Measurement-Robust Control Barrier Functions: Certainty in Safety with Uncertainty in State

Ryan K. Cosner, Andrew W. Singletary, Andrew J. Taylor, Tamas G. Molnar, Katherine L. Bouman, and Aaron D. Ames

***Abstract*— The increasing complexity of modern robotic systems and the environments they operate in necessitates the formal consideration of safety in the presence of imperfect measurements. In this paper we propose a rigorous framework for safety-critical control of systems with erroneous state estimates. We develop this framework by leveraging Control Barrier Functions (CBFs) and unifying the method of Backup Sets for synthesizing control invariant sets with robustness requirements—the end result is the synthesis of *Measurement-Robust Control Barrier Functions (MR-CBFs)*. This provides theoretical guarantees on safe behavior in the presence of imperfect measurements and improved robustness over standard CBF approaches. We demonstrate the efficacy of this framework both in simulation and experimentally on a Segway platform using an onboard stereo-vision camera for state estimation.**

I. INTRODUCTION

Safety is of utmost importance in many modern control applications, including autonomous vehicles, medical and industrial robotics [1]. The growing complexity of these systems demands that safety properties be rigorously encoded in the controller design. Such systems are typically described as safe if their state never leaves a prescribed *safe set*, and *Control Barrier Functions (CBFs)* [2], [3] have become increasingly popular [4], [5] as a tool for achieving safety. In this paper, we focus on two challenges related to safety-critical control realized via CBFs: finding admissible inputs and making these inputs robust to uncertainty.

The first challenge is guaranteeing that a safe control input is always available. If safe control actions exist—i.e., satisfy input constraints—over the entire safe set, the set is called *control invariant* [6]. Yet control invariance is not guaranteed in general—safe actions may not exist for all points in a given safe set. Therefore, identifying control invariant sets is critically important for implementing safety-critical controllers in robotic systems. Hamilton-Jacobi reachability analysis can be performed to compute such sets [7], but is intractable for high dimensional systems. Here we adapt the method of *Backup Sets* introduced in [8] as a computationally tractable way of achieving control invariance.

This research is supported in part by the National Science Foundation, CPS Award #1932091; DOW Chemical, project 227027AT; British Petroleum; and Aerovironment.

R. K. Cosner, A. W. Singletary, T. G. Molnar, and A. D. Ames are with the Department of Mechanical and Civil Engineering, California Institute of Technology, Pasadena, CA 91125, USA, {rkcosner, asinglet, tmolnar, ames}@caltech.edu.

A. J. Taylor and K. L. Bouman are with the Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, CA 91125, USA, {ajtaylor, klbouman}@caltech.edu.

Fig. 1. Visualization of desired Segway behavior. The Segway is driven from left to right and must not cross the red line. The transparent blue images represent the measured position whereas the opaque images represent the true position. Traditional CBFs do not account for this uncertainty.

The second challenge is that controllers rely on state measurements that are often imperfect or uncertain—especially for dynamic robotic systems. This can cause unsafe behavior if not accounted for in the control design and, as such, has been addressed from multiple perspectives. The work in [9], [10] considers robust CBF formulations with worst-case disturbance bounds to achieve safety. Safety guarantees in the presence of measurement noise are addressed from a stochastic perspective in [11], [12]. Controllers robust to state estimation errors were proposed for sampled-data-systems via an interval-arithmetic condition in [13] and for continuous systems via estimate-error bounding in [14]. In [14] safety and robustness were enforced by *Measurement-Robust Control Barrier Functions (MR-CBFs)*. This approach was inspired by vision-based control [15], [16], [17], where state information is observed through a complex transformation.

This paper presents a safety-critical control framework that allows for the synthesis of control invariant sets that are robust to measurement uncertainty, all with a view toward experimental realization. The main contributions of this work are twofold. Firstly, we integrate the method of Backup Sets for ensuring control invariance [8] with the framework of MR-CBFs [14]. This leads to practically achievable safety guarantees even in the presence of measurement uncertainty, establishing measurement-robust safety-critical control. Secondly, we present the first experimental demonstration of both MR-CBFs and the proposed method by controlling the motion of a Segway using camera data. The experiments validate the robust safety guarantees provided by our method.

II. PRELIMINARIES

First we provide a review of safety-critical control through Control Barrier Functions (CBFs) and synthesis of control

invariant sets via the Backup Set method.

A. Control Barrier Functions

Consider the nonlinear control affine system given by:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + \mathbf{g}(\mathbf{x})\mathbf{u}, \quad \mathbf{x} \in \mathbb{R}^n,\ \mathbf{u} \in \mathbb{R}^m, \tag{1}$$

where $\mathbf{f} : \mathbb{R}^n \to \mathbb{R}^n$ and $\mathbf{g} : \mathbb{R}^n \to \mathbb{R}^{n\times m}$ are locally Lipschitz continuous. Given a locally Lipschitz continuous controller $\mathbf{k} : \mathbb{R}^n \to \mathbb{R}^m$, the closed-loop dynamics are:

$$\dot{\mathbf{x}} = \mathbf{f}_{\text{cl}}(\mathbf{x}) = \mathbf{f}(\mathbf{x}) + \mathbf{g}(\mathbf{x})\mathbf{k}(\mathbf{x}), \tag{2}$$

where $\mathbf{f}_{\text{cl}} : \mathbb{R}^n \to \mathbb{R}^n$ is also locally Lipschitz continuous. Therefore, for any initial condition $\mathbf{x}(0) = \mathbf{x}_0 \in \mathbb{R}^n$ there exists an interval $I(\mathbf{x}_0) \triangleq [0, t_{\max})$ such that $\mathbf{x}(t)$ is the unique solution to (2) for $t \in I(\mathbf{x}_0)$ [18]. Throughout this paper we assume $I(\mathbf{x}_0) = [0, \infty)$.

The notion of safety is formalized by defining a *safe set* $\mathcal{C} \subset \mathbb{R}^n$ in the state space that the system must remain within. In particular, consider the set $\mathcal{C}$ as the 0-superlevel set of a continuously differentiable function $h : \mathbb{R}^n \to \mathbb{R}$:

$$\begin{aligned} \mathcal{C} &\triangleq \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) \geq 0\}, \\ \partial\mathcal{C} &\triangleq \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) = 0\}, \\ \text{Int}(\mathcal{C}) &\triangleq \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) > 0\}. \end{aligned} \tag{3}$$

We assume that zero is a regular value of h and $\mathcal{C}$ is non-empty and has no isolated points, that is, $h(\mathbf{x}) = 0 \implies \frac{\partial h}{\partial \mathbf{x}}(\mathbf{x}) \neq 0$, $\text{Int}(\mathcal{C}) \neq \emptyset$, and $\overline{\text{Int}(\mathcal{C})} = \mathcal{C}$. In this context, safety is synonymous with the forward invariance of $\mathcal{C}$:

Definition 1 (*Forward Invariance and Safety*)**.** A set $\mathcal{C} \subset \mathbb{R}^n$ is *forward invariant* if for every $\mathbf{x}_0 \in \mathcal{C}$, the solution to (2) satisfies $\mathbf{x}(t) \in \mathcal{C}$ for all $t \geq 0$. The closed-loop system (2) is *safe* with respect to set $\mathcal{C}$ if $\mathcal{C}$ is forward invariant.

We call a continuous function $\alpha : \mathbb{R} \to \mathbb{R}$ an extended class-$\mathcal{K}_\infty$ ($\mathcal{K}_{\infty,e}$) if it is strictly monotonically increasing and satisfies $\alpha(0) = 0$, $\lim_{r\to-\infty} \alpha(r) = -\infty$, and $\lim_{r\to\infty} \alpha(r) = \infty$. Control Barrier Functions (CBF) [2] can be used to synthesize controllers which ensure the safety of the closed-loop system (2) with respect to a given set $\mathcal{C}$.

Definition 2 (*Control Barrier Function (CBF)*)**.** Let $\mathcal{C} \subset \mathbb{R}^n$ be a safe set given by (3). The function h is a *Control Barrier Function* (CBF) for (1) on $\mathcal{C}$ if there exists $\alpha \in \mathcal{K}_{\infty,e}$ such that for all $\mathbf{x} \in \mathcal{C}$:

$$\sup_{\mathbf{u}\in\mathbb{R}^m} \dot{h}(\mathbf{x}, \mathbf{u}) \triangleq \underbrace{\frac{\partial h}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x})}_{L_\mathbf{f} h(\mathbf{x})} + \underbrace{\frac{\partial h}{\partial \mathbf{x}}(\mathbf{x})\mathbf{g}(\mathbf{x})}_{L_\mathbf{g} h(\mathbf{x})}\mathbf{u} \geq -\alpha(h(\mathbf{x})), \tag{4}$$

where $L_\mathbf{f} h : \mathbb{R}^n \to \mathbb{R}$ and $L_\mathbf{g} h : \mathbb{R}^n \to \mathbb{R}^m$ are the Lie derivatives of h with respect to $\mathbf{f}$ and $\mathbf{g}$, respectively.

Intuitively, the CBF constraint (4) requires the system to slow down as it approaches the boundary of the safe set (the right-hand side of (4) increases to 0 as the value of h approaches 0). A main result in [19], [20] relates CBFs to the safety of the closed-loop system (2) with respect to $\mathcal{C}$:

Theorem 1. *Given a safe set $\mathcal{C} \subset \mathbb{R}^n$, if h is a CBF for* (1) *on $\mathcal{C}$, then any locally Lipschitz continuous controller $\mathbf{k} : \mathbb{R}^n \to \mathbb{R}^m$ satisfying*

$$L_\mathbf{f} h(\mathbf{x}) + L_\mathbf{g} h(\mathbf{x})\mathbf{k}(\mathbf{x}) \geq -\alpha(h(\mathbf{x})) \tag{5}$$

for all $\mathbf{x} \in \mathcal{C}$, renders the system (2) *safe w.r.t. $\mathcal{C}$.*

Given a nominal (but not necessarily safe) locally Lipschitz continuous controller $\mathbf{k}_d : \mathbb{R}^n \to \mathbb{R}^m$ and a CBF h, the CBF-Quadratic Program (CBF-QP) [2] ensures safety:

$$\begin{aligned} \mathbf{k}(\mathbf{x}) = \ \underset{\mathbf{u}\in\mathbb{R}^m}{\text{argmin}} \quad & \frac{1}{2}\|\mathbf{u} - \mathbf{k}_d(\mathbf{x})\|_2^2 \\ \text{s.t.} \quad & L_\mathbf{f} h(\mathbf{x}) + L_\mathbf{g} h(\mathbf{x})\mathbf{u} \geq -\alpha(h(\mathbf{x})). \end{aligned} \tag{CBF-QP}$$

B. Generating Control Invariant Sets via Backup Sets

To guarantee that a safe control action exists, one needs to ensure the existence of a function h satisfying the CBF condition (4). For a given safe-set $\mathcal{C}$, fulfilling this requirement can be nontrivial and potentially impossible. To this end, we restrict our focus to a set $\mathcal{C}_I \subseteq \mathcal{C}$ which is control invariant:

Definition 3 (*Control Invariance*)**.** A set $\mathcal{C}_I \subseteq \mathcal{C}$ is *control invariant* if there exists a controller $\mathbf{k} : \mathbb{R}^n \to \mathbb{R}^m$ such that $\mathcal{C}_I$ is forward invariant with respect to the system (2).

While directly computing control invariant sets remains challenging in general, we may define one implicitly via a backup set [8]. Consider a desired safe set $\mathcal{C} \subset \mathbb{R}^n$, which is not necessarily control invariant. Suppose there exists a set $\mathcal{C}_B \subset \mathcal{C}$, defined as the 0-superlevel set of a continuously differentiable function $h_B : \mathbb{R}^n \to \mathbb{R}$, which is known *a priori* to be control invariant and can be rendered forward invariant by a known locally Lipschitz continuous *backup controller* $\mathbf{k}_B : \mathbb{R}^n \to \mathbb{R}^m$. We refer to $\mathcal{C}_B$ as the *backup set*. For simple backup controllers (such as linear state feedback controllers designed for the linearization of a system) it is possible to find analytical expressions for local regions of attraction to serve as backup sets. Alternatively, numerical tools such as Sums-of-Squares (SOS) may be used to synthesize control invariant sets [21].

We extend the backup set to a larger control invariant set $\mathcal{C}_I \subset \mathbb{R}^n$, satisfying $\mathcal{C}_B \subseteq \mathcal{C}_I \subseteq \mathcal{C}$, by considering the *backup trajectory* over a finite and fixed time $T \in \mathbb{R}_{>0}$ as follows. By assumption, for any $\mathbf{x} \in \mathbb{R}^n$ there exists a unique solution $\boldsymbol{\varphi} : [0, T] \to \mathbb{R}^n$ satisfying:

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}\tau}\boldsymbol{\varphi}(\tau) &= \mathbf{f}(\boldsymbol{\varphi}(\tau)) + \mathbf{g}(\boldsymbol{\varphi}(\tau))\mathbf{k}_B(\boldsymbol{\varphi}(\tau)), \\ \boldsymbol{\varphi}(0) &= \mathbf{x}. \end{aligned} \tag{6}$$

The solution $\boldsymbol{\varphi}$ may be interpreted as the evolution of the system over the interval $[0, T]$ from a state, $\mathbf{x}$, under the backup controller $\mathbf{k}_B$. In particular, the current state $\mathbf{x}(t)$ may be used as initial condition in specifying $\boldsymbol{\varphi}$. We denote $\phi_\tau^{\mathbf{k}_b}(\mathbf{x}) \triangleq \boldsymbol{\varphi}(\tau)$ for the initial condition $\mathbf{x}$.

Using this notation, we may define the set $\mathcal{C}_I \subseteq \mathcal{C}$ as:

$$\mathcal{C}_I = \left\{ \mathbf{x} \in \mathcal{C} \;\middle|\; \begin{array}{c} h(\phi_\tau^{\mathbf{k}_B}(\mathbf{x})) \geq 0, \forall \tau \in [0, T] \\ \text{and} \\ h_B(\phi_T^{\mathbf{k}_B}(\mathbf{x})) \geq 0 \end{array} \right\}. \tag{7}$$

The first inequality implies safety under the backup policy ($\phi_\tau^{\mathbf{k}_B}(\mathbf{x}) \in \mathcal{C}$ for all $\tau \in [0,T]$), and the second inequality implies the backup trajectory reaches $\mathcal{C}_B$ by time T ($\phi_T^{\mathbf{k}_B}(\mathbf{x}) \in \mathcal{C}_B$). The set $\mathcal{C}_I$ is thus control invariant as there exists at least one controller, $\mathbf{k}_B$, which renders it forward invariant. While $\mathcal{C}_I$ is not necessarily the largest control invariant subset of $\mathcal{C}$ (see *viability kernel*, [6]), the backup sets provide a computationally tractable method for finding an under-approximation of the largest control invariant set.

For notational simplicity, we define the continuously differentiable functions $\overline{h}_\tau : \mathbb{R}^n \to \mathbb{R}$ and $\overline{h}_B : \mathbb{R}^n \to \mathbb{R}$ as:

$$\overline{h}_\tau(\mathbf{x}) \triangleq h(\phi_\tau^{\mathbf{k}_B}(\mathbf{x})), \qquad \overline{h}_B(\mathbf{x}) \triangleq h_B(\phi_T^{\mathbf{k}_B}(\mathbf{x})). \tag{8}$$

Given these definitions, the CBF condition (4) can then be specified for the set $\mathcal{C}_I$ at a point $\mathbf{x} \in \mathcal{C}_I$ as follows:

$$\begin{aligned} &L_\mathbf{f}\overline{h}_\tau(\mathbf{x}) + L_\mathbf{g}\overline{h}_\tau(\mathbf{x})\mathbf{u} \geq -\alpha(\overline{h}_\tau(\mathbf{x})), \quad \forall \tau \in [0,T], \\ &L_\mathbf{f}\overline{h}_B(\mathbf{x}) + L_\mathbf{g}\overline{h}_B(\mathbf{x})\mathbf{u} \geq -\alpha(\overline{h}_B(\mathbf{x})). \end{aligned} \tag{9}$$

Any locally Lipschitz continuous controller that takes values satisfying (9) for all $\mathbf{x} \in \mathcal{C}_I$ will keep the closed loop system (2) safe with respect to $\mathcal{C}_I$; see [22, p. 6].

We note that enforcing the first constraint in (9) is not necessarily tractable as it must hold for all $\tau \in [0,T]$. To resolve this, it can be reduced to a finite collection of more conservative constraints through constraint tightening. A controller which implements the finite number of tightened constraints, and thus renders (2) safe with respect to $\mathcal{C}_I$, is given by the Backup Set Quadratic Program (BS-QP):

$$\begin{aligned} \mathbf{k}(\mathbf{x}) = \ \underset{\mathbf{u}\in\mathbb{R}^m}{\operatorname{argmin}} \quad & \frac{1}{2}\|\mathbf{u} - \mathbf{k}_d(\mathbf{x})\|_2^2 \qquad \text{(BS-QP)} \\ \text{s.t.} \quad & L_\mathbf{f}\overline{h}_{\tau_j}(\mathbf{x}) + L_\mathbf{g}\overline{h}_{\tau_j}(\mathbf{x})\mathbf{u} \geq -\alpha(h_{\tau_j}(\mathbf{x}) - \mu), \\ & L_\mathbf{f}\overline{h}_B(\mathbf{x}) + L_\mathbf{g}\overline{h}_B(\mathbf{x})\mathbf{u} \geq -\alpha(h_B(\mathbf{x})), \end{aligned}$$

for all $\tau_j \in \{0, \Delta_t, \ldots, T\}$, where $\Delta_t \in \mathbb{R}_{>0}$ is a time-step such that $T/\Delta_t \in \mathbb{N}$ and $\mu \in \mathbb{R}_{>0}$ satisfies:

$$\mu \geq \frac{\Delta_t}{2}\mathfrak{L}_h \sup_{\mathbf{x}\in\mathcal{C}} \|\mathbf{f}(\mathbf{x}) + \mathbf{g}(\mathbf{x})\mathbf{k}_B(\mathbf{x})\|_2, \tag{10}$$

with $\mathfrak{L}_h \in \mathbb{R}_{>0}$ a Lipschitz constant for h on $\mathcal{C}$ [8, Thm. 1].

III. Measurement Robustness

The guarantees endowed by the above controllers require perfect knowledge of the state $\mathbf{x}$, which is unattainable in practice. In particular, the relationship between the state of the system and the measurements, such as images or point clouds, can be complex and not fully known [15], [16], [17]. In this section we revisit measurement-model uncertainty and present our main result in the form of a measurement-robust version of the BS-QP.

A. Measurement-Model Uncertainty

To achieve robustness, we consider a structured form of measurement-model uncertainty that modifies the CBF condition (4) [14]. We assume the state $\mathbf{x}$ is not directly available, but rather a state-dependent sensor measurement:

$$\mathbf{y} = \mathbf{p}(\mathbf{x}), \tag{11}$$

where $\mathbf{y} \in \mathbb{R}^k$ and $\mathbf{p} : \mathbb{R}^n \to \mathbb{R}^k$ is locally Lipschitz continuous. An estimate of the state, $\widehat{\mathbf{x}} \in \mathbb{R}^n$, is reconstructed from $\mathbf{y}$ (such as through measurement models or data-driven methods [16], [17]). In particular, we assume the map from measurements to state estimates is imperfect (does not recover the true state exactly), and is given by the locally Lipschitz continuous function $\widehat{\mathbf{q}} : \mathbb{R}^k \to \mathbb{R}^n$ as follows:

$$\widehat{\mathbf{x}} \triangleq \widehat{\mathbf{q}}(\mathbf{y}) = \mathbf{x} + \mathbf{e}(\mathbf{x}), \tag{12}$$

where the state error function $\mathbf{e} : \mathbb{R}^n \to \mathbb{R}^n$ is unknown and implicitly defined by $\widehat{\mathbf{q}}$.

The error function $\mathbf{e}$ can often be characterized via upper bounds on measurement-model uncertainty. In particular, we assume that while the state error $\mathbf{e}(\mathbf{x})$ is not known for a given state $\mathbf{x} \in \mathbb{R}^n$, it is within a compact error set $\mathcal{E}(\mathbf{y})$ specified by a set-valued function $\mathcal{E} : \mathbb{R}^k \to \mathcal{P}(\mathbb{R}^n)$ ($\mathcal{P}$ denotes the power set), that is, we have $\mathbf{e}(\mathbf{x}) \in \mathcal{E}(\mathbf{y}) = \mathcal{E}(\mathbf{p}(\mathbf{x}))$. The error set can be conservatively characterized via the function $\epsilon : \mathbb{R}^k \to \mathbb{R}_{\geq 0}$ defined as:

$$\epsilon(\mathbf{y}) \triangleq \max_{\mathbf{e}\in\mathcal{E}(\mathbf{y})} \|\mathbf{e}\|_2. \tag{13}$$

Since the controller only has access to the measurement and the state estimate, systems with measurement-model uncertainty evolve according to:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + \mathbf{g}(\mathbf{x})\mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}}). \tag{14}$$

Qualitatively this uncertainty is similar to error in the dynamics model since the true values of $\mathbf{f}(\mathbf{x})$ and $\mathbf{g}(\mathbf{x})$ are unknown to the controller. The error bound can be used to synthesize controllers which render such systems provably safe as follows [14]:

Theorem 2. *Given a safe set $\mathcal{C} \subset \mathbb{R}^n$, assume that $L_\mathbf{f}h$, $L_\mathbf{g}h$, and $\alpha \circ h$ are Lipschitz continuous on $\mathcal{C}$ with Lipschitz constants $\mathfrak{L}_{L_\mathbf{f}h}, \mathfrak{L}_{L_\mathbf{g}h}$, and $\mathfrak{L}_{\alpha\circ h} \in \mathbb{R}_{\geq 0}$, respectively. Define the function $\epsilon : \mathbb{R}^k \to \mathbb{R}_{\geq 0}$ as in* (13)*, and define the functions $a, b : \mathbb{R}^k \to \mathbb{R}_{\geq 0}$ as $a(\mathbf{y}) = (\mathfrak{L}_{L_\mathbf{f}h} + \mathfrak{L}_{\alpha\circ h})\epsilon(\mathbf{y})$ and $b(\mathbf{y}) = \mathfrak{L}_{L_\mathbf{g}h}\epsilon(\mathbf{y})$. If $\mathbf{k} : \mathbb{R}^k \times \mathbb{R}^n \to \mathbb{R}^m$ is a Lipschitz continuous controller satisfying:*

$$\begin{aligned} &L_\mathbf{f}h(\widehat{\mathbf{x}}) + L_\mathbf{g}h(\widehat{\mathbf{x}})\mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}}) \\ &\qquad - (a(\mathbf{y}) + b(\mathbf{y})\|\mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}})\|_2) \geq -\alpha(h(\widehat{\mathbf{x}})) \end{aligned} \tag{15}$$

for all $\mathbf{x} \in \mathcal{C}$, with $\mathbf{y} = \mathbf{p}(\mathbf{x})$ and $\widehat{\mathbf{x}} = \widehat{\mathbf{q}}(\mathbf{y})$, then the system (14) *is safe with respect to $\mathcal{C}$.*

A continuously differentiable function $h : \mathbb{R}^n \to \mathbb{R}$ for which such a controller exists is termed a Measurement-Robust Control Barrier Function (MR-CBF) [14]. As compared to the original CBF constraint (4), the MR-CBF constraint (15) adds additional terms incorporating bounds on the measurement error that ensure that the system is safe with respect to all possible states which could have generated the measurement. The original CBF constraint is recovered in the absence of measurement error, i.e. when $\epsilon(\mathbf{y}) = 0$.

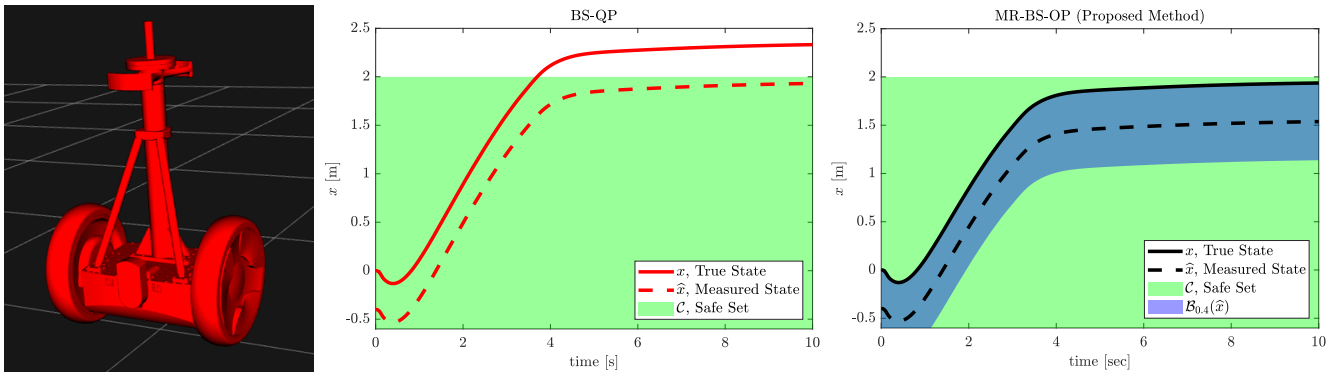

Fig. 2. Simulation results for a measurement model of $\widehat{x} = x - 0.4$ m and constant desired velocity of 1 m/s. **(Left)** An image of the simulated Segway model. **(Center)** Trajectories generated using the BS-QP. Solid line represents the true state, dashed line shows the estimated state, and green region indicates the safe set $\mathcal{C}$. The true trajectory fails to be safe and exits the safe set at $t = 3$ s. **(Right)** Trajectories generated using the MR-BS-OP. An additional robustness region is plotted in blue to indicate the set of of true states which the control input renders safe. Both the true and measured trajectories are safe demonstrating the robustness of the MR-BS-OP when compared to the BS-QP.

B. Measurement-Robust Backup Set Optimization Program

In this section we present our main result in the form of a safety-critical control paradigm that is robust to measurement uncertainty. This is accomplished by unifying the Backup Set method with MR-CBFs, using the MR-CBF condition (15) the finite set of constraints imposed in the BS-QP become:

$$\begin{aligned} &L_{\mathbf{f}}\overline{h}_{\tau_j}(\widehat{\mathbf{x}}) + L_{\mathbf{g}}\overline{h}_{\tau_j}(\widehat{\mathbf{x}})\mathbf{u} \\ &\quad - (a_{\tau_j}(\mathbf{y}) + b_{\tau_j}(\mathbf{y})\|\mathbf{u}\|_2) \geq -\alpha(\overline{h}_{\tau_j}(\widehat{\mathbf{x}}) - \mu), \\ &L_{\mathbf{f}}\overline{h}_{B}(\widehat{\mathbf{x}}) + L_{\mathbf{g}}\overline{h}_{B}(\widehat{\mathbf{x}})\mathbf{u} \\ &\quad - (a_{B}(\mathbf{y}) + b_{B}(\mathbf{y})\|\mathbf{u}\|_2) \geq -\alpha(\overline{h}_{B}(\widehat{\mathbf{x}})), \end{aligned} \tag{16}$$

with parameter functions:

$$\begin{aligned} a_{\tau_j}(\mathbf{y}) &= (\mathfrak{L}_{L_{\mathbf{f}}\overline{h}_{\tau_j}} + \mathfrak{L}_{\alpha}\mathfrak{L}_{\overline{h}_{\tau_j}})\epsilon(\mathbf{y}), \quad b_{\tau_j}(\mathbf{y}) = \mathfrak{L}_{L_{\mathbf{g}}\overline{h}_{\tau_j}}\epsilon(\mathbf{y}), \\ a_{B}(\mathbf{y}) &= (\mathfrak{L}_{L_{\mathbf{f}}\overline{h}_{B}} + \mathfrak{L}_{\alpha}\mathfrak{L}_{\overline{h}_{B}})\epsilon(\mathbf{y}), \quad b_{B}(\mathbf{y}) = \mathfrak{L}_{L_{\mathbf{g}}\overline{h}_{B}}\epsilon(\mathbf{y}), \end{aligned} \tag{17}$$

for all $\tau_j \in \{0, \Delta_t, \dots, T\}$, with $\epsilon(\mathbf{y})$ defined as in (13) and $\mathfrak{L}$ represents the Lipschitz constant of its subscripted function on $\mathbb{R}^n$. These constructions enable the following definition:

Definition 4 (*Measurement-Robust Implicit Safe Set*)**.** The set $\mathcal{C}_I \subseteq \mathcal{C} \subseteq \mathbb{R}^n$ defined as in (7) is a *Measurement-Robust Implicit Safe Set* (MRISS) for the error bound $\epsilon : \mathbb{R}^k \to \mathbb{R}_{\geq 0}$ with parameter functions $(a_0, b_0, \dots, a_{\Delta_t}, b_{\Delta_t}, a_B, b_B) : \mathbb{R}^k \to \mathbb{R}_{\geq 0}$ if:

- the functions $\{\overline{h}_0, \overline{h}_{\Delta_t}, \dots, \overline{h}_T, \overline{h}_B\}$, their Lie derivatives, and α are Lipschitz continuous on $\mathcal{C}_I$,
- the constant $\mu \in \mathbb{R}_{\geq 0}$ satisfies (10),
- and for all $\mathbf{x} \in \mathcal{C}_I$ there exists $\mathbf{u} \in \mathbb{R}^m$ satisfying (16).

Next, using this definition, we show that the safety of such sets can be made robust to measurement model uncertainty.

Theorem 3. *Given a MRISS $\mathcal{C}_I$, if $\mathbf{k} : \mathbb{R}^k \times \mathbb{R}^n \to \mathbb{R}^m$ is a Lipschitz continuous controller that satisfies* (16) *with parameter functions* (17) *for all $\mathbf{x} \in \mathcal{C}_I$ with $\mathbf{y} = \mathbf{p}(\mathbf{x})$ and $\widehat{\mathbf{x}} = \widehat{\mathbf{q}}(\mathbf{y})$, then system* (14) *is safe with with respect to $\mathcal{C}_I$.*

Proof. For any function $\overline{h} \in \{\overline{h}_0, \overline{h}_{\Delta_t}, \dots, \overline{h}_T, \overline{h}_B\}$ let

$$c(\mathbf{x}, \mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}})) = L_{\mathbf{f}}\overline{h}(\mathbf{x}) + L_{\mathbf{g}}\overline{h}(\mathbf{x})\mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}}) + \alpha(\overline{h}(\mathbf{x}) - \nu),$$

where we choose $\nu = \mu$ if $\overline{h} = \overline{h}_{\tau_j}$ and $\nu = 0$ if $\overline{h} = \overline{h}_B$. It follows by Lipschitz continuity that:

$$\begin{aligned} \|L_{\mathbf{f}}\overline{h}(\widehat{\mathbf{x}}) - L_{\mathbf{f}}\overline{h}(\mathbf{x})\|_2 &\leq \mathfrak{L}_{L_{\mathbf{f}}\overline{h}}\epsilon(\mathbf{y}), \\ \|\alpha(\overline{h}(\widehat{\mathbf{x}}) - \nu) - \alpha(\overline{h}(\mathbf{x}) - \nu)\|_2 &\leq \mathfrak{L}_{\alpha}\mathfrak{L}_{\overline{h}}\epsilon(\mathbf{y}), \\ \|L_{\mathbf{g}}\overline{h}(\widehat{\mathbf{x}}) - L_{\mathbf{g}}\overline{h}(\mathbf{x})\|_2\|\mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}})\|_2 &\leq \mathfrak{L}_{L_{\mathbf{g}}\overline{h}}\epsilon(\mathbf{y})\|\mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}})\|_2. \end{aligned}$$

As $\mathbf{k}$ satisfies (16), we have that:

$$\begin{aligned} &c(\mathbf{x},\mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}})) \\ &\quad = c(\widehat{\mathbf{x}}, \mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}})) + c(\mathbf{x}, \mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}})) - c(\widehat{\mathbf{x}}, \mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}})) \\ &\quad \geq c(\widehat{\mathbf{x}}, \mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}})) - (a(\mathbf{y}) + b(\mathbf{y})\|\mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}})\|_2) \geq 0. \end{aligned}$$

Since $c(\mathbf{x}, \mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}})) \geq 0$ and μ satisfies (10), we have that the system (14) is safe with respect to $\mathcal{C}_I$ by [8, Lemma 2]. □

This result allows us to present an alternative to the BS-QP controller which adds the measurement-robustness of MR-CBFs. The constraints (16) can be directly integrated into a Measurement-Robust Backup Set Optimization Program controller MR-BS-OP as:

$$\begin{aligned} \mathbf{k}(\mathbf{y}, \widehat{\mathbf{x}}) = \underset{\mathbf{u} \in \mathbb{R}^m}{\operatorname{argmin}} \quad & \frac{1}{2}\|\mathbf{u} - \mathbf{k}_d(\widehat{\mathbf{x}})\|_2^2 \qquad \text{(MR-BS-OP)} \\ \text{s.t.} \quad & L_{\mathbf{f}}\overline{h}_{\tau_j}(\widehat{\mathbf{x}}) + L_{\mathbf{g}}\overline{h}_{\tau_j}(\widehat{\mathbf{x}})\mathbf{u} \\ & \quad - (a_{\tau_j}(\mathbf{y}) + b_{\tau_j}(\mathbf{y})\|\mathbf{u}\|_2) \geq -\alpha(\overline{h}_{\tau_j}(\widehat{\mathbf{x}}) - \mu) \\ & L_{\mathbf{f}}\overline{h}_{B}(\widehat{\mathbf{x}}) + L_{\mathbf{g}}\overline{h}_{B}(\widehat{\mathbf{x}})\mathbf{u} \\ & \quad - (a_{B}(\mathbf{y}) + b_{B}(\mathbf{y})\|\mathbf{u}\|_2) \geq -\alpha(\overline{h}_{B}(\widehat{\mathbf{x}})) \end{aligned}$$

for all $\tau_j \in \{0, \Delta_t, \dots, T\}$. Since this controller is a second-order cone program (SOCP), there exist a variety of solvers capable of implementing it including ECOS [23]. Notably, the conservative nature of the method scales with the bound on the measurement-model error $\epsilon(\mathbf{y})$ and the MR-BS-OP reduces to the BS-QP when $\epsilon(\mathbf{y}) = 0$. We remark that the feasibility of MR-BS-OP for all $\widehat{\mathbf{x}} \in \mathbb{R}^n$ can be ensured by adding a slack variable to the optimization problem. The impact of the slack variable on safety can be understood via the concept of projection-to-state safety [24].

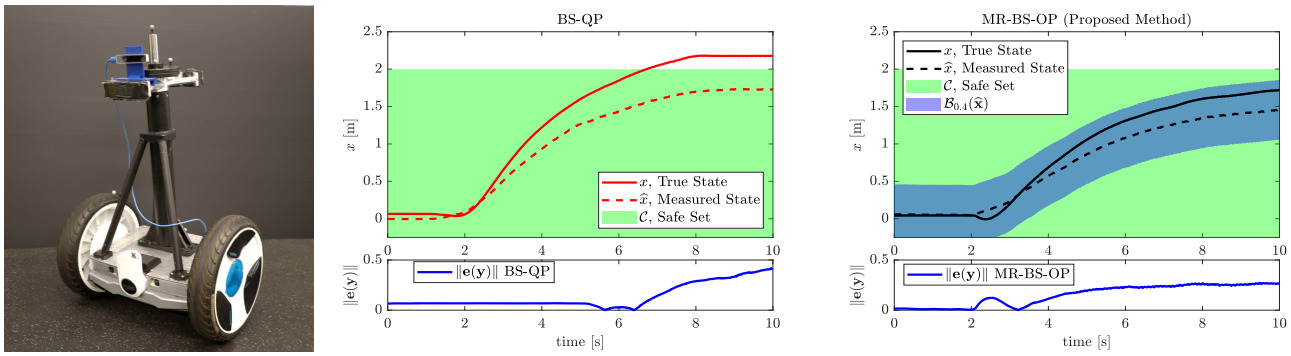

Fig. 3. Experimental results using SLAM from the onboard Intel RealSense T265 and constant desired velocity of 1 m/s. The notation and color schemes are the same as in Fig. 2. **(Left)** An image of the Segway platform. **(Center)** Trajectories generated using the BS-QP. The true trajectory exits the safe set at $t = 6.7$ s. The measurement error is plotted in blue. **(Right)** Trajectories generated using the MR-BS-OP. Both the true and measured trajectories are safe demonstrating the robustness of the MR-BS-OP when compared to the BS-QP.

IV. EXPERIMENTAL RESULTS

In this section we demonstrate the efficacy of the proposed MR-BS-OP controller on a modified Ninebot E+ Segway platform in both simulation and hardware experiment.

We consider a 4-dimensional asymmetrical Segway model shown in Figures 2 and 3. The state of the system consists of the position x, the forward velocity $\dot{x}$, the pitch angle ψ, and the pitch rate $\dot{\psi}$. The equations of motion were derived using Newton-Euler method treating the Segway as an inverted pendulum with control input as torque command at the wheels; see [8]. The Backup Set method for generating control invariant sets is particularly relevant for this system due to its non-minimum phase dynamics.

The desired safe set was chosen empirically to be the set of states with position less than 2 m from the origin, i.e. $\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : x \leq 2\}$ and $h(\mathbf{x}) = 2 - x$. The backup controller was an LQR controller on the linearized system dynamics and the backup set was an estimate of the region of attraction of the LQR controller to the upright equilibrium state, given by a quadratic Lyapunov function. This set is then translated to match the current position of the Segway, while not allowing it to exceed the set boundary. The functions $\overline{h}_\tau$, $\tau \in [0, T]$ were converted into four CBFs $\overline{h}_{\tau_j}$. Lastly, the Lipschitz constants for $\overline{h}_{\tau_j}$ were found explicitly by inspection of the Segway dynamics and the Lipschitz constants for $\overline{h}_B$ were found by sampling the state space in simulation and taking the largest numerical gradient.

Simulation Results. The MR-BS-OP was first validated in simulation in a ROS-based environment, found here[1]. Measurement-model uncertainty was achieved by artificially adding a constant error of -0.4 m to the true state. The simple test scenario involved driving the Segway forward with a constant desired velocity of 1 m/s. As seen in Figure 2, the MR-BS-OP provided robustness to this error. Importantly, without measurement-robustness, the system would be unsafe due to uncertainty in the state.

Hardware Results. The MR-BS-OP was then implemented on hardware. State estimates for $\dot{x}, \psi$, and $\dot{\psi}$ were found using wheel incremental encoders and a VectorNav VN-100 IMU. The position estimate for x was obtained from an Intel RealSense T265 onboard camera running proprietary Visual Inertial Odometry (VIO) based SLAM. Onboard computation was performed by a Jetson TX2 which computes control actions and relays them to the low-level motor controllers. The TX2 concurrently runs Linux with ROS, enabling external communication and logging, and the ERIKA3 real-time operating system, which enables real-time low-level communication and computation of the control action.

As the $(\dot{x}, \psi, \dot{\psi})$ state estimates provided by the encoders and IMU are highly accurate, we focus on making the system robust to measurement error in its vision-based position estimate $\hat{x}$. An OptiTrack motion capture system was used in laboratory experiments to provide x estimates which are considered true. These closely matched the encoder position estimates for short trials, so the encoder x estimates were considered true in the outdoor experiments. This data was used to determine the error bound $\epsilon(\mathbf{y})$ that appears in the MR-CBF constraint when using the onboard camera.

The value $\epsilon(\mathbf{y}) = 0.4$ was chosen as an upper bound on the measurement error for all $\mathbf{y} \in \mathbf{p}(\mathcal{C})$. The MR-BS-OP was implemented at the embedded level in the ERIKA3 operating system using the ECOS SOCP solver [23]. The desired controller $\mathbf{k}_d$ was a proportional-derivative controller tracking user velocity inputs. The backup trajectory $\phi_\tau^{\mathbf{k}_B}(\hat{\mathbf{x}})$ and its partial derivatives were approximated via Euler integration using a time step of $\Delta t = 5$ ms and the time used to expand the backup set $\mathcal{C}_B$ to $\mathcal{C}_I$ was $T = 1$ s. The MR-BS-OP ran at 250 Hz with 5 decision variables, 4 linear constraints, and 6 second order cone constraints and saturated at ± 20 Nm.

To demonstrate the method, a simple scenario is executed on the Segway in which it is driven forward at a desired velocity of 1 m/s. This scenario is performed with both the BS-QP and the MR-BS-OP. The results of these experiments can be found in Figure 3, images from the experiment can be seen in Figure 4, and a video can be found at [25]. With the BS-QP controller the estimated state $\hat{\mathbf{x}}$ remains safe, but the true state $\mathbf{x}$ becomes unsafe whereas with the MR-BS-OP controller both the estimated and the true state are kept safe. This highlights the importance of providing robustness against measurement uncertainty, as achieved by Theorem 3.

[1]Simulation code `github.com/rkcosner/mrcbf_IROS21.git`

Fig. 4. Images from the experiment using the MR-BS-OP controller. The Segway is piloted towards a wall of yellow boxes and the controller ensures that it remains safe, i.e. that it does not crash into the boxes. **(Top)** Time lapse of the Segway trajectory. **(Bottom)** Camera images taken from the perspective of the Segway throughout the experiment. The images are displayed in chronological order from left to right. A video can be found at [25].

V. CONCLUSION

This paper established robust controller synthesis with formal safety guarantees for systems relying on uncertain measurements. We approached this problem through the framework of CBFs. We additionally highlighted the importance of control invariant sets and experimentally implemented the Backup Set method to produce such a set for a Segway. Our theoretical construction culminated in the integration of the Backup Set method with MR-CBFs, which provides robustness to state measurement uncertainty in the safety guarantees. We implemented the proposed control method on a Segway platform and demonstrated robustly safe operation in experiments. Future work includes addressing feasibility of the MR-BS-OP for general systems and developing online methods to efficiently identify the required error bound in the context of probabilistic and time-varying uncertainties.

REFERENCES

[1] J. C. Knight, "Safety critical systems: challenges and directions," in *International Conference on Software Engineering (ICSE)*, 2002, pp. 547–550.

[2] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *Transactions on Automatic Control*, vol. 62, no. 8, 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] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *European Control Conference (ECC)*. IEEE, 2019, pp. 3420–3431.

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

[6] J.-P. Aubin, A. M. Bayen, and P. Saint-Pierre, *Viability theory: new directions*. Springer Science & Business Media, 2011.

[7] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-Jacobi reachability: A brief overview and recent advances," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*. IEEE, 2017, pp. 2242–2253.

[8] T. Gurriet, M. Mote, A. Singletary, P. Nilsson, E. Feron, and A. D. Ames, "A scalable safety critical control framework for nonlinear systems," *IEEE Access*, vol. 8, pp. 187 249–187 275, 2020.

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

[10] R. Takano and M. Yamakita, "Robust constrained stabilization control using control Lyapunov and control barrier function in the presence of measurement noises," in *Conference on Control Technology and Applications (CCTA)*. IEEE, 2018, pp. 300–305.

[11] A. Clark, "Control barrier functions for complete and incomplete information stochastic systems," in *American Control Conference (ACC)*. IEEE, 2019, pp. 2928–2935.

[12] P. Nilsson and A. D. Ames, "Lyapunov-like conditions for tight exit probability bounds through comparison theorems for SDEs," in *American Control Conference (ACC)*. IEEE, 2020, pp. 5175–5181.

[13] A. Singletary, Y. Chen, and A. D. Ames, "Control barrier functions for sampled-data systems with input delays," *arXiv preprint arXiv:2005.06418*, 2020.

[14] S. Dean, A. J. Taylor, R. K. Cosner, B. Recht, and A. D. Ames, "Guaranteeing safety of learned perception modules via measurement-robust control barrier functions," *arXiv preprint arXiv:2010.16001*, 2020.

[15] F. Codevilla, M. Müller, A. López, V. Koltun, and A. Dosovitskiy, "End-to-end driving via conditional imitation learning," in *International Conference on Robotics and Automation (ICRA)*. IEEE, 2018, pp. 1–9.

[16] A. Lambert, A. Shaban, A. Raj, Z. Liu, and B. Boots, "Deep forward and inverse perceptual models for tracking and prediction," in *International Conference on Robotics and Automation (ICRA)*. IEEE, 2018, pp. 675–682.

[17] S. Tang, V. Wüest, and V. Kumar, "Aggressive flight with suspended payloads using vision-based control," *Robotics and Automation Letters*, vol. 3, no. 2, pp. 1152–1159, 2018.

[18] L. Perko, *Differential equations and dynamical systems*. Springer Science & Business Media, 2013, vol. 7.

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

[20] 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.

[21] W. Tan and A. Packard, "Stability region analysis using sum of squares programming," in *2006 American Control Conference*, 2006, pp. 2297–2302.

[22] T. Gurriet, M. Mote, A. D. Ames, and E. Feron, "An online approach to active set invariance," in *Conference on Decision & Control (CDC)*. IEEE, 2018, pp. 3592–3599.

[23] A. Domahidi, E. Chu, and S. Boyd, "ECOS: An SOCP solver for embedded systems," in *European Control Conference (ECC)*. IEEE, 2013, pp. 3071–3076.

[24] A. J. Taylor, A. Singletary, Y. Yue, and A. D. Ames, "A control barrier perspective on episodic learning via projection-to-state safety," *IEEE Control Systems Letters*, vol. 5, no. 3, pp. 1019–1024, 2021.

[25] Supplementary video, https://vimeo.com/520247516.