeta_i}$.

For $t \in [\zeta_i, \eta_{i+1}]$,

$$\tilde{B}_t = L + \sum_{j=0}^{i} \left[\int_{\eta_j}^{\eta_{j+1}} \alpha_3(\alpha_2^{-1}\left(\frac{1}{L}\right)) d\tau + \int_{\eta_j}^{\eta_{j+1}} \frac{\partial B}{\partial x}\sigma(x_\tau) dW_\tau\right]$$

$$= \tilde{B}_{\eta_{i+1}} \geq L \geq B_t$$

by definition of $\eta_i$ and $\zeta_i$. Hence $B_t \leq \tilde{B}_t$ for all $t$ almost surely. As a corollary, $B_{t\wedge \beta} \leq \tilde{B}_{t\wedge \beta}$ almost surely, and
we have

\[
Pr \left( \sup_{t' \in [0,t]} B_{t'} > K \right) = Pr \left( \sup_{t' \in [0,t]} B_{t' \wedge \beta} > K \right) \quad (14)
\]

\[
\leq Pr \left( \sup_{t' \in [0,t]} \tilde{B}_{t'} > K \right)
\]

Eq. (14) holds since \( B_t = B_{t \wedge \beta} \) when \( t < \beta \), and hence, if \( \tilde{B}_{t'} > K \) for some \( t' < t \), then \( \tilde{B}_{t' \wedge \beta} > K \). It therefore suffices to prove that \( Pr(\sup_{t' < t} \tilde{B}_{t' \wedge \beta} > K) < \delta \). We first show that \( \tilde{B}_t \) is a submartingale. We have

\[
E(\tilde{B}_t | \tilde{B}_s) = \tilde{B}_s + E \left[ \sum_{i=0}^{\xi_1 \wedge t} \alpha_3 (\alpha_2^{-1}(1/\ell)) \right] d\tau + \int_{\eta_1 \wedge t}^{\xi_1 \wedge t} \partial B_{\sigma(\tau)} dW_{\tau} \]

\[
= \tilde{B}_s + E \left[ \sum_{i=0}^{\xi_1 \wedge t} \alpha_3 (\alpha_2^{-1}(1/\ell)) \right] \geq \tilde{B}_s
\]

implying that \( \tilde{B}_t \) is a submartingale.

Doob’s Martingale Inequality (Theorem 1) then yields

\[
KPr \left( \sup_{\tau \in [0,t]} \tilde{B}_{t \wedge \beta} > K \right) \leq E(\tilde{B}_{t \wedge \beta}) \leq L + \alpha_3 (\alpha_2^{-1}(1/\ell)) \leq L + t \alpha_3 (\alpha_2^{-1}(1/\ell)).
\]

Rearranging terms and using the choice of \( K \) implies that

\[
Pr \left( \sup_{\tau \in [0,t]} B_{t \wedge \beta} > K \right) < \delta,
\]

as desired. \( \square \)

Theorem 2 implies that, by choosing \( u_t \) at each time \( t \) to satisfy (7), safety is guaranteed with probability 1.

4.3 Zero Control Barrier Function Construction

An alternative construction for CBFs is the zero-CBF (ZCBF). The idea of the zero-CBF is to ensure that the function \( h(x_i) \) remains positive, instead of ensuring that a barrier function \( B(x_i) \sim \frac{1}{h(x_i)} \) is finite. The advantage of this approach is that the CBF remains well-defined even outside the region \( C \) [2]. In what follows, we present a zero-CBF construction for stochastic systems that generalizes the construction in the deterministic case by using the Ito derivative instead of the Lie derivative. The zero-CBF is defined as follows.

**Definition 6** The function \( h(x) \) serves as a zero-CBF for a system described by SDE (5) if for all \( x \) satisfying \( h(x) > 0 \), there is a \( u \) satisfying

\[
\frac{\partial h}{\partial x}(f(x) + g(x)u) + \frac{1}{2} \text{tr} \left( \sigma \partial^2 h \partial^2 \sigma \right) \geq -h(x) \quad (15)
\]

We next state the main result on safety via zero-CBFs.

**Theorem 3** For any time \( t \), if \( u_t \) satisfies (15) for all \( t' \leq t \), then \( \Pr(x_t \in C \forall t' < t) = 1 \), provided \( x_0 \in C \).

**Proof:** Our approach is to show that, for any \( t > 0 \), any \( \epsilon > 0 \), and any \( \delta \in (0,1) \),

\[
Pr \left( \inf_{t' < t} h(x_{t'}) < -\epsilon \right) < \delta.
\]

Let \( \theta = \min \{ \frac{\delta}{2t}, h(x_0) \} \). By Itô’s Lemma, we have \( h(x_i) \) is given by

\[
h(x_i) = h(x_0) + \int_0^t \frac{\partial h}{\partial x}(f(x_\tau) + g(x_\tau)u) + \frac{1}{2} \text{tr} \left( \sigma(x_\tau) \partial^2 h \sigma(x_\tau) \right) d\tau + \int_0^t \sigma(x_\tau) \frac{\partial h}{\partial x} dW_\tau \]

We construct a sequence of stopping times \( \eta_i \) and \( \zeta_i \) for \( i = 0, 1, \ldots \) as

\[
\eta_0 = 0, \quad \zeta_0 = \inf \{ t : h(x_t) > \theta \}
\]

\[
\eta_i = \inf \{ t : h(x_t) < \theta, t > \zeta_{i-1}, i = 1, 2, \ldots \}
\]

\[
\zeta_i = \inf \{ t : h(x_t) > \theta, t > \eta_{i-1}, i = 1, 2, \ldots \}
\]

The stopping times \( \eta_i \) and \( \zeta_i \) are the down- and up-crossings of \( h(x_i) \) over \( \theta \), respectively. Define a random process \( U_t \) as follows. Let \( U_0 = \theta \), and let \( U_t \) be given by

\[
U_t = U_0 + \sum_{i=0}^{\infty} \left[ \int_{\eta_i \wedge t}^{\zeta_i \wedge t} \frac{\partial h}{\partial x} dW_\tau - \theta d\tau \right] \leq U_s
\]

We have that \( U_t \) is a semimartingale. Furthermore, we have

\[
E(U_t | U_s) = U_s + \text{E} \left[ \sum_{i=0}^{\infty} \int_{\eta_i \wedge t}^{\zeta_i \wedge t} -\theta d\tau \right] \leq U_s
\]
and therefore \( U_t \) is a supermartingale.

We will first prove by induction that \( h(x_t) \geq U_t \) and \( U_t \leq \theta \). Initially, \( U_0 = \theta < h(x_0) \) by construction. Suppose the result holds up to time \( t \in [\eta_i, \zeta_i] \) for \( i \geq 0 \). Then the first term of (16) is an upper bound on the first term of (17) and the third terms are equal. For \( t \in [\eta_i, \zeta_i] \), the first terms of (18) and (19) are equal. Since \( \zeta_i \) for \( t \) for \( \eta_i \), \( \zeta_i \), \( \phi \) gives \( \bar{U}_t \) and \( \theta_t = \theta/t \), we have \( \mathbf{E}(U_t^\theta) \leq \theta \). Combining these yields

\[
\mathbf{E}(U_t^\theta) \leq \theta t - \theta + \theta = \theta.
\]

We therefore have

\[
\Pr \left( \inf_{\nu < t} h(x_{\nu}) < -\epsilon \right) \leq \Pr \left( \inf_{\nu < t} U_{\nu} < -\epsilon \right) \leq \frac{\theta t}{\epsilon} \leq \frac{\delta \epsilon t}{2t^2} < \delta,
\]

completing the proof. \( \square \)

### 4.4 High-Degree Systems

The safety guarantees of the preceding section rely on the existence of a control input satisfying (15) at each time \( t \). In order for (15) to hold, we must have \( \frac{\partial h}{\partial x} g(x) \neq 0 \). In systems with high relative degree, however, it may be the case that \( \frac{\partial h}{\partial x} g(x) = 0 \) for some \( x \), potentially preventing the system from satisfying (15) and rendering the safety guarantees inapplicable. In what follows, we propose an approach to constructing ZCBFs for such high-degree systems. We develop our approach for linear systems with \( f(x) = Fx \) and \( g(x) = G \) for some matrices \( F \) and \( G \), and for which the function \( h(x) = a^T x - b \) for some \( a \in \mathbb{R}^n \) and \( b \in \mathbb{R} \). We assume that the system is controllable, and hence \( a^T F G \neq 0 \) for some \( i \). We let \( r = \min \{ i : a^T F_i G \neq 0 \} \).

We define a set of functions \( h_i(x) \) for \( i = 0, \ldots, r \) as \( h_0(x) = h(x) \),

\[
h_{i+1}(x) = \frac{\partial h_i}{\partial x} f(x) + \frac{1}{2} \text{tr} \left( \sigma^T \frac{\partial^2 h_i}{\partial x^2} \sigma \right) + h_i(x).
\]

Define \( C_i = \{ x : h_i(x) \geq 0 \} \). The following lemma describes the structure of these functions.

**Lemma 2** The function \( h_i(x) \) can be written in the form

\[
h_i(x) = \sum_{r_0, \ldots, r_{i-1} = 0}^{r_i} \beta_i^{r_0, \ldots, r_{i-1}} (a^T F^0 x)^{r_0} \cdots (a^T F^{i-1} x)^{r_{i-1}} + a^T F^i x
\]

for some values of the coefficients \( \beta_i^{r_0, \ldots, r_{i-1}} \).

**Proof:** The proof is by induction on \( i \). When \( i = 0 \), the function can be written in the form \( h_i(x) = a^T F^0 x - b \), i.e., \( \beta_0^{0} = -b \) and all other values of \( \beta_0^{r_0} \) are zero.
Inducting on $i$, we can then write

$$h_i(x) = z_i(x) + a^T F^i x$$

$$\frac{\partial h_i}{\partial x} = \sum_{j=0}^{i-1} \theta_{ij}(x)a^T F^j + a^T F^i$$

$$\frac{\partial^2 h_i}{\partial x^2} = \sum_{j=0}^{i} \sum_{l=0}^{i} \zeta_{ijl}(x)(F^j)^T aa^T F^l$$

where the functions $z_i(x)$, $\theta_{ij}(x)$, and $\zeta_{ijl}(x)$ are polynomial in $(a^T F^j(x))$ for $j = 0, \ldots, (i-1)$. We therefore have

$$h_{i+1}(x) = \left( \sum_{j=0}^{i-1} \theta_{ij}(x)a^T F^j + a^T F^i \right) F x$$

$$+ \frac{1}{2} \text{tr} \left( \sigma^T \left( \sum_{j=0}^{i} \sum_{l=0}^{i} \zeta_{ijl}(x)(F^j)^T aa^T F^l \right) \sigma \right) + h_i(x)$$

$$= \sum_{j=0}^{i-1} \theta_{ij}(x)a^T F^{j+1} x + a^T F^{i+1} x$$

$$+ \frac{1}{2} \sum_{j=0}^{i} \sum_{l=0}^{i} \zeta_{ijl}(x) \text{tr}(\sigma^T (F^j)^T aa^T F^l \sigma) + h_i(x)$$

Hence $h_{i+1}(x)$ is polynomial in $(a^T F^0 x), \ldots, (a^T F^{i+1} x)$. Furthermore, all terms except $a^T F^{i+1} x$ do not contain any powers of $(a^T F^{i+1} x)$, completing the proof. $\Box$

By the preceding lemma, we have, for any $x \in \mathcal{C} \equiv \bigcap_{i=0}^{r} \mathcal{C}_i$,

$$\frac{\partial h_i}{\partial x} Gu = \begin{cases} 0, & i < r \\ a^T F^i Gu, & i = r \end{cases}$$

We are now ready to state the safety result for high degree systems.

**Theorem 4** If $x_0 \in \bigcap_{i=0}^{r} \mathcal{C}_i$ and

$$\frac{\partial h_r}{\partial x} g(x) u \geq -\frac{\partial h_r}{\partial x} f(x) - \frac{1}{2} \text{tr} \left( \sigma^T \frac{\partial^2 h_r}{\partial x^2} \sigma \right) - h_r(x)$$

for all $t$, then $Pr(|x_t| > \mathcal{C}) = 1$. In particular, $x_t$ satisfies the safety constraint $\{h(x_t) > 0\}$ with probability 1.

**Proof:** The proof is by backwards induction on $i$. For $i = r$, we have that $x_t \in \mathcal{C}_r$ for all $t$ with probability 1 by Theorem 3. For $\mathcal{C}_r$, assuming $x_{t'} \in \mathcal{C}_r$ for all $t' < t$ with probability 1, we have $h_i(x_{t'}) > 0$ for all $t' < t$. Hence (15) holds for the 2CBF $h_{i-1}(x)$. By Theorem 3, $h_{i-1}(x_t) > 0$ with probability 1, and therefore $x_t \in \mathcal{C}_{i-1}$ for all $t$ with probability 1. $\Box$

### 5 Incomplete Information CBFs

This section presents CBF techniques for ensuring stability of stochastic systems with incomplete information due to noisy measurements. We first give the problem statement, followed by reciprocal and zero CBF constructions.

#### 5.1 Problem Statement

We consider a system with time-varying state $x_t \in \mathbb{R}^n$, a control input $u_t \in \mathbb{R}^m$, and output $y_t \in \mathbb{R}^p$ described by the SDEs

$$dx_t = (f(x_t) + g(x_t)u_t) dt + \sigma_t dV_t$$

$$dy_t = cx_t dt + \nu_t dW_t$$

where $V_t$ and $W_t$ are Brownian motions, $c$ is a $p \times n$ matrix, and $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ and $g : \mathbb{R}^n \rightarrow \mathbb{R}^m$ are locally Lipschitz continuous functions. Define $f(x, u) = f(x) + g(x)u$. We first define uniform detectability as follows.

**Definition 7** The pair $[\frac{\partial f}{\partial x}(x, u)]$ is uniformly detectable if there exists a bounded, matrix-valued function $\Lambda(x)$ and a real number $\rho > 0$ such that

$$w^T \left( [\frac{\partial f}{\partial x}(x, u)] + \Lambda(x) c \right) w \leq -\rho \|w\|^2$$

for all $w, z, \text{ and } x$.

We make the following additional assumptions on the system dynamics.

**Assumption 1** The SDEs (22) and (23) satisfy:

1. There exist constants $g, r \in \mathbb{R}_{\geq 0}$ such that $E(\sigma_t \sigma_t^T) \geq gI$ and $E(\nu_t \nu_t^T) \geq rI$ for all $x$ and $t$.
2. The pair $[\frac{\partial f}{\partial x}(x, u), c]$ is uniformly detectable.
3. Let $\phi$ be defined by

$$\bar{f}(x, u) - f(\hat{x}, u) = \frac{\partial f}{\partial x}(x - \hat{x}) + \phi(x, \hat{x}, u).$$

Then there exist real numbers $k_\phi$ and $\epsilon_\phi$ such that

$$||\phi(x, \hat{x}, u)|| \leq k_\phi ||x - \hat{x}||_2$$

for all $x$ and $\hat{x}$ satisfying $||x - \hat{x}||_2 \leq \epsilon_\phi$.

We further assume that the initial state $x_0$ is known.

The safety condition is defined as in Section 4.1. In the incomplete information case, the problem studied is stated as, For given $\epsilon \in (0, 1)$, how to design a control policy
that maps the sequence \( \{y_t : t' \in [0, t]\} \) to an input \( u_t \) at each time \( t \) such that \( \Pr(x_t \in \mathcal{C}) \forall t \geq (1 - \epsilon)^2 \)? In other words, how to ensure that the system remains safe with a given probability \( (1 - \epsilon) \)?

Our CBF approaches are in two parts. First, we compute an estimate of the system state and construct a safe region for the estimated state based on the accuracy of the estimator. Second, we show that the problem reduces to a complete-information stochastic SDE on the estimated state value and apply the approaches developed in Section 4.

We use the Extended Kalman Filter (EKF) [22] as a state estimator. Let \( \hat{x}_t \) denote the estimated value of \( x_t \), and define matrix \( A_t \) by

\[
A_t = \frac{\partial T}{\partial x}(\hat{x}_t, u_t).
\]

Let \( R_t \) be equal to the solution to the Riccati differential equation

\[
dP_t = A_tP_t + P_tA_t^T + Q_t - Pt_v^TR_t^{-1}c_tP_t.
\]

The EKF estimator is defined by the SDE

\[
dx_t = f(\hat{x}_t, u_t) dt + K_t(dy_t - c\hat{x}_t dt).
\]

The following result describes the stability and accuracy of the EKF.

**Proposition 1** Suppose that the conditions of Assumption 1 hold. There exists \( \delta > 0 \) such that \( \sigma_i \sigma_i^T \leq \delta I \) and \( \nu_i \nu_i^T \leq \delta I \), for any \( \epsilon > 0 \), there exists \( \gamma > 0 \) with

\[
\Pr\left(\sup_{t \geq 0} \|x_t - \hat{x}_t\|_2 \leq \gamma\right) \geq 1 - \epsilon.
\]

Proposition 1 implies that, if the level of noise is sufficiently small, then the EKF is stochastically stable. We make two remarks on Proposition 1. First, the accuracy guarantees of the EKF do not depend on the magnitude of the control input \( u_t \). Second, if the system is highly nonlinear, then the constant \( \delta > 0 \) may be small [22], rendering the results inapplicable. In the sequel, we assume that the conditions of Proposition 1 hold, noting that, for example, \( \delta = \infty \) for any detectable LTI systems [22].

Define

\[
\overline{h}_\gamma = \sup \{h(x) : \|x - x^0\|_2 \leq \gamma \text{ for some } x^0 \in h^{-1}(\{0\})\}.
\]

The following lemma gives a sufficient condition for safety of the incomplete information system.

**Lemma 3** If \( \|x_t - \hat{x}_t\|_2 \leq \gamma \) for all \( t \) and \( h(\hat{x}_t) > \overline{h}_\gamma \) for all \( t \), then \( x_t \in \mathcal{C} \) for all \( t \).

**Proof:** Suppose that \( x_t \notin \mathcal{C} \) for some \( t \). Since each sample path of \( x_t \) is continuous, we must have \( h(x_t) = 0 \) for some \( \tau \in [0, t] \). By assumption, \( \|x_t - x_{\tau}\|_2 \leq \gamma \), i.e., \( \hat{x}_t \in B(x_{\tau}, \gamma) \). Since \( x_{\tau} \in h^{-1}(\{0\}) \), we have

\[
h(\hat{x}_t) < \sup \{h(x) : \|x - x_{\tau}\|_2 \leq \gamma\}
\]

\[
\leq \sup \{h(x) : \|x - x^0\|_2 \leq \gamma \text{ for some } x^0 \in h^{-1}(\{0\})\} = \overline{h}_\gamma.
\]

This contradicts the assumption that \( h(\hat{x}_t) > \overline{h}_\gamma \) and hence we must have \( x_t \in \mathcal{C} \) for all \( t \). \( \Box \)

Combining Proposition 1 and Lemma 3, we have that it suffices to select \( \gamma \) such that \( \|x_t - \hat{x}_t\|_2 \) is bounded by \( \gamma \) with probability \( (1 - \epsilon) \), and then design a control law such that \( h(\hat{x}_t) > \overline{h}_\gamma \) for all \( t \).

### 5.2 Reciprocal CBF Approach

The RCBF for incomplete information systems is described as follows.

**Theorem 5** Suppose that the conditions of Proposition 1 are satisfied and there exists a function \( B : \mathbb{R}^n \to \mathbb{R} \) and class-K functions \( \alpha_1, \alpha_2, \alpha_3 \) such that

\[
\frac{1}{\alpha_1(h(x))} \leq B(x) \leq \frac{1}{\alpha_2(h(x))} \quad (26)
\]

\[
\frac{\partial B}{\partial x}(\hat{x}_t, u_t) + \gamma \|\frac{\partial B}{\partial x}K_t\|_2 + \frac{1}{2} \text{tr} \left( \nu_t K_t^T \frac{\partial^2 B}{\partial x^2} K_t \nu_t \right) \leq \alpha_3(h(\hat{x}_t)) \quad (27)
\]

and \( \gamma \) satisfies (25) for some \( \epsilon > 0 \). \( \Pr(x_t \in \mathcal{C}) \forall t \geq (1 - \epsilon) \) if \( h(x_0) > 0 \).

**Proof:** Our approach is to show that \( \hat{h}(\hat{x}_t) \geq 0 \) for all \( t \) if \( \|x_t - \hat{x}_t\|_2 \leq \gamma \) for all \( t \). Combining Eqs. (23) and (24), we have

\[
dx_t = f(\hat{x}_t, u_t) dt + K_t(c x_t dt + \nu_t dW_t - c \hat{x}_t dt)
\]

\[
= f(\hat{x}_t, u_t) + K_t(c (x_t - \hat{x}_t)) dt + K_t \nu_t dW_t
\]

Define \( B_t = B(\hat{x}_t) \). Hence

\[
dB_t = \left( \frac{\partial B}{\partial x}(\hat{x}_t, u_t) + K_t c(x_t - \hat{x}_t) \right)
\]

\[
+ \frac{1}{2} \text{tr} \left( \nu_t K_t^T \frac{\partial^2 B}{\partial x^2} K_t \nu_t \right) \quad dt + \frac{\partial B}{\partial x} K_t \nu_t dW_t \quad (28)
\]

If \( \|x_t - \hat{x}_t\|_2 \leq \gamma \), then

\[
\frac{\partial B}{\partial x} K_t c(x_t - \hat{x}_t) \leq \|\frac{\partial B}{\partial x} K_t c\|_2 \|x_t - \hat{x}_t\|_2 \leq \gamma \|\frac{\partial B}{\partial x} K_t c\|_2.
\]
Theorem 5 implies that, if the parameter $\gamma$ serves safety. This constraint is linear in $u$ such that the estimation error remains bounded by with sufficient probability, then selecting a control input $u$ satisfying $P_r(h(\hat{x}_t)) \geq 0 \forall t = 1$ by Theorem 2. Hence, by Lemma 3, $Pr(h(\hat{x}_t)) \geq 0 \forall t||x_t - \hat{x}_t||2 \geq \gamma \forall t = 1$, and so $Pr(h(x_t)) \geq 0 \geq 1 - \epsilon$. °

Theorem 5 implies that, if the parameter $\gamma$ is chosen such that the estimation error remains bounded by $\gamma$ with sufficient probability, then selecting a control input $u_t$ at each time $t$ such that (27) holds is sufficient to ensure safety. This constraint is linear in $u_t$, and all other parameters can be evaluated based on the noise characteristics and system and Kalman filter matrices.

5.3 Zero CBF Construction

The following definition describes the zero CBF in the incomplete information case.

**Definition 8** The function $\hat{h}(x)$ serves as a zero CBF for an incomplete-information system described by (22) and (25) if for all $x$ satisfying $\hat{h}(x) > 0$, there exists $u$ satisfying

$$\frac{\partial \hat{h}}{\partial x}g(x)u \geq -\frac{\partial \hat{h}}{\partial x}f(\hat{x}_t) + \frac{\partial \hat{h}}{\partial x}K_t c||2\gamma$$

$$-\frac{1}{2} \text{tr} \left( \sigma^T \frac{\partial^2 \hat{h}}{\partial x^2} \sigma \right) - \hat{h}(\hat{x}_t) \tag{29}$$

The following theorem describes the safety guarantees of the incomplete-information ZCBF.

**Theorem 6** Suppose that $x_0$ satisfies $\hat{h}(x_0) > 0$ and, at each time $t$, $u_t$ satisfies (29). If the conditions of Proposition 1 are satisfied, then $Pr(x_t \in C \forall t) \geq (1 - \epsilon)$.

**Proof:** Our approach is to show that $\hat{h}(\hat{x}_t) > 0$ for all $t$ when $||x_t - \hat{x}_t||2 \leq \gamma$, and hence safety is satisfied with probability at least $(1 - \epsilon)$ by Lemma 3. The dynamics of $\hat{x}_t$ are given by the SDE (22). Note that

$$-\frac{\partial \hat{h}}{\partial x}K_t c(x_t - \hat{x}_t) \leq ||\frac{\partial \hat{h}}{\partial x}K_t c||2||x_t - \hat{x}_t||2 \leq ||\frac{\partial \hat{h}}{\partial x}K_t c||2\gamma. \tag{30}$$

We then have

$$\frac{\partial \hat{h}}{\partial x}(f(\hat{x}_t) + K_t c(x_t - \hat{x}_t)) - \frac{1}{2} \text{tr} \left( \sigma^T \frac{\partial^2 \hat{h}}{\partial x^2} \sigma \right) \tag{31}$$

$$\leq -\frac{\partial \hat{h}}{\partial x}f(\hat{x}_t) + ||\frac{\partial \hat{h}}{\partial x}K_t c||2\gamma - \frac{1}{2} \text{tr} \left( \sigma^T \frac{\partial^2 \hat{h}}{\partial x^2} \sigma \right) \tag{32}$$

$$\leq \frac{\partial \hat{h}}{\partial x^2}c h(\hat{x}_t)u_t \tag{33}$$

where (32) follows from (30) and (33) follows from (29). Hence, by Theorem 3, we have $h(\hat{x}_t) > 0$ for all $t$ if $||x_t - \hat{x}_t||2 \leq \gamma$ for all $t$, and thus $Pr(h(x_t) > 0 \forall t) \geq (1 - \epsilon)$. °

6 CBF-Based Control Policies

In what follows, we describe control policies that use stochastic CBFs to provide provable safety guarantees. We consider a case where the goal of the system is to minimize the expected value of a positive-definite quadratic objective function

$$V_t(x_t, u_t) = \begin{pmatrix} x_t \\ u_t \end{pmatrix}^T \begin{pmatrix} Q_t & S_t \\ S_t^T & R_t \end{pmatrix} \begin{pmatrix} x_t \\ u_t \end{pmatrix}. \tag{34}$$

In the complete information case, the controller input $u_t$ at time $t$ can be computed as the solution to the quadratic program

minimize $V_t(x_t, u_t)$

$$u_t$$

s.t. $u_t \in \Omega_t(x_t)$

where the set $\Omega_t(x_t)$ is an affine subspace in $u_t$. The value of $\Omega_t(x_t)$ depends on whether the RCBF or ZCBF construction is used, as shown in Table 1.

In the incomplete information case, the controller contains an Extended Kalman Filter, which computes an estimate $\hat{x}_t$ of the state $x_t$ as a function of the prior observations $\{y_t : \tau \in [0, t]\}$. The controller computes each control input $u_t$ as a solution to the optimization problem

minimize $V_t(\hat{x}_t, u_t)$

$$u_t$$

s.t. $u_t \in \Omega_t(\hat{x}_t)$

where $\Omega_t(\hat{x}_t)$ is an affine subspace in $u_t$. The values of $\Omega_t(\hat{x}_t)$ are shown in Table 1.

We observe that these quadratic programs can be extended to describe multiple safety constraints, for example, when the region $C = \cap_{i=1}^N \{ x : h_i(x) = 0 \}$. This
extension can be performed by having a set of linear constraints, one for each safety condition \( \{h_i(x) \geq 0\} \). There is no guarantee, however, that such a program has a feasible solution \( u_t \).

An advantage of the CBF method in the deterministic case is that CBFs can be composed with Control Lyapunov Functions to provide joint guarantees on safety and stability. Such CLFs are defined in the stochastic setting as follows.

**Proposition 2** Suppose there exists a function \( V: \mathbb{R}^n \) such that, for every \( x \), there exists \( u \) satisfying

\[
\frac{\partial V}{\partial x}(f(x) + g(x)u) + \text{tr} \left( \sigma^T \frac{\partial^2 V}{\partial x^2} \sigma \right) \leq 0 \quad (36)
\]

If \( u_t \) is chosen to satisfy (36) at each time \( t \), then \( 0 \) is stochastically asymptotically stable.

Proposition 2 implies that stability requirements can be incorporated as a linear constraint on the optimization-based control. In order to ensure feasibility at each time step, the constraints (36) can be relaxed to the objective function with a suitable trade-off parameter; see the numerical study (Section 7) for an example.

### 7 Numerical Study

Our proposed approach was validated through a numerical study using a modified version of the automatic cruise control example introduced in [4]. We consider a system with three states \( (x_1 \ x_2 \ x_3)^T \), where \( x_1 = v_f \) denotes the velocity of the following vehicle, \( x_2 \) denotes the velocity of the leading vehicle, and \( x_3 \) denotes the distance between the vehicles. The velocity of the leading vehicle was chosen to be constant. The input is the force applied to the following vehicle, leading to dynamics

\[
dx_t = \begin{pmatrix} -F_r(x_t)/M \\ 0 \\ x_2 - x_1 \end{pmatrix} + \begin{pmatrix} 1/M \\ 0 \\ 0 \end{pmatrix} u \ dt + dW_t
\]

where \( F_r(x) = f_0 + f_1 v_f + f_2 v_f^2 \) with constants \( f_0 = 0.1 \), \( f_1 = 5 \), and \( f_2 = 0.25 \). The mass \( M = 1650 \). The initial state was chosen as \( x_1 = 18 \), \( x_2 = 10 \), and \( x_3 = 150 \).

The goal of the following vehicle is to achieve a desired velocity \( v_d = 22 \) while minimizing control effort, equal to the integral of \( u_t^2 \). The safety constraint was chosen to avoid collisions with the lead vehicle, and is encoded as \( x_3 - 1.8x_1 \geq 0 \). The target velocity was encoded in a CLF \( V(x) = (x_1 - v_d)^2 \).

We compared four controllers for this problem. The first controller was a naive optimization-based controller that, at each time \( t \), minimized the objective function

\[
(u \ \delta) \begin{pmatrix} 1 \\ 0 \\ 100 \end{pmatrix} \begin{pmatrix} u \\ \delta \end{pmatrix},
\]

under the constraint \( V(x, u) \leq \delta \). Hence the controller attempts to follow the instruction encoded in the CLF while minimizing the control input magnitude, but does not consider safety. The second controller was our proposed RCBF based on the measurement \( dy_t = x_t \ dt + \sigma dW_t \), where \( \sigma = 2 \). The parameter \( \gamma \) in our method was selected by simulating the nonlinear dynamics (37) in the absence of any control, observing the maximum deviation \( ||x - \hat{x}||_2 \), and choosing \( \gamma \) to be ten times the maximum deviation. The barrier function was chosen as

\[
B(x) = -\log \left( \frac{h(x)}{1 + h(x)} \right),
\]

and \( \alpha_3(x) = 1/x \).

The third simulated controller was a simplified version of the RCBF method, in which the barrier constraint was equal to

\[
\frac{\partial B}{\partial x}(f(\hat{x}_t) + g(\hat{x}_t)u) \leq \alpha_3(B(\hat{x}_t)).
\]

This constraint can be interpreted as a deterministic CBF based on the estimated value \( \hat{x}_t \). The fourth simulated controller was the ZCBF method.

The results of the simulation are shown in Figure 1. The naive method begins to approximate the desired velocity (Fig. 1(a)), but violates the safety constraint and collides with the leading vehicle. Both the ZCBF and RCBF methods track the naive method until they approach the lead vehicle and then trigger a sudden braking (Fig.
1(b)) to avoid collision. The CBF settles on a slower velocity that matches the leading vehicle, thus satisfying safety for all time $t$. The RCBF has a larger and more rapidly varying input value, but also maintains a closer velocity to the desired velocity. The ZCBF has a smaller and more consistent input value, but also maintains a lower velocity.

The simplified CBF method tracks the naive method and attempts to brake in order to avoid collision, but the braking does not occur rapidly enough due to the presence of measurement and process noise. This results in a safety violation (Fig. 1(c)). This example illustrates that the uncertainty arising due to noise must be incorporated when choosing the control policy and that adopting a “certainty equivalent” control strategy based on an estimated value may be insufficient to ensure safety.

8 Conclusion

This paper developed a framework for safe control of stochastic systems via Control Barrier Functions. We considered two scenarios, namely, complete information in which the true state state is known to the controller at each time, and incomplete information in which the controller only has access to sensor measurements that are corrupted by Gaussian noise. For each case, we constructed Reciprocal and Zero CBFs. We proved that both constructions guarantee safety with probability 1 in the complete information case, and provide stochastic safety guarantees that depend on the estimation accuracy in the incomplete information case. We proposed control policies that ensure safety and stability by solving quadratic programs containing CBFs and stochastic Control Lyapunov Functions (CLFs) at each time step. We evaluated our approach through a numerical simulation on an adaptive cruise control scenario.

References

[1] Matthias Althoff, Colas Le Guernic, and Bruce H Krogh. Reachable set computation for uncertain time-varying linear systems. In Proceedings of the 14th international conference on Hybrid systems: computation and control, pages 93–102. ACM, 2011.

[2] Aaron D Ames, Samuel Coogan, Magnus Egerstedt, Gennaro Notomista, Koushil Sreenath, and Paulo Tabuada. Control barrier functions: Theory and applications. In 2019 18th European Control Conference (ECC), pages 3420–3431. IEEE, 2019.

[3] Aaron D Ames, Jessy W Grizzle, and Paulo Tabuada. Control barrier function based quadratic programs with application to adaptive cruise control. In Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on, pages 6271–6278. IEEE, 2014.

[4] Aaron D Ames, Xiangru Xu, Jessy W Grizzle, and Paulo Tabuada. Control barrier function based quadratic programs for safety critical systems. IEEE Transactions on Automatic Control, 62(8):3861–3876, 2016.

[5] Yuxiao Chen, Huei Peng, and Jessy Grizzle. Obstacle avoidance for low-speed autonomous vehicles with barrier function. IEEE Transactions on Control Systems Technology, 26(1):194–206, 2017.

[6] Alongkrit Chutinan. Hybrid system verification using discrete model approximations. Ph. D. dissertation, Department of Electrical and Computer Engineering, Carnegie Mellon University, 1999.

[7] Andrew Clark. Control barrier functions for complete and incomplete information stochastic systems. In 2019 American Control Conference (ACC), pages 2928–2935. IEEE, 2019.

[8] Ekaterina Dolginova and Nancy Lynch. Safety verification for automated platoon maneuvers: A case study. In International Workshop on Hybrid and Real-Time Systems, pages 154–170. Springer, 1997.

[9] Antoine Girard, Colas Le Guernic, and Oded Maler. Efficient computation of reachable sets of linear time-invariant systems with inputs. In International Workshop on Hybrid Systems: Computation and Control, pages 257–271. Springer, 2006.

[10] Shao-Chen Hsu, Xiangru Xu, and Aaron D Ames. Control barrier function based quadratic programs with application
to bipedal robotic walking. In *American Control Conference (ACC)*, 2015, pages 4542–4548. IEEE, 2015.

[11] Mrdjan Jankovic. Control barrier functions for constrained control of linear systems with input delay. In *2018 Annual American Control Conference (ACC)*, pages 3316–3321. IEEE, 2018.

[12] Ioannis Karatzas and Steven Shreve. *Brownian motion and stochastic calculus*, volume 113. Springer Science & Business Media, 2012.

[13] Lars Lindemann and Dimos V Dimarogonas. Control barrier functions for signal temporal logic tasks. *IEEE Control Systems Letters*, 3(1):96–101, 2019.

[14] Akar Mehr, Wen-Loong Ma, Forrest Berg, Paulo Tabuada, Jessy W Grizzle, and Aaron D Ames. Adaptive cruise control: Experimental validation of advanced controllers on scale-model cars. In *2015 American Control Conference (ACC)*, pages 1411–1418. IEEE, 2015.

[15] Sayan Mitra, Tichakorn Wongpiromsarn, and Richard M Murray. Verifying cyber-physical interactions in safety-critical systems. *IEEE Security & Privacy*, 11(4):28–37, 2013.

[16] Quan Nguyen and Koushil Sreenath. Exponential control barrier functions for enforcing high relative-degree safety-critical constraints. In *American Control Conference (ACC)*, 2016, pages 322–328. IEEE, 2016.

[17] Quan Nguyen and Koushil Sreenath. Optimal robust control for constrained nonlinear hybrid systems with application to bipedal locomotion. In *2016 American Control Conference (ACC)*, pages 4807–4813. IEEE, 2016.

[18] Stephen Prajna and Ali Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *International Workshop on Hybrid Systems: Computation and Control*, pages 477–492. Springer, 2004.

[19] Stephen Prajna, Ali Jadbabaie, and George J Pappas. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8):1415–1428, 2007.

[20] Stefan Ratschan and Zhikun She. Safety verification of hybrid systems by constraint propagation based abstraction refinement. In *International Workshop on Hybrid Systems: Computation and Control*, pages 573–589. Springer, 2005.

[21] Manuel Rauscher, Melanie Kimmel, and Sandra Hirche. Constrained robot control using control barrier functions. In *Intelligent Robots and Systems (IROS), 2016 IEEE/RSJ International Conference on*, pages 279–285. IEEE, 2016.

[22] Konrad Reif, Stefan Gunther, Engin Yaz, and Rolf Unbehauen. Stochastic stability of the continuous-time extended kalman filter. *IEE Proceedings-Control Theory and Applications*, 147(1):45–52, 2000.

[23] Muhammad Zakiyullah Romdlony and Bayu Jayawardhana. Stabilization with guaranteed safety using control lyapunov–barrier function. *Automatica*, 66:39–47, 2016.

[24] Cesar Santoyo, Maxence Dutreix, and Samuel Coogan. Verification and control for finite-time safety of stochastic systems via barrier functions. In *2019 IEEE Conference on Control Technology and Applications (CCTA)*, pages 712–717. IEEE, 2019.

[25] Paulo Tabuada. *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.

[26] Claire Tomlin, George J Pappas, and Shankar Sastry. Conflict resolution for air traffic management: A study in multiagent hybrid systems. *IEEE Transactions on automatic control*, 43(4):509–521, 1998.