Disturbance-Robust Backup Control Barrier Functions: Safety Under Uncertain Dynamics

David E.J. van Wijk[1], Samuel Coogan[2], Tamas G. Molnar[3], Manoranjan Majji[1], and Kerianne L. Hobbs[4]

***Abstract*—Obtaining a controlled invariant set is crucial for safety-critical control with control barrier functions (CBFs) but is non-trivial for complex nonlinear systems and constraints. Backup control barrier functions allow such sets to be constructed online in a computationally tractable manner by examining the evolution (or flow) of the system under a known backup control law. However, for systems with unmodeled disturbances, this flow cannot be directly computed, making the current methods inadequate for assuring safety in these scenarios. To address this gap, we leverage bounds on the nominal and disturbed flow to compute a forward invariant set online by ensuring safety of an expanding norm ball tube centered around the nominal system evolution. We prove that this set results in robust control constraints which guarantee safety of the disturbed system via our *Disturbance-Robust Backup Control Barrier Function (DR-bCBF)* solution. The efficacy of the proposed framework is demonstrated in simulation, applied to a double integrator problem and a rigid body spacecraft rotation problem with rate constraints.**

I. Introduction

Control barrier functions (CBFs) [1], are a popular approach to assuring safety of autonomous systems by encoding safety into existing controllers and providing sufficient conditions for forward invariance of safe sets. However, obtaining safe sets for which every state has a safe control action (a.k.a. *controlled invariant* sets) is difficult for high-dimensional systems, especially when considering input bounds. Additionally, dynamics models are seldom perfect. In this letter we seek to solve both of these problems simultaneously.

To address the problem of controlled invariance, we adapt the *backup set method* [2]–[4] based on online backward reachability. This method establishes a controlled invariant safe set *implicitly* using the flow of the system under a prescribed backup control law. This approach is computationally tractable even for complex systems. For affine nonlinear systems, this technique generates linear control constraints which can be used to efficiently solve for point-wise optimal control signals for an arbitrary primary controller.

The second problem we address is that of model uncertainty, which has been studied extensively in the CBF literature. Robust methods [5]–[8] typically rely on accounting for worst-case disturbances through an upper disturbance bound, and these methods can be made less conservative via disturbance estimation [9]. The notion of input-to-state safety, defined first in [10] and extended for CBFs in [11], provides a technique for handling input disturbances and has been successfully applied in multiple scenarios [12], [13]. Adaptive CBF methods have been shown to assure safety in the presence of parametric dynamics uncertainty [14], [15] and a robust adaptive CBF extension can reduce conservatism and closed-loop chattering [16]. Learning [17], [18] and data-driven [19]–[21] approaches have also been developed to account for uncertainty in dynamics, state, or both. Lastly, for mixed-monotone systems their decomposable structure can be exploited to produce robustly forward invariant sets [22]. While these approaches present viable solutions to addressing model uncertainty, they assume that a controlled invariant safe set can be found explicitly—a strong assumption for many systems and safety constraints. Works [23] and [24] do not make this assumption, but the former is specific to mixed-monotone systems, and the latter assumes perfect dynamics knowledge and bounded measurement error.

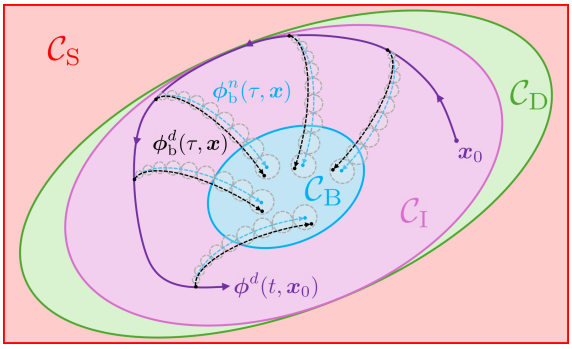

Fig. 1. Depiction of the proposed disturbance-robust safety-critical control framework. $\mathcal{C}_\mathrm{I}$ represents a forward invariant subset of an unknown controlled invariant set $\mathcal{C}_\mathrm{D}$ and guarantees safety of the disturbed system.

The main contribution of this work is a novel approach to address controlled invariance and dynamics disturbances simultaneously through the formulation of *disturbance-robust backup CBFs*. Unlike existing works, a controlled invariant set describing safety is not assumed to be known a priori, but is instead constructed online. We first derive forward invariance conditions for a subset inside a controlled invariant set of the disturbed system (displayed in Figure 1). Then we robustify these conditions and integrate them with existing controllers via a quadratic program. The proposed framework guarantees safety for a broad class of nonlinear systems with limited control authority even in the presence of unknown, bounded disturbances. We demonstrate the effectiveness of the approach using two numerical simulations: an illustrative double integrator system and a spacecraft rotation example.

Approved for public release. Distribution is unlimited. Case #AFRL-2024-4823. This work was sponsored by AFRL under the STARS Seedlings for Disruptive Capabilities Program including contracts with UDRI (#FA8650-22-C-1017). S. Coogan was supported in part by the NSF, award #2219755.

[1]Aerospace Engineering, Texas A&M University, College Station TX 77845, U.S.A, {davidvanwijk,mmajji}@tamu.edu.

[2]Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta GA 30332, U.S.A, sam.coogan@gatech.edu.

[3]Mechanical Engineering, Wichita State University, Wichita KS 67260, U.S.A, tamas.molnar@wichita.edu.

[4]Safe Autonomy Lead, Air Force Research Laboratory, Wright-Patterson Air Force Base OH 45433, U.S.A, kerianne.hobbs@afrl.af.mil.

II. Preliminaries

A. Control Barrier Functions

Consider a nonlinear control affine system of the form

$$\dot{\boldsymbol{x}} = f(\boldsymbol{x}) + g(\boldsymbol{x})\boldsymbol{u}, \;\; \boldsymbol{x} \in \mathcal{X} \subseteq \mathbb{R}^n, \;\; \boldsymbol{u} \in \mathcal{U} \subseteq \mathbb{R}^m, \quad (1)$$

where $f : \mathcal{X} \to \mathbb{R}^n$ and $g : \mathcal{X} \to \mathbb{R}^{n\times m}$ are Lipschitz continuous functions. It is assumed that $\mathcal{U}$ is an m-dimensional convex polytope. For an initial condition $\boldsymbol{x}(0) = \boldsymbol{x}_0 \in \mathcal{X}$ if $\boldsymbol{u}$ is given by a locally Lipschitz feedback controller $k : \mathcal{X} \to \mathcal{U}$, $\boldsymbol{u} = k(\boldsymbol{x})$, the closed-loop system (1) has a unique solution $\boldsymbol{\phi}^n(t, \boldsymbol{x}_0)$ over an interval of existence.

In the context of this work, safety is defined by membership to set $\mathcal{C}_\mathrm{S}$. Safe controllers are ones that render this safe set forward invariant. A set $\mathcal{C} \subset \mathbb{R}^n$ is *forward invariant* along (1) if $\boldsymbol{x}_0 \in \mathcal{C} \implies \boldsymbol{\phi}^n(t, \boldsymbol{x}_0) \in \mathcal{C}$, for all $t > 0$. Now, consider the safe set $\mathcal{C}_\mathrm{S}$ as the 0-superlevel set of a continuously differentiable function $h : \mathcal{X} \to \mathbb{R}$ with $\mathcal{C}_\mathrm{S} \triangleq \{\boldsymbol{x} \in \mathcal{X} : h(\boldsymbol{x}) \geq 0\}$, where the gradient of h along the boundary of $\mathcal{C}_\mathrm{S}$ remains nonzero. A function $h : \mathcal{X} \to \mathbb{R}$ is a CBF [1] for (1) on $\mathcal{C}_\mathrm{S}$ if there exists a class-$\mathcal{K}_\infty$ function[1] α such that for all $\boldsymbol{x} \in \mathcal{C}_\mathrm{S}$

$$\sup_{\boldsymbol{u}\in\mathcal{U}} \dot{h}(\boldsymbol{x}, \boldsymbol{u}) \triangleq \underbrace{\nabla h(\boldsymbol{x}) f(\boldsymbol{x})}_{L_f h(\boldsymbol{x})} + \underbrace{\nabla h(\boldsymbol{x}) g(\boldsymbol{x})}_{L_g h(\boldsymbol{x})} \boldsymbol{u} \geq -\alpha(h(\boldsymbol{x})),$$

where $L_{(\cdot)}h$ is the Lie derivative of h along function $(\cdot)$.

Theorem 1 ([1]). *If h is a CBF for (1) on $\mathcal{C}_\mathrm{S}$, then any locally Lipschitz controller $k : \mathcal{X} \to \mathcal{U}$, $\boldsymbol{u} = k(\boldsymbol{x})$ satisfying*

$$L_f h(\boldsymbol{x}) + L_g h(\boldsymbol{x})\boldsymbol{u} \geq -\alpha(h(\boldsymbol{x})) \quad (2)$$

for all $\boldsymbol{x} \in \mathcal{C}_\mathrm{S}$ renders the set $\mathcal{C}_\mathrm{S}$ forward invariant.

For an arbitrary primary controller, $\boldsymbol{u}_\mathrm{p} \in \mathcal{U}$, it is possible to ensure the safety of (1) by solving the following point-wise optimization problem for the safe control, $\boldsymbol{u}_\mathrm{safe}$:

$$\begin{aligned} \boldsymbol{u}_\mathrm{safe} = \underset{\boldsymbol{u}\in\mathcal{U}}{\operatorname{argmin}} \;\; & \frac{1}{2}\left\|\boldsymbol{u}_\mathrm{p} - \boldsymbol{u}\right\|^2 \qquad \text{(CBF-QP)} \\ \text{s.t.} \;\; & L_f h(\boldsymbol{x}) + L_g h(\boldsymbol{x})\boldsymbol{u} \geq -\alpha(h(\boldsymbol{x})). \end{aligned}$$

A key challenge is obtaining an explicit representation of such a function h where a safe control signal satisfying (2) can always be found. Depending on the safe set this may be difficult or impossible, especially for high dimensional systems. This therefore motivates the use of an extension of CBFs known as backup CBFs.

B. Implicitly Defined Controlled Invariant Sets

First introduced in [2] and expanded upon in [3], the backup CBF approach relies on obtaining an implicitly defined controlled invariant set. A set $\mathcal{C} \subset \mathbb{R}^n$ is *controlled invariant* if there exists a controller $k : \mathcal{X} \to \mathcal{U}$, $\boldsymbol{u} = k(\boldsymbol{x})$ which renders $\mathcal{C}$ forward invariant for (1).

[1] $\alpha : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is a class-$\mathcal{K}_\infty$ function if it is continuous, $\alpha(0) = 0$ and $\lim_{x\to\infty} \alpha(x) = \infty$.

To construct an implicit controlled invariant set, first assume that we have defined a set $\mathcal{C}_\mathrm{S}$ describing our state constraints, which is not necessarily controlled invariant. Now suppose that there exists a set within $\mathcal{C}_\mathrm{S}$ which we call a *backup set*, $\mathcal{C}_\mathrm{B}$, such that $\mathcal{C}_\mathrm{B} \subset \mathcal{C}_\mathrm{S}$. This set is defined similar to $\mathcal{C}_\mathrm{S}$ with a continuously differentiable function h_b, it is known to be controlled invariant, and it is made forward invariant by a *backup control law* defined by $\boldsymbol{u}_\mathrm{b} : \mathcal{X} \to \mathcal{U}$. The closed-loop system under $\boldsymbol{u}_\mathrm{b}$ is denoted as

$$f_\mathrm{cl}(\boldsymbol{x}) \triangleq f(\boldsymbol{x}) + g(\boldsymbol{x})\boldsymbol{u}_\mathrm{b}(\boldsymbol{x}). \quad (3)$$

It is assumed that for any $\boldsymbol{x} \in \mathcal{X}$ there exists a unique solution $\boldsymbol{\phi}^n_\mathrm{b} : [0, T] \times \mathcal{X} \to \mathcal{X}$ which satisfies:

$$\dot{\boldsymbol{\phi}}^n_\mathrm{b}(\tau, \boldsymbol{x}) = f_\mathrm{cl}(\boldsymbol{\phi}^n_\mathrm{b}(\tau, \boldsymbol{x})), \;\; \boldsymbol{\phi}^n_\mathrm{b}(0, \boldsymbol{x}) = \boldsymbol{x}. \quad (4)$$

The solution is the *flow* of the system over the interval $[0, T]$ for $T \in \mathbb{R}_{>0}$ starting at state $\boldsymbol{x}$ under the backup control law $\boldsymbol{u}_\mathrm{b}$. To obtain an implicitly defined controlled invariant set, $\mathcal{C}_\mathrm{BI}$, satisfying $\mathcal{C}_\mathrm{B} \subseteq \mathcal{C}_\mathrm{BI} \subseteq \mathcal{C}_\mathrm{S}$, one must ensure that the trajectory of the system under $\boldsymbol{u}_\mathrm{b}(\boldsymbol{x})$ remains in $\mathcal{C}_\mathrm{S}$ over a finite time horizon, and that the final point in the trajectory lies within the backup set $\mathcal{C}_\mathrm{B}$. Therefore $\mathcal{C}_\mathrm{BI}$ is defined as

$$\mathcal{C}_\mathrm{BI} \triangleq \left\{ \boldsymbol{x} \in \mathcal{X} \;\middle|\; \begin{array}{c} h(\boldsymbol{\phi}^n_\mathrm{b}(\tau, \boldsymbol{x})) \geq 0, \forall \tau \in [0, T], \\ h_\mathrm{b}(\boldsymbol{\phi}^n_\mathrm{b}(T, \boldsymbol{x})) \geq 0 \end{array} \right\}. \quad (5)$$

The sufficient condition for forward invariance of $\mathcal{C}_\mathrm{BI}$, and thus safety with respect to $\mathcal{C}_\mathrm{S}$, is then

$$\nabla h(\boldsymbol{\phi}^n_\mathrm{b}(\tau, \boldsymbol{x}))\boldsymbol{\Phi}^n_\mathrm{b}(\tau, \boldsymbol{x})\dot{\boldsymbol{x}} \geq -\alpha(h(\boldsymbol{\phi}^n_\mathrm{b}(\tau, \boldsymbol{x}))), \quad (6a)$$

$$\nabla h_\mathrm{b}(\boldsymbol{\phi}^n_\mathrm{b}(T, \boldsymbol{x}))\boldsymbol{\Phi}^n_\mathrm{b}(T, \boldsymbol{x})\dot{\boldsymbol{x}} \geq -\alpha_\mathrm{b}(h_\mathrm{b}(\boldsymbol{\phi}^n_\mathrm{b}(T, \boldsymbol{x}))), \quad (6b)$$

for all $\tau \in [0, T]$ and class-$\mathcal{K}_\infty$ functions α and α_b. Here, $\dot{\boldsymbol{x}} = f(\boldsymbol{x}) + g(\boldsymbol{x})\boldsymbol{u}$ and $\boldsymbol{\Phi}^n_\mathrm{b}(\tau, \boldsymbol{x}) \triangleq \partial\boldsymbol{\phi}^n_\mathrm{b}(\tau, \boldsymbol{x})/\partial\boldsymbol{x}$ is the sensitivity matrix, or state-transition matrix (STM), which captures the sensitivity of the flow to perturbations in the initial condition $\boldsymbol{x}$. The STM is the solution to

$$\dot{\boldsymbol{\Phi}}^n_\mathrm{b}(\tau, \boldsymbol{x}) = F_\mathrm{cl}(\boldsymbol{\phi}^n_\mathrm{b}(\tau, \boldsymbol{x}))\boldsymbol{\Phi}^n_\mathrm{b}(\tau, \boldsymbol{x}), \;\; \boldsymbol{\Phi}^n_\mathrm{b}(0, \boldsymbol{x}) = \boldsymbol{I}, \quad (7)$$

where F_cl is the Jacobian of the closed-loop backup dynamics (3) evaluated at $\boldsymbol{\phi}^n_\mathrm{b}(\tau, \boldsymbol{x})$ and $\boldsymbol{I}$ is the $n \times n$ identity matrix.

Because the inequality in (6a) represents an infinite number of constraints, in practice these are discretized and enforced at discrete times along the flow. To ensure safety between sample points, (6a) is tightened via a constant ε_Δ [4, Thm. 3]:

$$\varepsilon_\Delta \geq \frac{\Delta}{2}\mathcal{L}_h \sup_{\boldsymbol{x}\in\mathcal{C}_\mathrm{S}} \left\|f_\mathrm{cl}(\boldsymbol{x})\right\|, \quad (8)$$

where $\Delta \in \mathbb{R}_{>0}$ is a discretization time step satisfying $T/\Delta \in \mathbb{N}$, $\mathcal{L}_h \in \mathbb{R}_{>0}$ is the Lipschitz constant of h with respect to the Euclidean norm and $\sup_{\boldsymbol{x}\in\mathcal{C}_\mathrm{S}} \|f_\mathrm{cl}(\boldsymbol{x})\|$ is the maximal velocity of the backup vector field.

As in (CBF-QP), the safety of (1) can be enforced for a primary controller, $\boldsymbol{u}_\mathrm{p} \in \mathcal{U}$, by solving an optimization problem for the safe control with constraints (6), where the right-hand side of (6a) is replaced by $-\alpha(h(\boldsymbol{\phi}^n_\mathrm{b}(\tau, \boldsymbol{x})) - \varepsilon_\Delta)$.

III. Disturbance Robustness

While the standard backup set method reviewed in Section II-B can guarantee safety for a system in which the dynamics are perfectly known, in practice there are always unmodeled parameters or external disturbances which perturb the dynamics. Therefore, it is desirable to leverage the advantages offered by the backup CBF approach, for dynamics with process disturbances. As such, consider the system

$$\dot{\boldsymbol{x}} = f(\boldsymbol{x}) + g(\boldsymbol{x})\boldsymbol{u} + \boldsymbol{d}_x, \tag{9}$$

where $\boldsymbol{d}_x \in \mathcal{D}_x \subseteq \mathbb{R}^n$ is an unknown additive process disturbance and there exists a constant $\xi \in \mathbb{R}_{>0}$ such that $\|\boldsymbol{d}_x\| \leq \xi$. For an initial condition $\boldsymbol{x}(0) = \boldsymbol{x}_0 \in \mathcal{X}$ and a locally Lipschitz controller $\boldsymbol{u} = k(\boldsymbol{x})$, if $\boldsymbol{d}_x$ is piecewise continuous in time, the closed-loop system (9) has a unique solution $\boldsymbol{\phi}^d(t, \boldsymbol{x}_0)$ over an interval of existence.

We assume that a backup control law $\boldsymbol{u}_\mathrm{b}$ can be obtained which renders a backup set $\mathcal{C}_\mathrm{B}$ inside $\mathcal{C}_\mathrm{S}$ robustly forward invariant. This is made more precise below.

Assumption 1. *The backup controller $\boldsymbol{u}_\mathrm{b}$ renders the backup set $\mathcal{C}_\mathrm{B}$ forward invariant along (9) for any disturbance $\boldsymbol{d}_x$ which satisfies $\|\boldsymbol{d}_x\| \leq \xi$.*

Backup sets are often defined by a level set of a quadratic Lyapunov function based on the linearized dynamics about a stabilizable equilibrium point [3], [25], and a simple feedback controller such as a linear quadratic regulator can be used to render this set forward invariant. Techniques to robustify such quadratic Lyapunov functions have been studied in the literature [5], [26, Ch. 13.1], [27, Ch. 3]. While this robustification may result in a smaller backup set, this set is expanded to generate a larger controlled invariant set.

Next we define two separate flows: the nominal and the disturbed backup flow. The nominal backup flow $\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})$ satisfies (4) under the robust control law $\boldsymbol{u}_\mathrm{b}$, while the disturbed backup flow, denoted $\boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x})$, is the solution to

$$\dot{\boldsymbol{\phi}}_\mathrm{b}^d(\tau, \boldsymbol{x}) = f_\mathrm{cl}(\boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x})) + \boldsymbol{d}_x, \quad \boldsymbol{\phi}_\mathrm{b}^d(0, \boldsymbol{x}) = \boldsymbol{x}. \tag{10}$$

Again, it is assumed that for any $\boldsymbol{x} \in \mathcal{X}$ there exists a unique solution $\boldsymbol{\phi}_\mathrm{b}^d : [0, T] \times \mathcal{X} \to \mathcal{X}$ to (10). Consider $\mathcal{C}_\mathrm{D} \subseteq \mathcal{C}_\mathrm{S}$

$$\mathcal{C}_\mathrm{D} \triangleq \left\{ \boldsymbol{x} \in \mathcal{X} \;\middle|\; \begin{array}{c} h(\boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x})) \geq 0, \forall \tau \in [0, T], \\ h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^d(T, \boldsymbol{x})) \geq 0 \end{array} \right\}. \tag{11}$$

We are interested in forward invariance conditions for $\mathcal{C}_\mathrm{D}$, but since the disturbance is unknown, we will instead derive forward invariance conditions for a set which over-approximates the disturbed flow. Consider a new set, $\mathcal{C}_\mathrm{I}$, defined by

$$\mathcal{C}_\mathrm{I} \triangleq \left\{ \boldsymbol{x} \in \mathcal{X} \;\middle|\; \begin{array}{c} h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) \geq \epsilon_\tau, \forall \tau \in [0, T], \\ h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x})) \geq \epsilon_\mathrm{b} \end{array} \right\}. \tag{12}$$

The set is entirely governed by the nominal trajectory and additional tightening terms ϵ_τ and ϵ_b. For judiciously chosen values of ϵ_τ and ϵ_b, we show that $\mathcal{C}_\mathrm{I}$ is a subset of $\mathcal{C}_\mathrm{D}$.

Lemma 1. *Let $\mathcal{L}_h$ and $\mathcal{L}_{h_\mathrm{b}}$ be the Lipschitz constants of h and h_b, respectively, and let $\delta_\mathrm{max}(\tau)$ be a norm bound on the deviation between $\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})$ and $\boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x})$ at time $\tau \in [0, T]$:*

$$\left\| \boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x}) - \boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x}) \right\| \leq \delta_\mathrm{max}(\tau), \tag{13}$$

for all $\boldsymbol{x} \in \mathcal{C}_\mathrm{S}$. If $\epsilon_\tau \geq \mathcal{L}_h \delta_\mathrm{max}(\tau)$ holds for all $\tau \in [0, T]$ and $\epsilon_\mathrm{b} \geq \mathcal{L}_{h_\mathrm{b}} \delta_\mathrm{max}(T)$ also holds, then $\mathcal{C}_\mathrm{I} \subseteq \mathcal{C}_\mathrm{D}$.

Proof. Consider any state $\boldsymbol{x} \in \mathcal{C}_\mathrm{I}$. Membership to $\mathcal{C}_\mathrm{I}$ implies that $h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) \geq \epsilon_\tau \geq \mathcal{L}_h \delta_\mathrm{max}(\tau)$. Hence it follows that

$$\begin{aligned} h(\boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x})) &= h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) - \big(h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) - h(\boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x}))\big) \\ &\geq \mathcal{L}_h \delta_\mathrm{max}(\tau) - \big|h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) - h(\boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x}))\big|. \end{aligned}$$

By Lipschitz continuity of the constraint function h

$$\begin{aligned} &|h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) - h(\boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x}))| \\ &\quad \leq \mathcal{L}_h \left\| \boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x}) - \boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x}) \right\| \leq \mathcal{L}_h \delta_\mathrm{max}(\tau), \end{aligned}$$

we obtain $h(\boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x})) \geq 0$ for any $\boldsymbol{x} \in \mathcal{C}_\mathrm{I}$. Similar logic can be applied to the constraint on the reachability of the backup set. For any $\boldsymbol{x} \in \mathcal{C}_\mathrm{I}$, the nominal backup trajectory from $\boldsymbol{x}$ satisfies $h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x})) \geq \epsilon_\mathrm{b} \geq \mathcal{L}_{h_\mathrm{b}} \delta_\mathrm{max}(T)$, and we have

$$|h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x})) - h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^d(T, \boldsymbol{x}))| \leq \mathcal{L}_{h_\mathrm{b}} \delta_\mathrm{max}(T).$$

These guarantee that $h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^d(T, \boldsymbol{x})) \geq 0$. Thus, all the functions which define $\mathcal{C}_\mathrm{D}$ are nonnegative, meaning that $\boldsymbol{x} \in \mathcal{C}_\mathrm{D}$ for all $\boldsymbol{x} \in \mathcal{C}_\mathrm{I}$, and so $\mathcal{C}_\mathrm{I} \subseteq \mathcal{C}_\mathrm{D}$. ■

Lemma 1 assumes that a time-varying bound on the deviation between the nominal and disturbed backup flow, $\delta_\mathrm{max}(\tau)$, can be found. While problem-specific bounds can be obtained, we utilize a generalization of the Gronwall-Bellman inequality to obtain a bound for a wide class of nonlinear systems.

Lemma 2 (Theorem 2.5 in [26])**.** *For systems (4) and (10), let f_cl be locally Lipschitz on $\mathcal{X}$ with Lipschitz constant $\mathcal{L}_\mathrm{cl}$ and $\boldsymbol{d}_x$ be piecewise continuous in τ on $[0, T]$. If $\|\boldsymbol{d}_x\| \leq \xi$ for all $\boldsymbol{d}_x$ and some $\xi > 0$, then for all $\tau \in [0, T]$ one has*

$$\left\| \boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x}) - \boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x}) \right\| \leq \frac{\xi}{\mathcal{L}_\mathrm{cl}} (e^{\mathcal{L}_\mathrm{cl} \tau} - 1) \triangleq \delta_\mathrm{max}(\tau).$$

Remark 1. *Backup strategies often drive the system to an equilibrium and thus may be (at least weakly) contracting. When contraction bounds on the deviation between the disturbed and nominal backup flow can be obtained, $\delta_\mathrm{max}(\tau)$ can be made less conservative, and it will converge to a near-constant value as T increases. Details on such bounds can be found in [28, Corollary 3.17]. A contraction bound is used effectively in the spacecraft rotation example in Section IV-B. For linear systems, flow deviation bounds can be even tighter.*

Using the definition of $\mathcal{C}_\mathrm{D}$ and the corresponding robust backup controller $\boldsymbol{u}_\mathrm{b}$, we now examine the properties of $\mathcal{C}_\mathrm{D}$.

Lemma 3. *The set $\mathcal{C}_\mathrm{D}$ is controlled invariant, and the robust backup controller $\boldsymbol{u}_\mathrm{b}$ renders $\mathcal{C}_\mathrm{D}$ forward invariant along (9), such that*

$$\boldsymbol{x} \in \mathcal{C}_\mathrm{D} \implies \boldsymbol{\phi}_\mathrm{b}^d(\vartheta, \boldsymbol{x}) \in \mathcal{C}_\mathrm{D}, \forall \vartheta \geq 0. \tag{14}$$

Proof. From the definition of $\mathcal{C}_\mathrm{D}$ and with Assumption 1

$$\boldsymbol{x} \in \mathcal{C}_\mathrm{D} \implies \boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x}) \in \mathcal{C}_\mathrm{B} \subseteq \mathcal{C}_\mathrm{S}, \forall \tau \geq T. \tag{15}$$

By definition, the flow is recursive in nature and thus for any $\boldsymbol{x} \in \mathbb{R}^n$ and $\tau, \vartheta \geq 0$, $\boldsymbol{\phi}_\mathrm{b}^d(\tau + \vartheta, \boldsymbol{x}) = \boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{\phi}_\mathrm{b}^d(\vartheta, \boldsymbol{x}))$. Using (15) and the recursive property of the flow

$$\boldsymbol{x} \in \mathcal{C}_\mathrm{D} \implies \boldsymbol{\phi}_\mathrm{b}^d(T, \boldsymbol{\phi}_\mathrm{b}^d(\vartheta, \boldsymbol{x})) \in \mathcal{C}_\mathrm{B}, \forall \vartheta \geq 0. \tag{16}$$

From (15) and by definition (11) $\boldsymbol{x} \in \mathcal{C}_\mathrm{D} \implies \boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{x}) \in \mathcal{C}_\mathrm{S}, \forall \tau \geq 0$. Using the recursive property once more

$$\boldsymbol{x} \in \mathcal{C}_\mathrm{D} \implies \boldsymbol{\phi}_\mathrm{b}^d(\tau, \boldsymbol{\phi}_\mathrm{b}^d(\vartheta, \boldsymbol{x})) \in \mathcal{C}_\mathrm{S}, \forall \tau \in [0, T], \forall \vartheta \geq 0. \tag{17}$$

Definition (11) with (16) and (17) completes the proof. ∎

While the controlled invariance of $\mathcal{C}_\mathrm{D}$ has been established, the conditions on $\boldsymbol{u}$ for forward invariance cannot yet be obtained as $\mathcal{C}_\mathrm{D}$ itself is unknown. This motivates the following theorems.

Theorem 2. *For any $\boldsymbol{x} \in \mathcal{C}_\mathrm{I}$, there exists a controller $\boldsymbol{u}$ such that $\boldsymbol{\phi}^d(\vartheta, \boldsymbol{x}) \in \mathcal{C}_\mathrm{D} \subseteq \mathcal{C}_\mathrm{S}, \forall \vartheta \geq 0$.*

Proof. By Lemma 1, $\boldsymbol{x} \in \mathcal{C}_\mathrm{I} \implies \boldsymbol{x} \in \mathcal{C}_\mathrm{D}$, and by Lemma 3, $\boldsymbol{u}_\mathrm{b}$ ensures $\boldsymbol{\phi}^d(\vartheta, \boldsymbol{x}) \in \mathcal{C}_\mathrm{D} \subseteq \mathcal{C}_\mathrm{S}$, $\forall \vartheta \geq 0$. ∎

We are now ready to establish the conditions that enable a controller to ensure the robust safety of (9). From the definition of $\mathcal{C}_\mathrm{I}$ we have

$$\begin{aligned} \dot{h}(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x}), \boldsymbol{u}) &\geq -\alpha(h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) - \epsilon_\tau), \\ \dot{h}_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x}), \boldsymbol{u}) &\geq -\alpha_\mathrm{b}(h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x})) - \epsilon_\mathrm{b}), \end{aligned} \tag{18}$$

where by expanding the total derivatives for system (9) this becomes, $\forall \tau \in [0, T]$,

$$\begin{aligned} \nabla h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) \boldsymbol{\Phi}_\mathrm{b}^n(\tau, \boldsymbol{x}) \dot{\boldsymbol{x}}^d &\geq -\alpha(h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) - \epsilon_\tau), \\ \nabla h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x})) \boldsymbol{\Phi}_\mathrm{b}^n(T, \boldsymbol{x}) \dot{\boldsymbol{x}}^d &\geq -\alpha_\mathrm{b}(h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x})) - \epsilon_\mathrm{b}). \end{aligned} \tag{19}$$

Here, $\dot{\boldsymbol{x}}^d \triangleq f(\boldsymbol{x}) + g(\boldsymbol{x})\boldsymbol{u} + \boldsymbol{d}_x$. Using this expansion, we can show that a controller which realizes forward invariance of $\mathcal{C}_\mathrm{I}$ keeps the disturbed system safe, and that conditions for such a controller can be directly computed, despite the unknown disturbance.

Theorem 3. *If any controller $\boldsymbol{u}$ satisfies*

$$\begin{aligned} \nabla h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) \boldsymbol{\Phi}_\mathrm{b}^n(\tau, \boldsymbol{x}) \big(f(\boldsymbol{x}) + g(\boldsymbol{x})\boldsymbol{u}\big) - \eta \geq \\ -\alpha(h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) - \epsilon_\tau), \\ \nabla h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x})) \boldsymbol{\Phi}_\mathrm{b}^n(T, \boldsymbol{x}) \big(f(\boldsymbol{x}) + g(\boldsymbol{x})\boldsymbol{u}\big) - \eta_\mathrm{b} \geq \\ -\alpha_\mathrm{b}(h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x})) - \epsilon_\mathrm{b}), \end{aligned} \tag{20}$$

with robustness terms defined by

$$\begin{aligned} \eta &\triangleq \xi \left\| \nabla h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) \boldsymbol{\Phi}_\mathrm{b}^n(\tau, \boldsymbol{x}) \right\|, \\ \eta_\mathrm{b} &\triangleq \xi \left\| \nabla h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x})) \boldsymbol{\Phi}_\mathrm{b}^n(T, \boldsymbol{x}) \right\|, \end{aligned}$$

then $\boldsymbol{x}_0 \in \mathcal{C}_\mathrm{I} \implies \boldsymbol{\phi}^d(t, \boldsymbol{x}_0) \in \mathcal{C}_\mathrm{I} \subseteq \mathcal{C}_\mathrm{D} \subseteq \mathcal{C}_\mathrm{S}$, for all $t > 0$.

Proof. As done in [5], the robustness terms η and η_b upper-bound the unknown $\boldsymbol{d}_x$ term in (19). Thus the condition (20) implies (19). From a direct application of Theorem 1 to system (9), we obtain that (19) ensures $\boldsymbol{\phi}^d(t, \boldsymbol{x}_0) \in \mathcal{C}_\mathrm{I}$, $\forall t > 0$ for any $\boldsymbol{x}_0 \in \mathcal{C}_\mathrm{I}$. From Lemma 1, we have $\mathcal{C}_\mathrm{I} \subseteq \mathcal{C}_\mathrm{D}$. ∎

Naturally, the original backup CBF constraints (6) are recovered in the absence of disturbances (i.e., $\xi = 0$). As the constraints in (20) are continuous in τ, the trajectory is again discretized similar to [4, Thm. 3] and appropriately tightened via a constant term ε_Δ where

$$\varepsilon_\Delta \geq \frac{\Delta}{2} \mathcal{L}_h \big(\sup_{\boldsymbol{x} \in \mathcal{C}_\mathrm{S}} \|f_\mathrm{cl}(\boldsymbol{x})\| + \xi \big). \tag{21}$$

The result of Theorem 3 is now ready to be directly utilized in a new point-wise optimal controller accounting for disturbances. The *Disturbance-Robust Backup CBF (DR-bCBF)* optimization problem is written as:

$$\begin{aligned} \boldsymbol{u}_\mathrm{safe} = \underset{\boldsymbol{u} \in \mathcal{U}}{\operatorname{argmin}} \ & \frac{1}{2} \|\boldsymbol{u}_\mathrm{p} - \boldsymbol{u}\|^2 \qquad \text{(DR-bCBF-QP)} \\ \text{s.t. } & \nabla h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) \boldsymbol{\Phi}_\mathrm{b}^n(\tau, \boldsymbol{x}) \big(f(\boldsymbol{x}) + g(\boldsymbol{x})\boldsymbol{u}\big) - \eta \geq \\ & \qquad -\alpha(h(\boldsymbol{\phi}_\mathrm{b}^n(\tau, \boldsymbol{x})) - \epsilon_\tau - \varepsilon_\Delta), \\ & \nabla h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x})) \boldsymbol{\Phi}_\mathrm{b}^n(T, \boldsymbol{x}) \big(f(\boldsymbol{x}) + g(\boldsymbol{x})\boldsymbol{u}\big) - \eta_\mathrm{b} \geq \\ & \qquad -\alpha_\mathrm{b}(h_\mathrm{b}(\boldsymbol{\phi}_\mathrm{b}^n(T, \boldsymbol{x})) - \epsilon_\mathrm{b}), \end{aligned}$$

for all $\tau \in \{0, \Delta, \ldots, T\}$. As before, $\Delta \in \mathbb{R}_{>0}$ is a discretization time step satisfying $T/\Delta \in \mathbb{N}$. Because ϵ_τ and ϵ_b only depend on a priori known values and τ, they can be pre-computed and reused each time (DR-bCBF-QP) is solved. Furthermore, the robustness terms η and η_b depend on values that must be computed for the standard backup set method already, hence disturbance robustness adds negligible computational cost.

Remark 2. *From Theorem 2, $\mathcal{C}_\mathrm{D}$ is controlled invariant, however the controlled invariance of $\mathcal{C}_\mathrm{I}$ itself cannot be proven without additional assumptions on $\boldsymbol{u}_\mathrm{b}$ and $\mathcal{C}_\mathrm{B}$. Therefore, the feasibility of the optimization problem (DR-bCBF-QP) is not guaranteed. However, in the case that the optimization problem becomes infeasible, the robust backup control law $\boldsymbol{u}_\mathrm{b}$ can be used to stay in $\mathcal{C}_\mathrm{D}$ until the optimization problem becomes feasible again.*

IV. Numerical Examples

In this section we demonstrate the effectiveness of the proposed method in assuring safety under bounded disturbances using two simulation examples. Code and videos are available at: https://github.com/davidvwijk/DR-bCBF.

A. Double Integrator

Consider a simple example of a double integrator given by

$$\dot{\boldsymbol{x}} = \begin{bmatrix} x_2, u \end{bmatrix}^T + \boldsymbol{d}_x, \tag{22}$$

with a state vector $\boldsymbol{x} = [x_1, x_2]^T \in \mathbb{R}^2$ where x_1 is the position and x_2 is the velocity, and an acceleration control variable $u \in \mathcal{U} = [-1, 1]$. The safe set is defined as $\mathcal{C}_\mathrm{S} \triangleq \{\boldsymbol{x} \in \mathbb{R}^2 : -x_1 \geq 0\}$. The unknown additive process disturbance is bounded with $\|\boldsymbol{d}_x\| \leq \xi \in \mathbb{R}_{>0}$. In this

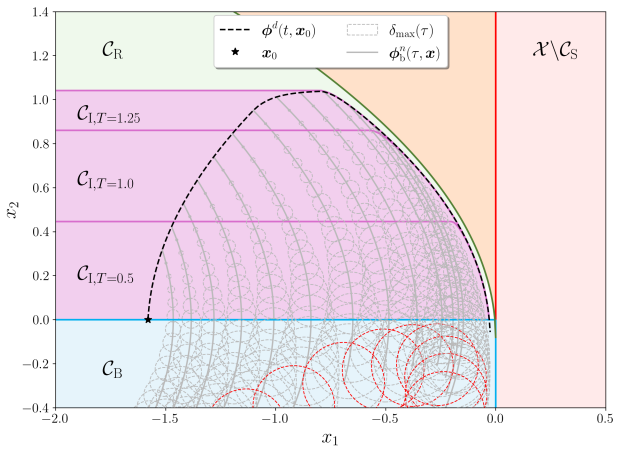

Fig. 2. Phase space visualization of safety-critical control for a double integrator system under bounded disturbances, using the proposed disturbance-robust backup control barrier function approach. Nominal backup trajectories in gray emanate from the disturbed trajectory (dotted black line) and the gray circles centered on the nominal trajectories are Gronwall norm balls from Lemma 2. The Gronwall norm ball at $\tau = T$, colored in red, is always contained in $\mathcal{C}_\mathrm{B}$, as required by (12).

particular example, the unknown disturbance is constant, with $\boldsymbol{d}_x = \xi\frac{\boldsymbol{v}}{\|\boldsymbol{v}\|}$ where $\boldsymbol{v} = [1,1]^T$, and $\xi = 0.08$. The backup control law $\boldsymbol{u}_\mathrm{b}(\boldsymbol{x}) = -1$ brings the system to the backup set $\mathcal{C}_\mathrm{B} \triangleq \{\boldsymbol{x} \in \mathbb{R}^2 : -x_1 \geq 0, -x_2 \geq 0\}$ as long as $\xi < 1$. The discretization time step for computing the nominal backup flow is $\Delta = 0.02\,\mathrm{s}$. The primary control law is $\boldsymbol{u}_\mathrm{p} = 1$ which drives the system to the right half-plane (unsafe region).

Using the proposed disturbance-robust backup CBF approach, the forward invariant set $\mathcal{C}_\mathrm{I}$ is computed for various values of T between $0.5\,\mathrm{s}$ and $1.25\,\mathrm{s}$, plotted on Figure 2 in pink. The backup set, $\mathcal{C}_\mathrm{B}$, is plotted in blue and a robust controlled invariant set $\mathcal{C}_\mathrm{R}$ is plotted in green. For this simple linear system, such a set can be computed by analytically solving for the flow and accounting for worst-case disturbances. The black dotted line represents the trajectory of the disturbed system using the proposed controller, with an integration horizon $T = 1.25\,\mathrm{s}$. Notably, safety is maintained along this trajectory, as stated by Theorem 3.

The plots show that as the backup horizon T is increased, the forward invariant set $\mathcal{C}_\mathrm{I}$ increases in size, up to a certain point. Since the Gronwall bound grows exponentially with time, the longer the backup horizon is, the larger the final bound, $\delta_{\max}(T)$, will be. If T is too large, the constraint on the terminal point of the nominal backup trajectory will dominate, and the set $\mathcal{C}_\mathrm{I}$ will begin to shrink. This therefore introduces a trade-off as T cannot be made arbitrarily large when using Lemma 2. Naturally, as the disturbance bound ξ increases, the size of $\mathcal{C}_\mathrm{I}$ will shrink since the bound on the backup flows is proportional to ξ.

B. Rigid Body Spacecraft Rotation

Consider next an example of a rigid body spacecraft with a known inertia tensor in the body frame given by $\boldsymbol{J}$, where the dynamics of the angular velocities can be described by Euler's rotational equations of motion

$$\dot{\boldsymbol{\omega}} = \boldsymbol{J}^{-1}(-\boldsymbol{\omega} \times \boldsymbol{J}\boldsymbol{\omega} + \boldsymbol{u}) + \boldsymbol{d}_x. \tag{23}$$

Here, $\boldsymbol{u} \in \mathcal{U} = [-1,1]^3\,\mathrm{Nm}$ is the control torque vector that can be applied by the spacecraft to control the angular velocity and $\boldsymbol{d}_x$ is an unknown but bounded additive disturbance vector, such that $\|\boldsymbol{d}_x\| \leq \xi \in \mathbb{R}_{>0}$. The states of interest are the angular velocity vector elements in the body frame.

The safety objective is to ensure that the norm of the angular velocity vector of the spacecraft does not exceed a maximum value, to prevent damage to onboard sensors. The safe set is therefore $\mathcal{C}_\mathrm{S} = \{\boldsymbol{\omega} \in \mathbb{R}^3 : h(\boldsymbol{\omega}) \geq 0\}$ where $h(\boldsymbol{\omega}) = \omega_{\max}^2 - \|\boldsymbol{\omega}\|^2 \geq 0$ and $\omega_{\max} \in \mathbb{R}_{>0}$ represents the maximum allowable angular velocity. The primary controller is given by $\boldsymbol{u}_\mathrm{p}(t) = \sin([\frac{t}{2}, \frac{t}{2} - \frac{\pi}{4}, \frac{t}{4} + \frac{\pi}{4}]^T)$. The robust backup control law $\boldsymbol{u}_\mathrm{b}(\boldsymbol{\omega}) = -k_b\boldsymbol{J}\boldsymbol{\omega} + \boldsymbol{\omega} \times \boldsymbol{J}\boldsymbol{\omega}$ renders the backup set $\mathcal{C}_\mathrm{B} \triangleq \{\boldsymbol{\omega} \in \mathbb{R}^3 : h_\mathrm{b}(\boldsymbol{\omega}) = \gamma - \frac{1}{2}\boldsymbol{\omega}^T\boldsymbol{J}\boldsymbol{\omega} \geq 0\}$ robustly forward invariant for sufficiently large gain k_b. $\mathcal{C}_\mathrm{B}$ is a level set of the spacecraft's rotational energy, defined by the scalar γ. Any $k_b > (\lambda_{\max}\xi)/(\sqrt{2\gamma\lambda_{\min}})$ ensures $\dot{h}_\mathrm{b}(\boldsymbol{\omega}, \boldsymbol{u}) \geq 0$ at the boundary of the level set for (23), where $\lambda_{\max}$ and $\lambda_{\min}$ are the maximum and minimum eigenvalues of $\boldsymbol{J}$, respectively. The proof is omitted for brevity.

It is straightforward to verify that the closed-loop nominal backup dynamics are strongly contracting with a rate of k_b since $f_\mathrm{cl}(\boldsymbol{\omega}) = -k_b\boldsymbol{\omega}$. Because the log norm of the closed-loop Jacobian $(\partial f_\mathrm{cl}/\partial\boldsymbol{\omega})$ is upper-bounded by $-k_b$, the disturbed and nominal backup flows can be bounded as

$$\left\|\phi_\mathrm{b}^n(\tau,\boldsymbol{\omega}) - \phi_\mathrm{b}^d(\tau,\boldsymbol{\omega})\right\| \leq \frac{\xi}{k_b}(1 - e^{-k_b\tau}), \tag{24}$$

by [28, Corollary 3.17]. This yields tighter ϵ_τ and ϵ_b terms than the general Gronwall bound.

For the simulations, $\omega_{\max} = 1\,\mathrm{rad/s}$, $\gamma = 2\,\mathrm{J}$, $\xi = 0.1\,\mathrm{rad/s^2}$ and $\boldsymbol{J}$ is diagonal with elements $[12, 12, 5]\,\mathrm{kgm^2}$. The discretization time step used for computing the nominal backup flow is $\Delta = 0.05\,\mathrm{s}$ and the integration horizon is $T = 1.75\,\mathrm{s}$. The disturbance vector is time-varying, given by $\boldsymbol{d}_x(t) = \xi\frac{\boldsymbol{v}(t)}{\|\boldsymbol{v}(t)\|}$ where $\boldsymbol{v}(t) = \sin([\frac{t}{2} + \frac{\pi}{2}, \frac{t}{2}, \frac{t}{2} - \frac{\pi}{2}]^T)$.

Figure 3 compares our disturbance-robust backup CBF method using the contraction bounds in (24) with the standard backup CBF approach. Our approach obeys the norm constraint on the angular velocity in the presence of unknown time-varying disturbances, while the standard backup CBF approach does not, violating safety multiple times.

V. Conclusions

In this article we presented a novel safety-critical control framework to handle unknown bounded disturbances for a broad class of nonlinear systems. We extended the method of backup CBFs to handle such disturbances by providing forward invariance conditions for a subset of a controlled invariant set governed by the disturbed system. We proved that enforcing these conditions guarantees safety for the disturbed system, and we demonstrated the effectiveness of the approach with two numerical simulation examples.

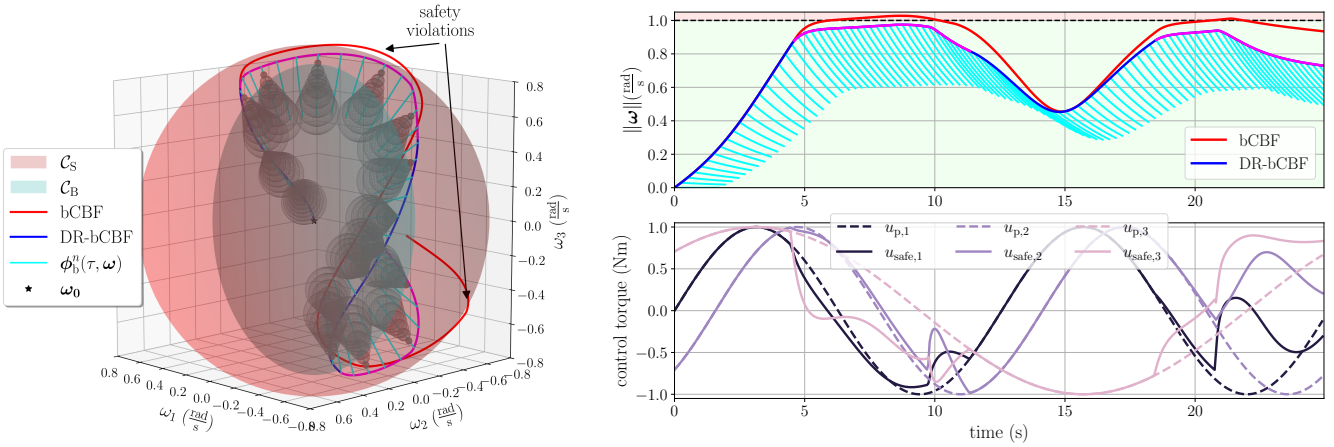

Fig. 3. Simulation results for a rigid body spacecraft, comparing the proposed disturbance-robust backup CBF approach and the standard backup CBF formulation. (**Left**) State-space visualization of angular velocity components showing the trajectory of the angular velocity vector over time. The objective is to keep the trajectory within the red sphere (safe region). The standard approach violates safety due to the disturbance, while the proposed disturbance-robust method does not. Magenta sections of the blue trajectory indicate that the primary control signal, $\boldsymbol{u}_\mathrm{p}$, has been modified to assure safety. Wire-frame spheres represent the contraction norm balls along the nominal backup flow in cyan. (**Right**) Angular velocity norm over time for both approaches (**top**), and commanded primary control and actual (safe) control signal over time for the robust approach (**bottom**).

References

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

[2] T. Gurriet, M. Mote, A. D. Ames, and E. Feron, "An Online Approach to Active Set Invariance," in *2018 IEEE Conference on Decision and Control (CDC)*, pp. 3592–3599, IEEE, Dec. 2018.

[3] 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. 187249–187275, 2020.

[4] T. Gurriet, *Applied Safety Critical Control*. PhD thesis, California Institute of Technology, 2020.

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

[6] K. Garg and D. Panagou, "Robust Control Barrier and Control Lyapunov Functions with Fixed-Time Convergence Guarantees," in *2021 American Control Conference (ACC)*, pp. 2292–2297, IEEE, May 2021.

[7] J. Breeden and D. Panagou, "Robust Control Barrier Functions under high relative degree and input constraints for satellite trajectories," *Automatica*, vol. 155, p. 111109, Sept. 2023.

[8] W. Shaw Cortez, D. Oetomo, C. Manzie, and P. Choong, "Control Barrier Functions for Mechanical Systems: Theory and Application to Robotic Grasping," *IEEE Transactions on Control Systems Technology*, vol. 29, pp. 530–545, Mar. 2021.

[9] E. Daş, S. X. Wei, and J. W. Burdick, "Robust control barrier functions with uncertainty estimation," *arXiv*, 2023.

[10] M. Z. Romdlony and B. Jayawardhana, "On the new notion of input-to-state safety," in *2016 IEEE 55th Conference on Decision and Control (CDC)*, pp. 6403–6409, 2016.

[11] S. Kolathaya and A. D. Ames, "Input-to-state safety with control barrier functions," *IEEE Control Systems Letters*, vol. 3, no. 1, pp. 108–113, 2019.

[12] A. Alan, A. J. Taylor, C. R. He, A. D. Ames, and G. Orosz, "Control barrier functions and input-to-state safety with application to automated vehicles," *IEEE Transactions on Control Systems Technology*, vol. 31, no. 6, pp. 2744–2759, 2023.

[13] I. Tezuka, T. Kuramoto, and H. Nakamura, "Input-to-state constrained safety zeroing control barrier function and its application to time-varying obstacle avoidance for electric wheelchair," *IFAC-PapersOnLine*, vol. 55, no. 41, pp. 44–51, 2022. 4th IFAC Workshop on Cyber-Physical and Human Systems CPHS 2022.

[14] A. J. Taylor and A. D. Ames, "Adaptive safety with control barrier functions," in *2020 American Control Conference (ACC)*, pp. 1399–1405, 2020.

[15] W. Xiao, C. Belta, and C. G. Cassandras, "Adaptive control barrier functions," *IEEE Transactions on Automatic Control*, vol. 67, no. 5, pp. 2267–2281, 2022.

[16] B. T. Lopez, J.-J. E. Slotine, and J. P. How, "Robust adaptive control barrier functions: An adaptive and data-driven approach to safety," *IEEE Control Systems Letters*, vol. 5, no. 3, pp. 1031–1036, 2021.

[17] A. J. Taylor, A. W. Singletary, Y. Yue, and A. D. Ames, "Learning for safety-critical control with control barrier functions," in *Conference on Learning for Dynamics & Control*, 2019.

[18] L. Lindemann, A. Robey, L. Jiang, S. Das, S. Tu, and N. Matni, "Learning robust output control barrier functions from safe expert demonstrations," *IEEE Open Journal of Control Systems*, vol. 3, pp. 158–172, 2024.

[19] A. J. Taylor, V. D. Dorobantu, S. Dean, B. Recht, Y. Yue, and A. D. Ames, "Towards robust data-driven control synthesis for nonlinear systems with actuation uncertainty," in *2021 60th IEEE Conference on Decision and Control (CDC)*, pp. 6469–6476, 2021.

[20] F. Castañeda, J. J. Choi, B. Zhang, C. J. Tomlin, and K. Sreenath, "Pointwise feasibility of Gaussian process-based safety-critical control under model uncertainty," in *2021 60th IEEE Conference on Decision and Control (CDC)*, pp. 6762–6769, 2021.

[21] Y. Emam, P. Glotfelter, S. Wilson, G. Notomista, and M. Egerstedt, "Data-driven robust barrier functions for safe, long-term operation," *IEEE Transactions on Robotics*, vol. 38, no. 3, pp. 1671–1685, 2022.

[22] M. Abate and S. Coogan, "Computing robustly forward invariant sets for mixed-monotone systems," in *2020 59th IEEE Conference on Decision and Control (CDC)*, pp. 4553–4559, 2020.

[23] M. Abate and S. Coogan, "Enforcing Safety at Runtime for Systems with Disturbances," in *2020 59th IEEE Conference on Decision and Control (CDC)*, pp. 2038–2043, IEEE, Dec. 2020.

[24] R. K. Cosner, A. W. Singletary, A. J. Taylor, T. G. Molnar, K. L. Bouman, and A. D. Ames, "Measurement-robust control barrier functions: Certainty in safety with uncertainty in state," in *2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 6286–6291, IEEE, 2021.

[25] Y. Chen, M. Jankovic, M. Santillo, and A. D. Ames, "Backup control barrier functions: Formulation and comparative study," 2021.

[26] H. Khalil, *Nonlinear Systems*. Pearson Education, Prentice Hall, 2 ed., 2002.

[27] R. A. Freeman and P. Kokotović, *Robust Nonlinear Control Design*. Birkhäuser Boston, 1996.

[28] F. Bullo, *Contraction Theory for Dynamical Systems*. Kindle Direct Publishing, 1.1 ed., 2023.