Safe and Robust Observer-Controller Synthesis Using Control Barrier Functions

Devansh R. Agrawal, *Graduate Student Member, IEEE*, and Dimitra Panagou, *Senior Member, IEEE*

***Abstract*—This letter addresses the synthesis of safety-critical controllers using estimate feedback. We propose an observer-controller interconnection to ensure that the nonlinear system remains safe despite bounded disturbances on the system dynamics and measurements that correspond to partial state information. The co-design of observers and controllers is critical, since even in undisturbed cases, observers and controllers designed independently may not render the system safe. We propose two approaches to synthesize observer-controller interconnections. The first approach utilizes Input-to-State Stable observers, and the second uses Bounded Error observers. Using these stability and boundedness properties of the observation error, we construct novel Control Barrier Functions that impose inequality constraints on the control inputs which, when satisfied, certifies safety. We propose quadratic program-based controllers to satisfy these constraints, and prove Lipschitz continuity of the derived controllers. Simulations and experiments on a quadrotor demonstrate the efficacy of the proposed methods.**

***Index Terms*—Robust control, constrained control, observers for nonlinear systems.**

I. Introduction

FOR SAFETY-CRITICAL systems, one must not only design controllers that prioritize system safety above all else, but also certify that the system will remain safe when deployed. In recent years, Control Barrier Functions (CBFs) [1] have become a popular method to design safety-critical controllers, since a certifiably safe control input can be computed efficiently for nonlinear systems. Many extensions have been proposed to address specific challenges in using CBFs, including robustness [2], [3], sampled-data considerations [4] and integration with high-level planners [5]. However, these works assume the controller has access to perfect state information. In most practical systems, the true state of the system is unknown and must be reconstructed using only (often noisy) measurements obtained from sensors. In such systems, it is common to design a full-state feedback controller, and then replace the state by an estimate provided by an observer [6, Sec. 8.7]. It is well established that a controller capable of stabilizing a system with perfect state information may fail to do so when using the state estimate [7, Ch. 12]. Similarly, the use of imperfect information for feedback control may cause safety violations.

In this letter, we study the implications on safety that arise due to imperfect and partially available information, and propose a method to design safe observer-controllers. This important challenge has only recently received some attention. Measurement-Robust CBFs [8] have been proposed to address control synthesis in output-feedback, in the context of vision-based control. The authors assume sensors are noiseless and an imperfect inverse of the measurement map is known, i.e., from a single measurement, a ball containing the true state is known. Using this bound, a second-order cone program-based controller was proposed, although the Lipschitz continuity of this controller is yet to be established [8]. For many safety-critical systems, the measurement maps are non-invertible, limiting the scope for this method.

In [9], a safety critical controller is proposed for stochastic systems, and a probabilistic safety guarantee is proved. The authors consider linear (non-invertible) measurement maps, additive gaussian disturbances, and specifically use the Extended Kalman Filter (EKF) as the observer. In [10] this work is extended to consider a broader class of control-affine systems, and probabilistic guarantees of safety over a finite forward interval are obtained. Establishing safety in a deterministic (non-probabilistic) sense or using alternative observers remains challenging. It has also been demonstrated that in some cases, safety guarantees can be obtained by modeling the system as a Partially Observable Markov Decision Process, e.g., [11], although such methods are computationally expensive for high-dimensional systems and are more suitable for systems with discrete action/state spaces.

The primary contribution of this letter is in synthesizing safe and robust interconnected observer-controllers in such a manner as to establish rigorous guarantees of safety, despite bounded disturbances on the system dynamics and sensor measurements. We propose two approaches to solve this problem, owing to the wide range of nonlinear observers [6]. The first approach utilizes the class of Input-to-State Stable observers [12]. The second approach employs the more general

Manuscript received 21 March 2022; revised 24 May 2022; accepted 6 June 2022. Date of publication 22 June 2022; date of current version 11 July 2022. This work was supported by the National Science Foundation (NSF) under Grant 1942907. Recommended by Senior Editor S. Tarbouriech. *(Corresponding author: Devansh R. Agrawal.)*

The authors are with the Aerospace Engineering Department, University of Michigan at Ann Arbor, Ann Arbor, MI 48105 USA (e-mail: devansh@umich.edu; dpanagou@umich.edu).

Digital Object Identifier 10.1109/LCSYS.2022.3185142

class of 'Bounded Error' observers, in which a set containing the state estimation error is known at all times. This class of observers includes the Deterministic Extended Kalman Filter (DEKF) [7, Ch. 11.2], Lyapunov-based sum-of-squares polynomial observers [13], and others discussed later. We show that our safe estimate-feedback controller can be obtained by solving quadratic programs (QP), and prove Lipschitz continuity of these controllers, allowing for low-computational complexity real-time implementation. The efficacy of the methods is demonstrated both in simulations and in experiments on a quadrotor.

II. Preliminaries and Background

Notation: Let $\mathbb{R}$ be the set of reals, $\mathbb{R}_{\geq 0}$ the set of non-negative reals and $\mathbb{S}^n_{++}$ the set of symmetric positive definite matrices in $\mathbb{R}^{n\times n}$. $\lambda_{min}(P), \lambda_{max}(P)$ denote the smallest and largest eigenvalues of $P \in \mathbb{S}^n_{++}$. For $x \in \mathbb{R}^n$, x_i is the i-th element, $\|x\|$ is the Euclidean norm. The norm of a signal $w : \mathbb{R}_{\geq 0} \to \mathbb{R}^q$ is $\|w(t)\|_\infty \triangleq \sup_{t\geq 0} \|w(t)\|$. γ_f denotes the Lipschitz constant of a Lipschitz-continuous function $f : \mathbb{R}^n \to \mathbb{R}^m$. Class $\mathcal{K}$, extended class $\mathcal{K}$ and class $\mathcal{KL}$ functions are as defined in [14]. Lie derivatives of a scalar function $h : \mathcal{X} \to \mathbb{R}$, $(\mathcal{X} \subset \mathbb{R}^n)$, along a vector field $f : \mathcal{X} \to \mathbb{R}^n$ are denoted $L_f h(x) = \frac{\partial h}{\partial x}(x) f(x)$. If vector fields has an additional dependency, e.g., $f : \mathcal{X} \times \mathbb{R}^p \to \mathbb{R}^n$, the notation $L_f h(x, y) = \frac{\partial h}{\partial x}(x) f(x, y)$ is used.

1) System: Consider a nonlinear control-affine system:

$$\dot{x} = f(x) + g(x)u + g_d(x)d(t), \tag{1a}$$
$$y = c(x) + c_d(x)v(t), \tag{1b}$$

where $x \in \mathcal{X} \subset \mathbb{R}^n$ is the system state, $u \in \mathcal{U} \subset \mathbb{R}^m$ is the control input, $y \in \mathbb{R}^{n_y}$ is the measured output, $d : \mathbb{R}_{\geq 0} \to \mathbb{R}^{n_d}$ is a disturbance on the system dynamics, and $v : \mathbb{R}_{\geq 0} \to \mathbb{R}^{n_v}$ is the measurement disturbance. We assume d and v are piecewise continuous, bounded disturbances, $\sup_t \|d(t)\|_\infty = \bar{d}$ and $\|v(t)\|_\infty \leq \bar{v}$ for some known $\bar{d}, \bar{v} < \infty$. The functions $f : \mathcal{X} \to \mathbb{R}^n$, $g : \mathcal{X} \to \mathbb{R}^{n\times m}$, $c : \mathcal{X} \to \mathbb{R}^{n_y}$, $g_d : \mathcal{X} \to \mathbb{R}^{n\times n_d}$, and $c_d : \mathcal{X} \to \mathbb{R}^{n_y \times n_v}$ are all assumed to be locally Lipschitz continuous. Notice that $g_d(x)d(t)$ accounts for either matched or unmatched disturbances.

In observer-controller interconnections, the observer maintains a state estimate $\hat{x} \in \mathcal{X}$, from which the controller determines the control input. The observer-controller interconnection is defined to be of the form:

$$\dot{\hat{x}} = p(\hat{x}, y) + q(\hat{x}, y)u, \tag{2a}$$
$$u = \pi(t, \hat{x}, y), \tag{2b}$$

where $p : \mathcal{X} \times \mathbb{R}^{n_y} \to \mathbb{R}^n$, $q : \mathcal{X} \times \mathbb{R}^{n_y} \to \mathbb{R}^{n\times m}$ are locally Lipschitz in both arguments. The feedback controller $\pi : \mathbb{R}_{\geq 0} \times \mathcal{X} \times \mathbb{R}^p \to \mathcal{U}$ is assumed piecewise-continuous in t and Lipschitz continuous in the other two arguments. Then, the closed-loop system formed by (1, 2) is

$$\dot{x} = f(x) + g(x)u + g_d(x)d(t), \tag{3a}$$
$$\dot{\hat{x}} = p(\hat{x}, y) + q(\hat{x}, y)u, \tag{3b}$$
$$x(0) = x_0, \ \hat{x}(0) = \hat{x}_0, \tag{3c}$$

where y and u are defined in (1b) and (2b) respectively. Under the stated assumptions, there exists an interval $\mathcal{I} = \mathcal{I}(x_0, \hat{x}_0) = [0, t_{max}(x_0, \hat{x}_0))$ over which solutions to the closed-loop system exist and are unique [15, Th. 3.1].

2) Safety: Safety is defined as the true state of the system remaining within a *safe set*, $\mathcal{S} \subset \mathcal{X}$, for all times $t \in \mathcal{I}$. The safe set $\mathcal{S}$ is defined as the super-level set of a continuously-differentiable function $h : \mathcal{X} \to \mathbb{R}$:

$$\mathcal{S} = \{x \in \mathcal{X} : h(x) \geq 0\}. \tag{4}$$

A state-feedback controller[1] $\pi : \mathbb{R}_{\geq 0} \times \mathcal{X} \to \mathcal{U}$ *renders system* (1) *safe* with respect to the set $\mathcal{S}$, if for the closed-loop dynamics $\dot{x} = f(x) + g(x)\pi(t, x) + g_d(x)d(t)$, the set $\mathcal{S}$ is *forward invariant*, i.e., $x(0) \in \mathcal{S} \implies x(t) \in \mathcal{S}\ \forall t \in \mathcal{I}$. In output-feedback we define safety as follows.

Definition 1: An observer-controller pair (2) *renders system* (1) *safe* with respect to a set $\mathcal{S} \subset \mathcal{X}$ from the initial-condition sets $\mathcal{X}_0, \hat{\mathcal{X}}_0 \subset \mathcal{S}$ if for the closed-loop system (3),

$$x(0) \in \mathcal{X}_0 \text{ and } \hat{x}(0) \in \hat{\mathcal{X}}_0 \implies x(t) \in \mathcal{S} \quad \forall t \in \mathcal{I}. \tag{5}$$

Note the importance of the observer-controller connection, i.e., using only $\hat{x}(t)$, we must obtain guarantees on $x(t)$.

3) Control Barrier Functions: Control Barrier Functions (CBFs) have emerged as a tool to characterize and find controllers that can render a system safe [1]. Robust-CBFs [2] also account for the disturbances $d(t)$ in (1a). We introduce a modification to reduce conservatism, inspired by [3].

Definition 2: A continuously differentiable function $h : \mathcal{X} \to \mathbb{R}$ is a *Tunable Robust CBF* (TRCBF) for system (1) if there exists a class $\mathcal{K}$ function α, and a continuous, non-increasing function $\kappa : \mathbb{R}_{\geq 0} \to \mathbb{R}$ with $\kappa(0) = 1$, s.t.

$$\sup_{u\in\mathcal{U}} \ L_f h(x) + L_g h(x)u + \alpha(h(x)) \geq \kappa(h(x)) \left\| L_{g_d} h(x) \right\| \bar{d}, \ \forall x \in \mathcal{S}. \tag{6}$$

Examples include $\kappa(r) = 1$ and $\kappa(r) = 2/(1 + \exp(r))$. Given a TRCBF h for (1), the set of safe control inputs is

$$K_{trcbf}(x) = \{u \in \mathcal{U} : L_f h(x) + L_g h(x)u - \kappa(h(x)) \left\| L_{g_d} h(x) \right\| \bar{d} \geq -\alpha(h(x))\}, \tag{7}$$

and a safe state-feedback controller is obtained by solving a QP, as in [2, eq. (30)]. The main question is:

Problem 1: Given a system (1) with disturbances of known bounds $\|d(t)\|_\infty \leq \bar{d}$, $\|v(t)\|_\infty \leq \bar{v}$, and a safe set $\mathcal{S}$ defined by (4), synthesize an interconnected observer-controller (2) and the initial condition sets $\mathcal{X}_0, \hat{\mathcal{X}}_0$ to render the system safe.

We study systems subject to disturbances with a known bound. We will use this bound to derive sufficient conditions on the control policy to guarantee safety satisfaction. In practice, a conservative upper bounds can be used, although future work will address the probabilistic safety guarantees that are possible under probabilistic disturbances.

[1] In *state-feedback* the control input is determined from the true state, $u = \pi(t, x)$. In *estimate-feedback* the input is determined from the state estimate and measurements, $u = \pi(t, \hat{x}, y)$.

III. Main Results

A. Approach 1

Approach 1 relies on defining a set of state estimates, $\hat{\mathcal{S}} \subset \mathcal{X}$, such that if the estimate $\hat{x}$ lies in $\hat{\mathcal{S}}$, the true state x lies in the safe set $\mathcal{S}$. The controller is designed to ensure $\hat{x} \in \hat{\mathcal{S}}$ at all times. We consider Input-to-State Stable observers:

Definition 3 (Adapted From [12]): An observer (2) is an *Input-to-State Stable (ISS) Observer* for system (1), if there exists a class $\mathcal{KL}$ function β continuously differentiable wrt to the second argument, and a class $\mathcal{K}$ function η such that

$$\left\|x(t) - \hat{x}(t)\right\| \leq \beta(\left\|x(0) - \hat{x}(0)\right\|, t) + \eta(\bar{w}), \forall t \in \mathcal{I}, \quad (8)$$

where $\bar{w} = \max(\bar{d}, \bar{v})$.

Various methods to design ISS observers for nonlinear systems have been developed, and reader is referred to [6], [12], [16], [17], [18] and references within for specific techniques.

The key property of an ISS observer is that the estimation error is bounded with a known bound: for any $\delta > 0$, there exists a continuously differentiable, non-increasing function $M_\delta : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, such that

$$\left\|x(0) - \hat{x}(0)\right\| \leq \delta \Rightarrow \left\|x(t) - \hat{x}(t)\right\| \leq M_\delta(t) \ \forall t \in \mathcal{I}. \quad (9)$$

Comparing (8) and (9), $M_\delta(t) = \beta(\delta, t) + \eta(\bar{w})$. Define

$$\hat{\mathcal{S}} = \{\hat{x} \in \mathcal{X} : h(\hat{x}) - \gamma_h M_\delta(t) \geq 0\}, \quad (10)$$

the set of safe state-estimates, and we obtain the property $\hat{x}(t) \in \hat{\mathcal{S}} \implies x(t) \in \mathcal{S}$ by the Lipschitz continuity of h.[2] Then the conditions to guarantee safety are as follows:

Definition 4: A continuously differentiable function $h : \mathcal{X} \to \mathbb{R}$ is an *Observer-Robust CBF* for system (1) with an ISS observer (2a) of known estimation error bound (9), if there exists an extended class $\mathcal{K}$ function α s.t.[3]

$$\sup_{u \in \mathcal{U}} \ L_p h(\hat{x}, y) + L_q h(\hat{x}, y)u \geq -\alpha(h(\hat{x}) - \gamma_h M_\delta(0)) \quad (11)$$

for all $\hat{x} \in \mathcal{S}$, and all $y \in \mathcal{Y}(\hat{x}) = \{y : y = c(x) + c_d(x)v(t) \mid \|x - \hat{x}\| \leq M_\delta(0), \|v\| \leq \bar{v}\}$, an overapproximation of the set of possible outputs.[4]

Theorem 1: For system (1), suppose the observer (2a) is ISS with estimation error bound (9). Suppose $\mathcal{S}$ is defined by an Observer-Robust CBF $h{:}\mathcal{X} \to \mathbb{R}$ associated with extended class $\mathcal{K}$ function α. If the initial conditions satisfy

$$\hat{x}(0) \in \hat{\mathcal{X}}_0 = \{\hat{x} \in \mathcal{S} : h(\hat{x}) \geq \gamma_h M_\delta(0)\}, \quad (12)$$

$$x(0) \in \mathcal{X}_0 = \{x \in \mathcal{S} : \left\|x(0) - \hat{x}(0)\right\| \leq \delta\}, \quad (13)$$

then any Lipschitz continuous estimate-feedback controller $u = \pi(t, \hat{x}, y) \in K_{orcbf}(t, \hat{x}, y)$ where

$$K_{orcbf}(t, \hat{x}, y) = \{u \in \mathcal{U} : L_p h(\hat{x}, y) + L_q h(\hat{x}, y)u \geq -\alpha\big(h(\hat{x}) - \gamma_h M_\delta(t)\big) + \gamma_h \dot{M}_\delta(t)\} \quad (14)$$

renders the system safe from the initial-condition sets $\mathcal{X}_0, \hat{\mathcal{X}}_0$.

[2]By Lipschitz continuity, $|h(x) - h(\hat{x})| \leq \gamma_h \|x - \hat{x}\| \implies h(\hat{x}) - \gamma_h \|x - \hat{x}\| \leq h(x)$. Therefore, if $\hat{x} \in \hat{\mathcal{S}}$, then $0 \leq h(\hat{x}) - \gamma_h M_\delta(t) \leq h(\hat{x}) - \gamma_h \|x - \hat{x}\| \leq h(x)$, i.e., $x \in \mathcal{S}$. Thus, $\hat{x} \in \hat{\mathcal{S}} \implies x \in \mathcal{S}$.

[3]Recall the notation $L_p h(\hat{x}, y) = \frac{\partial h}{\partial \hat{x}}(\hat{x}) p(\hat{x}, y)$.

[4]$\mathcal{Y}$ is defined using $M_\delta(0)$ instead of δ since $\mathcal{Y}(\hat{x}(t))$ must contain the set of possible outputs at time t for all $t \in \mathcal{I}$.

Proof: Consider the function $H(t, \hat{x}) = h(\hat{x}) - \gamma_h M_\delta(t)$. By the Lipschitz continuity of h, and (9), $H(t, \hat{x}) \geq 0 \implies h(x) \geq 0$. The total derivative of H is

$$\dot{H} = \frac{\partial H}{\partial t} + \frac{\partial H}{\partial \hat{x}} \dot{\hat{x}} = -\gamma_h \dot{M}_\delta + L_p h(\hat{x}, y) + L_q h(\hat{x}, y)u$$

therefore, for any $\pi(t, \hat{x}, y) \in K_{orcbf}(t, \hat{x}, y)$ we have $\dot{H} \geq -\alpha(H)$. Since $H(0, \hat{x}_0) \geq 0$ (from the initial condition (12)), $H(t, \hat{x}) \geq 0, \forall t \in \mathcal{I}$, completing the proof. ∎

Remark 1: Under the same assumptions as Theorem 1, if $\mathcal{U} = \mathbb{R}^m$ and a desired control input $\pi_{des} : \mathbb{R}_{\geq 0} \times \mathcal{X} \to \mathbb{R}^m$ is provided, a QP-based safe estimate-feedback controller is

$$\pi(t, \hat{x}, y) = \underset{u \in \mathbb{R}^m}{\operatorname{argmin}} \left\|u - \pi_{des}(t, \hat{x})\right\|^2, \text{ s.t.}$$
$$L_p h(\hat{x}, y) + L_q h(\hat{x}, y)u \geq -\alpha(h(\hat{x}) - \gamma_h M_\delta(t)) + \gamma_h \dot{M}_\delta(t) \quad (15)$$

Remark 2: The constraint in (15) does not explicitly depend on the disturbances $d(t)$ and $v(t)$, since the effect of these disturbances is captured by the estimation error bound $M_\delta(t)$. Furthermore, since $\gamma_h \dot{M}_\delta(t) \leq 0$,[5] the constraint (15) is easier to satisfy for higher convergence rates of the observer.

Remark 3: For a linear class $\mathcal{K}$ function, $\alpha(r) = \gamma_\alpha r$, if $\dot{M}_\delta \leq -\gamma_\alpha M_\delta(t)$, a sufficient condition for (15) is

$$L_p h(\hat{x}, y) + L_q h(\hat{x}, y)u \geq -\gamma_\alpha h(\hat{x}).$$

which does not depend on the bound $M_\delta(t)$ or Lipschitz constant γ_h. In other words, if the observer converges faster than the rate at which the boundary of the safe set is approached, i.e., if $\dot{M}_\delta \leq -\gamma_\alpha M_\delta$, then a safe control input can be obtained without explicit knowledge of M_δ or γ_h. This matches the general principle that for good performance observers should be converge faster than controllers.

B. Approach 2

While in Approach 1 we used the stability guarantees of ISS observers to obtain safe controllers, in Approach 2 we consider observers that only guarantee boundedness of the estimation error. First, we define Bounded-Error Observers:

Definition 5: An observer (2a) is a *Bounded-Error (BE) Observer*, if there exists a bounded set $\mathcal{D}(\hat{x}_0) \subset \mathcal{X}$ and a (potentially) time-varying bounded set $\mathcal{P}(t, \hat{x}) \subset \mathcal{X}$ s.t.

$$x_0 \in \mathcal{D}(\hat{x}_0) \implies x(t) \in \mathcal{P}(t, \hat{x}) \ \forall t \in \mathcal{I}. \quad (16)$$

Figure 1 depicts the sets $\mathcal{D}$ and $\mathcal{P}$. Note, ISS observers are a subset of BE observers, using the definitions $\mathcal{D}(\hat{x}_0) = \{x : \|x - \hat{x}_0\| \leq \delta\}$ and $\mathcal{P}(t, \hat{x}) = \{x : \|x - \hat{x}(t)\| \leq M_\delta(t)\}$. BE observers are more general than ISS observers in the following ways: (A) The sets $\mathcal{D}$ and $\mathcal{P}$ do not have to be norm-balls. For example, they could be zonotopes [19], intervals [20], or sub-level sets of sum-of-squares polynomials [21]. (B) The shape and size of $\mathcal{P}$ is allowed to change over time.

The idea is to find a common, safe input for all $x \in \mathcal{P}(t, \hat{x})$:

Theorem 2: For system (1), suppose the observer (2a) is a Bounded-Error observer. Suppose the safe set $\mathcal{S}$ is defined by a continuously differentiable function $h : \mathcal{X} \to \mathbb{R}$, where h is a Tunable Robust-CBF for the system.

[5]Since $M_\delta(t) = \beta(\delta, t) + \eta(\bar{w})$, and β is a class $\mathcal{KL}$ function, $\dot{M}_\delta(t) = \partial\beta/\partial t < 0$. Finally since $\gamma_h \in \mathbb{R}_{\geq 0}$ is a Lipschitz constant, $\gamma_h \dot{M}_\delta(t) \leq 0$.

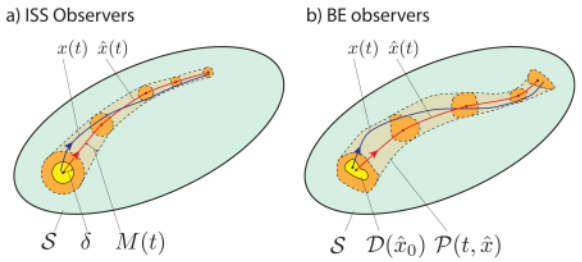

Fig. 1. Depiction of Input-to-State Stable observers and Bounded-Error observers. (a) In ISS observers, the estimation error is bounded by a norm-ball, and must be non-increasing in time. (b) In BE observers, the state estimate must be contained in a bounded set $\mathcal{P}(t,\hat{x})$.

Suppose $\pi : \mathbb{R}_{\geq 0} \times \mathcal{X} \to \mathcal{U}$ is an estimate-feedback controller, piecewise-continuous in the first argument and Lipschitz continuous in the second, s.t.

$$\pi(t,\hat{x}) \in \bigcap_{x \in \mathcal{P}(t,\hat{x})} K_{trcbf}(x), \tag{17}$$

where K_{trcbf} is defined in (7). Then the observer-controller renders the system safe from the initial-condition sets $x(0) \in \mathcal{X}_0 = \mathcal{D}(\hat{x}_0)$ and $\hat{x}_0 \in \hat{\mathcal{X}}_0 = \{\hat{x} : \mathcal{P}(0,\hat{x}_0) \subset \mathcal{S}\}$.

Proof: The total derivative of h for any $x \in \partial\mathcal{S}$ and $\pi(t,\hat{x}) \in K_{trcbf}(x)$ satisfies

$$\begin{aligned}\dot{h} &= L_f h(x) + L_g h(x)\pi(t,\hat{x}) + L_{g_d} h(x) w(t)\\ &\geq L_f h(x) + L_g h(x)\pi(t,\hat{x}) - \kappa(0)\left\|L_{g_d} h(x)\right\|\bar{w}\\ &\geq -\alpha(0) = 0\end{aligned}$$

since $h(x) = 0$, $\kappa(0) = 1$, and $x(t) \in \mathcal{P}(t,\hat{x})$. Therefore, at any $x \in \partial\mathcal{S}$, $\dot{h} \geq 0$, i.e., the system remains safe [22]. ∎

In general, designing a controller satisfying (17) can be difficult. We propose a method under the following assumptions:

Assumption 1: There exists a known function $a : \mathbb{R}_{\geq 0} \times \mathcal{X} \to \mathbb{R}$, piecewise continuous in the first argument and Lipschitz continuous in the second, such that for all $\hat{x} \in \mathcal{S}$,

$$a(t,\hat{x}) \leq \inf_{x \in \mathcal{P}(t,\hat{x})} L_f h(x) - \kappa(h(x))\left\|L_{g_d} h(x)\right\|\bar{w} + \alpha(h(x)).$$

By Assumption 1, $a(t,\hat{x})$ lower-bounds the terms in $\dot{h}$ independent of u. These bounds can be obtained using Lipschitz constants. Similarly, we bound each term of $L_g h$.

Assumption 2: There exist known functions $b_i^-, b_i^+ : \mathbb{R}_{\geq 0} \times \mathcal{X} \to \mathbb{R}$ for $i = \{1,\dots,m\}$, piecewise continuous in the first argument and Lipschitz continuous in the second, such that[6]

$$b_i^-(t,\hat{x}) \leq [L_g h(x)]_i \leq b_i^+(t,\hat{x})$$

for all $t \geq 0$, all $x \in \mathcal{S}$ and all $\hat{x} \in \{\hat{x} : x \in \mathcal{P}(t,\hat{x})\}$. Furthermore, suppose $\text{sign}(b_i^-(t,\hat{x})) = \text{sign}(b_i^+(t,\hat{x}))$ at every $t, \hat{x} \in \mathcal{S}$, and that h is of relative-degree 1, i.e., $L_g h(x) \neq 0$.

Intuitively, by assuming $\text{sign}(b_i^-(t,\hat{x})) = \text{sign}(b_i^+(t,\hat{x}))$ it is clear whether a positive or negative u_i increases $\dot{h}(x,u)$.[7]

Theorem 3: Consider a system (1) with $\mathcal{U} = \mathbb{R}^m$ and suppose the observer (2a) is a Bounded-Error observer. Suppose $\mathcal{S}$ is the safe set defined by an TRCBF h and Assumptions 1, 2 are satisfied. Suppose $\pi_{des} : \mathbb{R}_{\geq 0} \times \mathcal{X} \to \mathcal{U}$ is a desired controller, piecewise continuous wrt t and Lipschitz continuous wrt $\hat{x}$. Then the estimate-feedback controller $\pi : \mathbb{R}_{\geq 0} \times \mathcal{X} \to \mathbb{R}^m$

$$\begin{aligned}\pi(t,\hat{x}) = \underset{u \in \mathbb{R}^m}{\text{argmin}} \ & \left\|u - \pi_{des}(t,\hat{x})\right\|^2\\ \text{s.t.} \ & a(t,\hat{x}) + \sum_{i=1}^{m} \min\{b_i^-(t,\hat{x})u_i, b_i^+(t,\hat{x})u_i\} \geq 0\end{aligned} \tag{18}$$

is piecewise continuous wrt t, Lipschitz continuous wrt x, and renders the system safe from the initial-condition sets $x_0 \in \mathcal{X}_0 = \mathcal{D}(\hat{x}_0)$ and $\hat{x}_0 \in \hat{\mathcal{X}}_0 = \{\hat{x} : \mathcal{P}(0,\hat{x}_0) \subset \mathcal{S}\}$.

Proof: First, we prove existence and uniqueness of solutions to the QP. In standard form, the QP (18) is equivalent to

$$\begin{aligned}\min_{u \in \mathbb{R}^m, k \in \mathbb{R}^m} \ & \frac{1}{2}u^T u - \pi_{des}^T u\\ \text{s.t.} \ & \left[\begin{array}{ccc|ccc} b_1^- & \cdots & 0 & -1 & \cdots & 0\\ b_1^+ & \cdots & 0 & -1 & \cdots & 0\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ 0 & \cdots & b_m^- & 0 & \cdots & -1\\ 0 & \cdots & b_m^+ & 0 & \cdots & -1\\ \hline 0 & \cdots & 0 & 1 & \cdots & 1 \end{array}\right]\left[\begin{array}{c} u_1\\ \vdots\\ \frac{u_m}{k_1}\\ \vdots\\ k_m \end{array}\right] \geq \left[\begin{array}{c} 0\\ 0\\ \vdots\\ 0\\ \underline{0}\\ -a \end{array}\right]\end{aligned} \tag{19}$$

where the dependences on $(t,\hat{x})$ were omitted for brevity. Here $k \in \mathbb{R}^m$ is an auxiliary variable encoding the constraint $k_i \leq \min\{b_i^- u_i, b_i^+ u_i\}$ for all $i = \{1,\dots,m\}$. This constraint matrix has size $(2m+1, 2m)$. However, since $\text{sign}(b_i^-) = \text{sign}(b_i^+)$ by Assumption 2, only one of either the $(2i-1)$-th or $(2i)$-th constraints can be active.[8] Considering the sparsity pattern of active constraint matrix, these constraints must be linearly independent. Therefore, the proposed QP has $2m$ decision variables with at most $m+1$ linearly independent constraints, and thus a non-empty set of feasible solutions. Since the cost function is quadratic, there exists a unique minimizer.

Second, we prove Lipschitz continuity. Since the active constraints matrix has linearly independent rows, the regularity conditions in [23] are met. Thus the solution $\pi(t,\hat{x})$ is Lipschitz continuous wrt $\pi_{des}(t,\hat{x}), a(t,\hat{x}), b_i^-(t,\hat{x})$ and $b_i^+(t,\hat{x})$. Since these quantities are piecewise continuous wrt t and Lipschitz continuous wrt $\hat{x}$, the same is true for $\pi(t,\hat{x})$.

Finally, we prove safety. Since (omitting $t, x, \hat{x}$),

$$L_g h u = \sum_{i=1}^{m} [L_g h]_i u_i \geq \sum_{i=1}^{m} \min\{b_i^- u_i, b_i^+ u_i\},$$

satisfaction of the constraint in (18) implies satisfaction of (17). Therefore, by Theorem 2, the system is rendered safe. ∎

IV. Simulations and Experiments

Code and videos are available here: https://github.com/dev10110/robust-safe-observer-controllers

1) Simulation (Double Integrator): We simulate a double integrator system without disturbances, to demonstrate the importance of the observer-controller interconnection. The system is (with $\mathcal{U} = \mathbb{R}$)

$$\dot{x}_1 = x_2, \ \dot{x}_2 = u, \ y = x_1, \tag{20}$$

[6]Recall, $[L_g h(x)]_i$ refers to the i-th element of $L_g h(x)$.

[7]Future work will attempt to relax this assumption. In our limited experience, the estimation error can be sufficiently small that the assumption holds.

[8]Note, if $b_i^- = b_i^+ \neq 0$, then both constraints are equivalent, and thus still means a single constraints is active. Since $L_g h(x) \neq 0$ (Assumption 2), $b_i^- = b_i^+ \neq 0$ for atleast one of $i = 1,\dots,m$.

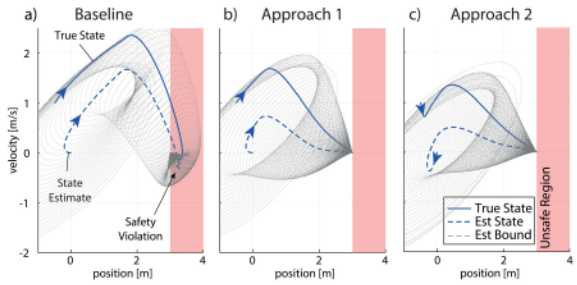

Fig. 2. Simulation results for the Double Integrator (20), using (a) the baseline CBF controller, (b) Approach 1 and (c) Approach 2. The same initial conditions and observer is used for each simulation.

and the safe set is defined as $\mathcal{S} = \{x : x_1 \leq x_{max}\}$. We use the CBF $h(x) = -x_2 + \alpha_0(x_{max} - x_1)$. A Luenberger-observer, $\dot{\hat{x}} = A\hat{x} + Bu + L(y - C\hat{x})$, is used, where $L = 1/2P^{-1}C^T$ and $P \in \mathbb{S}^2_{++}$ is the solution the Lyapunov equation $PA + A^TP - C^TC = -2\theta P$ for design parameter $\theta > 0$. This observer is ISS, since for any $\delta > 0$, (9) is satisfied with $M_\delta(t) = \sqrt{\lambda_{max}(P)/\lambda_{min}(P)}\delta e^{-\theta t}$. This observer is also a Bounded Error observer since for any $\delta > 0$, (16) is satisfied with $\mathcal{D}(\hat{x}_0) = \{x : \|x_0 - \hat{x}_0\| \leq \delta\}$ and $\mathcal{P}(t, \hat{x}) = \{x : (x - \hat{x})^T P(x - \hat{x}) \leq \lambda_{max}(P)\delta^2 e^{-2\theta t}\}$.

We compare the methods proposed in this letter to the CBF-QP of [1] (referred to as the Baseline-QP), using $\hat{x}$ in lieu of x. Plots of the resulting trajectory are depicted in Figure 4, demonstrating safety violation. The trajectory plots under the controllers based on Approaches 1 and 2 are shown in Figure 2, demonstrating that safety is maintained in both cases. In Approach 2, the function $L_f h(x)$ is affine in x and $L_g h(x) = -1$ is independent of x, and therefore the function $a(t, \hat{x})$ was determined using a box bound around $\mathcal{P}(t, \hat{x})$ and $b_i^-(t, \hat{x}) = b_i^+(t, \hat{x}) = -1$. Numerically, we have noticed that for some initial conditions and convergence rates, the controller of Approach 1 is less conservative than the controller of Approach 2, and in other cases the converse is true. Identifying conditions that determine whether Approach 1 or 2 is less conservative remains an open question.

2) Simulation (Planar Quadrotor): Consider

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \\ \dot{x}_5 \\ \dot{x}_6 \end{bmatrix} = \begin{bmatrix} x_4 \\ x_5 \\ x_6 \\ 0 \\ -g \\ 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \sin x_3/m & 0 \\ \cos x_3/m & 0 \\ 0 & J^{-1} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ d_1(t) \\ d_2(t) \\ 0 \end{bmatrix}$$
$$y = [x_1, x_2, x_3]^T + [v_1(t), v_2(t), v_3(t)]^T$$

where $[x_1, x_2]^T$ are the position coordinates of the quadrotor with respect to an inertial coordinate frame, x_3 is the pitch angle, $[x_4, x_5]^T$ are the linear velocities in the inertial frame, and x_6 is the rate of change of pitch. The quadrotor has mass $m = 1.0$ kg and moment of inertial $J = 0.25$ kg/m^2, and the acceleration due to the gravity is $g = 9.81$ m/s^2. The control inputs are thrust u_1 and torque u_2. The disturbances $d : \mathbb{R}_{\geq 0} \to \mathbb{R}^2$ captures the effect of unmodeled aerodynamic forces on the system, bounded by $\|d\| \leq 2$ m/s^2. The measurement disturbance is $v : \mathbb{R}_{\geq 0} \to \mathbb{R}^3$, bounded by 5 cm for position measurements, and 5° for pitch measurements.

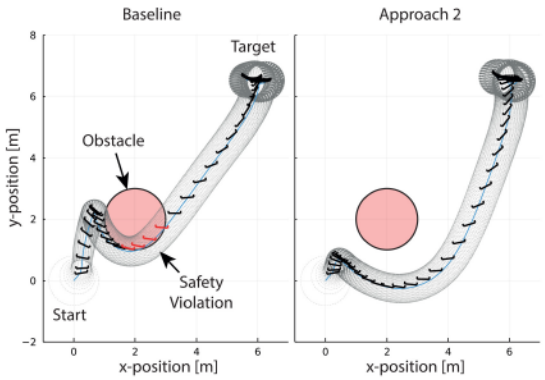

Fig. 3. Simulation Results for the Planar Quadrotor. The objective is to fly the quadrotor from the starting state to the target position while avoiding the circular obstacle region. The blue lines indicate the path of the state estimate and grey lines the projection of $\mathcal{P}(t, \hat{x})$ on the x-y plane. The icons show the quadrotor's true position every 0.2 s and is colored red while violating safety. (a) uses the baseline CBF controller, and (b) uses Approach 2.

The safety condition is to avoid collision with a circular obstacle at $[x_1^*, x_2^*]^T$ of radius r, i.e., $\mathcal{S} = \{x : (x_1 - x_1^*)^2 + (x_2 - x_2^*)^2 - r^2 \geq 0\}$. The CBF proposed in [24] is used. The desired control input is a LQR controller linearized about the hover state. The observer is a DEKF adapted from [25][9]: Defining constant matrices $D_1 = g_d(x)$ and $D_2 = c_d(x)$, the observer is

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) + g(\hat{x})u + PC^TR^{-1}(y - c(\hat{x})) \\ \dot{P} = PA^T + AP - PC^TR^{-1}CP + Q + 2\theta P \\ \dot{V} = -2\theta V + 2\sqrt{V}\left(\left\|D_1^T P^{-1/2}\right\|\bar{d} + \left\|(LD_2)^T P^{-1/2}\right\|\bar{v}\right) \end{cases}$$

where $\theta \geq 0$ is a design parameter, $A = \frac{\partial}{\partial x}(f(\hat{x}) + g(\hat{x})u)$, $C = \frac{\partial c}{\partial x}(\hat{x})$. In the standard form of EKFs [26, Sec. 5.3], the disturbances are assumed to be Weiner processes and Q, R represent the covariances of the $d(t)$ and $v(t)$. However in the Deterministic EKF, we assume $d(t), v(t)$ are bounded, and thus $Q \in \mathbb{S}^n_{++}, R \in \mathbb{S}^{n_y}_{++}$ can be freely chosen. Assuming there exist positive constants p_1, p_2 such that $p_1 I \leq P(t) \leq p_2 I \ \forall t \in \mathcal{I}$, (see [7, Sec. 11.2]), this observer is a Bounded-Error observer, and satisfies (16) with $\mathcal{D}(\hat{x}_0) = \mathcal{P}(0, \hat{x}_0)$, and $\mathcal{P}(t, \hat{x}) = \{x : (x - \hat{x})^T P(t)^{-1}(x - \hat{x}) \leq V(t)\}$.

The method in Approach 2 is used to synthesize the interconnected observer-controller. Specifically, the functions a, b_i^-, and b_i^+ were determined using Lipschitz bounds, and the QP (18) is used to determine the control input.

Figure 3 compares the trajectory of the planar quadrotor using the controller proposed in [24] (baseline case) to the proposed controller of Approach 2. In the baseline case, since the state estimate is used in lieu of the true state, safety is violated. By accounting for the state estimation uncertainty, the proposed controller avoids the obstacle.

3) Experiments (3D Quadrotor): For our experiments, we use the Crazyflie 2.0 quadrotor, using the on-board IMU and barometer sensors and an external Vicon motion capture system. The objective was to fly in a figure of eight

[9]In [25], only the undisturbed case is demonstrated. The extension to include bounded disturbances can be derived using the same techniques as in the original paper. The additional terms due to the disturbances are bounded using [7, eq. (B4)].

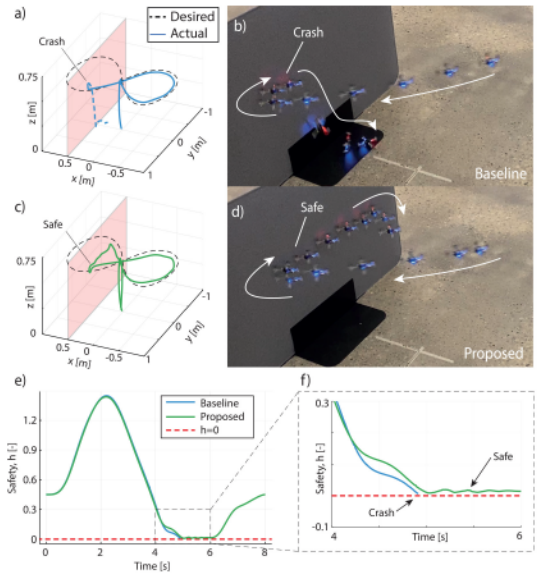

Fig. 4. Experimental results. The quadrotor is commanded to track a figure-of-eight trajectory, while avoiding the physical barrier at $x = 0.5$ m. Ground truth trajectories are plotted in (a, c) for the baseline CBF and proposed controllers respectively. Snapshots from the experiment are show in (b, d). (e, f) Plots of the safety value, h over time for both trajectories.

trajectory, but to not crash into a physical barrier placed at $x = 0.5$ meters. State was estimated using an EKF [27], assuming the true state lies within the 99.8% confidence interval of the EKF. To design the controller, first $\pi_{des}(t, \hat{x})$ is computed using an LQR controller, which computes desired accelerations wrt to an inertial frame to track the desired trajectory. This command is filtered using a safety critical QP, either the baseline CBF-QP (Figure 4a) or the proposed QP using Approach 2 (18) (Figure 4c). Finally, the internal algorithm of the Crazyflie (based on [28]) is used to map the output of the QP to motor PWM signals. The magnitude of the disturbances was estimated by collecting experimental data when the quadrotor was commanded to hover. The trajectories from the two flight controllers are compared in Figure 4. In the baseline controller, the quadrotor slows down as it approaches the barrier, but still crashes into barrier. In the proposed controller, the quadrotor remains safe, Figure 4e.

V. Conclusion

In this letter we have developed two methods to synthesize observer-controllers that are robust to bounded disturbances on system dynamics and measurements, and maintain safety in the presence of imperfect information. We have demonstrated the efficacy of these methods in simulation and experiments. Future work will investigate methods to learn the disturbance, such that the controller can adaptively tune itself to achieve better performance, and to extend the work to handle probabilistic guarantees of safety when the system is subject to stochastic disturbances instead of bounded disturbances.

References

[1] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 8, pp. 3861–3876, Aug. 2017.

[2] M. Jankovic, "Robust control barrier functions for constrained stabilization of nonlinear systems," *Automatica*, vol. 96, pp. 359–367, Oct. 2018.

[3] A. Alan, A. J. Taylor, C. R. He, G. Orosz, and A. D. Ames, "Safe controller synthesis with tunable input-to-state safe control barrier functions," *IEEE Contr. Syst. Lett.*, vol. 6, pp. 908–913, 2021.

[4] J. Breeden, K. Garg, and D. Panagou, "Control barrier functions in sampled-data systems," *IEEE Contr. Syst. Lett.*, vol. 6, pp. 367–372, 2021.

[5] D. R. Agrawal, H. Parwana, R. K. Cosner, U. Rosolia, A. D. Ames, and D. Panagou, "A constructive method for designing safe multirate controllers for differentially-flat systems," *IEEE Contr. Syst. Lett.*, vol. 6, pp. 2138–2143, 2021.

[6] P. Bernard, V. Andrieu, and D. Astolfi, "Observer design for continuous-time dynamical systems," *Annu. Rev. Control*, vol. 53, pp. 224–248, Jan. 2022.

[7] H. Khalil, *Nonlinear Control*. Boston, MA, USA: Pearson, 2015.

[8] S. Dean, A. Taylor, R. Cosner, B. Recht, and A. Ames, "Guaranteeing safety of learned perception modules via measurement-robust control barrier functions," in *Proc. Conf. Robot Learn.*, 2021, pp. 654–670.

[9] A. Clark, "Control barrier functions for complete and incomplete information stochastic systems," in *Proc. Amer. Control Conf. (ACC)*, 2019, pp. 2928–2935.

[10] N. Jahanshahi, P. Jagtap, and M. Zamani, "Synthesis of stochastic systems with partial information via control barrier functions," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 2441–2446, 2020.

[11] M. Ahmadi, A. Singletary, J. W. Burdick, and A. D. Ames, "Safe policy synthesis in multi-agent POMDPs via discrete-time barrier functions," in *Proc. IEEE 58th Conf. Decis. Control (CDC)*, 2019, pp. 4797–4803.

[12] H. Shim and D. Liberzon, "Nonlinear observers robust to measurement disturbances in an ISS sense," *IEEE Trans. Autom. Control*, vol. 61, no. 1, pp. 48–61, Jan. 2016.

[13] D. Pylorof, E. Bakolas, and K. S. Chan, "Design of robust Lyapunov-based observers for nonlinear systems with sum-of-squares programming," *IEEE Contr. Syst. Lett.*, vol. 4, pp. 283–288, 2020.

[14] X. Xu, P. Tabuada, J. W. Grizzle, and A. D. Ames, "Robustness of control barrier functions for safety critical control," *IFAC-PapersOnLine*, vol. 48, no. 27, pp. 54–61, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405896315024106

[15] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.

[16] A. Howell and J. K. Hedrick, "Nonlinear observer design via convex optimization," in *Proc. Amer. Control Conf. (ACC)*, vol. 3, 2002, pp. 2088–2093.

[17] A. Alessandri, "Observer design for nonlinear systems by using input-to-state stability," in *Proc. 43rd IEEE Conf. Decis. Control (CDC)*, vol. 4, 2004, pp. 3892–3897.

[18] M. Arcak and P. Kokotović, "Nonlinear observers: A circle criterion design and robustness analysis," *Automatica*, vol. 37, no. 12, pp. 1923–1930, 2001.

[19] T. Alamo, J. M. Bravo, and E. F. Camacho, "Guaranteed state estimation by zonotopes," *Automatica*, vol. 41, no. 6, pp. 1035–1043, 2005.

[20] L. Jaulin, "Nonlinear bounded-error state estimation of continuous-time systems," *Automatica*, vol. 38, no. 6, pp. 1079–1082, 2002.

[21] A. Alessandri, "Lyapunov functions for state observers of dynamic systems using Hamilton–Jacobi inequalities," *Mathematics*, vol. 8, no. 2, p. 202, 2020.

[22] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.

[23] W. W. Hager, "Lipschitz continuity for constrained processes," *SIAM J. Control Optim.*, vol. 17, no. 3, pp. 321–338, 1979.

[24] G. Wu and K. Sreenath, "Safety-critical control of a planar quadrotor," in *Proc. Amer. Control Conf. (ACC)*, 2016, pp. 2252–2258.

[25] K. Reif, F. Sonnemann, and R. Unbehauen, "An EKF-based nonlinear observer with a prescribed degree of stability," *Automatica*, vol. 34, no. 9, pp. 1119–1123, 1998. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0005109898000533

[26] F. L. Lewis, L. Xie, and D. Popa, *Optimal and Robust Estimation: With an Introduction to Stochastic Control Theory*. Boca Raton, FL, USA: CRC Press, 2017.

[27] M. W. Mueller, M. Hamer, and R. D'Andrea, "Fusing ultra-wideband range measurements with accelerometers and rate gyroscopes for quadrocopter state estimation," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May 2015, pp. 1730–1736.

[28] D. Mellinger and V. Kumar, "Minimum snap trajectory generation and control for quadrotors," in *Proc. IEEE Int. Conf. Robot. Autom.*, 2011, pp. 2520–2525.