2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Safe Control Design through Risk-Tunable Control Barrier Functions

Vipul K. Sharma and S. Sivaranjani

Abstract— **We consider the problem of designing controllers to guarantee safety for a class of nonlinear systems under uncertainties in the system dynamics and/or the environment. We define a class of uncertain control barrier functions (CBFs), and formulate the safe control design problem as a chance-constrained optimization problem with uncertain CBF constraints. We leverage the scenario approach for chance-constrained optimization to develop a risk-tunable control design that provably guarantees the satisfaction of uncertain CBF safety constraints up to a user-defined probabilistic risk bound, and provides a trade-off between the sample complexity and risk tolerance. We demonstrate the performance of this approach through simulations on a quadcopter navigation problem with obstacle avoidance constraints.**

I. INTRODUCTION

Safety is a central consideration in the design of autonomous systems that operate in uncertain and unknown environments, spanning numerous applications such as automated driving, robotics, and unmanned aerial vehicles. The problem of designing controllers that provably guarantee hard constraints on the safety of autonomous systems is a long-studied topic, and has seen a recent resurgence in interest due to advances in learning-based approaches as well as emerging applications such as self-driving cars, where autonomous systems are expected to closely interact with humans in safety-critical settings.

Model-based design approaches to guarantee safety often involve imposing Control Barrier Functions (CBF) constraints [1] on the control design problem. CBF constraints employ a Lyapunov-like argument to guarantee the invariance of a desired 'safe set' under the designed control law, essentially guaranteeing that a system that starts in a safe set always remains in the safe set. We refer the reader to [2] for a comprehensive survey on the various classes of CBF conditions commonly employed in control design. In situations where the control design problem involves uncertainty in the system dynamics or environment, robust control invariance conditions of a similar nature may be enforced to guarantee safety of the control design [3]–[9].

While CBF-based designs, including their robust versions, are effective in guaranteeing safety, a key challenge is that they are often conservative, imposing robustness to worst-case uncertainties, which may themselves be difficult to characterize in dynamic environments. Further, they may come at a great efficiency cost (both in terms of time-efficiency and control cost) that can make autonomous task execution practically unviable in several applications. Finally, notions of safety and risk can vary widely by domain. For example, in some applications, small safety constraint violations may be tolerable in order to increase task efficiency. Therefore, it is desirable to introduce probabilistic notions of safety with risk-efficiency tradeoffs that can be selected by designers based on application-specific considerations. In this context, this paper addresses the problem of introducing the notion of tunable risk into the safe control design problem.

Specifically, we consider a class of nonlinear control-affine systems with an additive uncertainty that may arise due to unknown dynamics and/or environmental variables (including obstacles). For this class of systems, we formulate a safe control design problem with uncertain CBF constraints that must be satisfied with a user-defined probabilistic risk bound. We pose this problem in a chance-constrained optimization setting, and propose a sampling-based control design based on the scenario approach [10]–[12] that allows the designer to tune the risk bound for safety constraint satisfaction, and provides a trade-off between the risk bound and the sample complexity of the problem. We demonstrate the performance of this design by simulation on a quadcopter navigation problem with obstacle avoidance constraints.

A. Related Work and Contributions

A common approach to safe control design for systems with uncertainties involves modeling the uncertainty by a known process, with Gaussian Process (GP) models receiving significant attention in typical MPC based control designs [13], [14], as well as CBF-based designs for safety-critical systems [7], [15]–[17]. However, these works do not typically consider the probabilistic notions of safety required to incorporate risk tunability that is the subject of this work. Control designs incorporating probabilistic notions of safety through chance-constrained CBFs have recently been proposed [17]–[22]. In general, such chance-constrained optimization problems are non-convex, even when the original CBF constraints are convex, and are often NP-hard [23], [24]. Solutions to such probabalistic safe control design problems typically involve either approximating the uncertainty by GP (or similar) models [20]–[22], or deriving convex relaxations or over-approximations that make the problem tractable [18], [19]. However, GP models may not hold in several safety-critical applications, and convex over-approximations may lead to conservative designs. In this paper, we introduce a sampling-based safe control design framework based on the scenario-approach for chance-constrained optimization [11] that does not make any assumptions regarding the underlying distribution of the uncertainty. The scenario approach has recently been utilized for safety verification with CBFs [25];

The authors are with the School of Industrial Engineering at Purdue University, West Lafayette, IN 47907, USA. {sharm697,sseetha}@purdue.edu

however, this work does not address control design, which is the central problem considered in this paper.

In this landscape, the key contribution of this paper is to introduce a framework to design controllers that can guarantee probabilistic notions of safety with user-defined risk bounds, with the advantage that the risk-efficiency and sample complexity trade-offs can be tuned by designers based on domain-specific requirements. We also note that most of the above safe control designs employ projection-based approaches, where a baseline controller (that is designed based on a separate optimization problem or is assumed to be given) is minimally modified through CBF constraints to enforce safety. Such projection-based approaches may result in sub-optimal controllers. In contrast, our approach directly solves a chance-constrained problem to optimize performance metrics while simultaneously guaranteeing safety, without the need for a two-stage solution.

B. Organization

This paper is organized as follows. Section II formulates the safe control design problem under uncertainties as a chance-constrained optimization problem with control barrier function constraints. Section III provides a risk-tunable design based on the scenario approach to solve the safe control design problem. Section IV demonstrates the design through simulation on a quadcopter navigation problem with uncertain obstacles. The proofs of all the results in this paper are presented in the Appendix.

C. Notation

We denote the sets of real numbers, positive real numbers including zero, and n-dimensional real vectors by $\mathbb{R}$, $\mathbb{R}_+$ and $\mathbb{R}^n$ respectively. For a matrix $A \in \mathbb{R}^{m\times n}$, $A^T \in \mathbb{R}^{n\times m}$ represents its transpose. A symmetric positive definite matrix $P \in \mathbb{R}^{n\times n}$ is represented as $P > 0$ (and as $P \geq 0$, if it is positive semi-definite). The standard identity matrix is denoted by I, with dimensions clear from the context. An $(n \times m)$ matrix with all elements equal to 1 is denoted by $\mathbf{1}_{n\times m}$. Similarly, an $(n \times m)$ matrix with all elements equal to zero is denoted by $\mathbf{0}_{n\times m}$. For any $N_1, N_2 \in \mathbb{R}_+$, $\begin{pmatrix} N_1 \\ N_2 \end{pmatrix}$ represents the number of ways to choose N_2 items from a set of N_1 items.

II. PROBLEM FORMULATION

We begin by formulating the safe control design problem addressed in this paper. We consider a nonlinear dynamical system with control-affine dynamics given by,

$$x_{t+1} = f(x_t) + g(x_t)u_t + d_t, \tag{1}$$

where $x_t \in X \subset \mathbb{R}^n$ is the state, $u_t \in U \subset \mathbb{R}^m$ is the control input, and $d_t \in U \subset \mathbb{R}^n$ is an additive disturbance at time $t \in \mathbb{R}_+$, and $f : \mathbb{R}^n \to \mathbb{R}^n$ and $g : \mathbb{R}^n \to \mathbb{R}^n \times \mathbb{R}^m$ are locally Lipschitz continuous. Moreover, we suppose that $U = [u^l, u^h]$, where u^l and u^h are actuator constraint lower and upper bounds respectively.

***Assumption** 2.1:* The dynamical system is assumed to be forward complete, that is, the solution to (1) is defined for all initial conditions $x_0 \in X$ and all admissible control inputs $u_t \in U$ for all time $t \in \mathbb{R}_+$.

We begin by defining control barrier functions (CBFs) and associated conditions that we will utilize in formulating the safe control design problem that is the subject of this work.

A. Control Barrier Functions (CBF)

Let $\mathcal{S}$ be a safe set, defined by the super-level set of a continuously differentiable function $\bar{h}\colon X \to \mathbb{R}$ as,

$$\mathcal{S} = \{x \in X \colon \bar{h}(x) \geq 0\}. \tag{2}$$

If the states always remain within this set, then we can guarantee the safety of the system as follows.

***Definition** 2.2:* The dynamical system (1) is said to be safe with respect to set $\mathcal{S}$ if $\mathcal{S}$ is *forward-invariant*, that is, $\forall x_0 \in \mathcal{S}$, $x_t \in \mathcal{S}, \forall t \in \mathbb{R}_+$.

A standard approach to establish forward invariance of the safe set $\mathcal{S}$ is to derive sufficient conditions using a Lyapunov-like argument as follows.

***Theorem** 2.3 (Adapted from [26]):* A continuously differentiable function $\bar{h}\colon X \to \mathbb{R}$ is a control barrier function for dynamical system (1) and renders the set $\mathcal{S}$ safe if there exists a control input u_t and a constant $\eta \in [0, 1]$ such that for all $x_t \in \mathcal{S}$, we have

$$\bar{h}(x_{t+1}) - (1 - \eta)\bar{h}(x_t) \geq 0. \tag{3}$$

In Theorem 2.3, the constant η determines how strongly the CBF pushes the states into the safe set [15].

B. Uncertain Control Barrier Functions

With the safe set defined in (2) and the CBF condition defined in Theorem 2.3, we now focus on the scenario where there is uncertainty in the CBF condition (3), either due to partially known/uncertain dynamics or due to the operating environment. We define a robust CBF condition as follows.

***Theorem** 2.4:* The dynamical system (1) can be rendered safe with safe set $\mathcal{S}$ if, for all $d_t \in D$, there exists control input $u_t \in U$ and a constant $\eta \in (0, 1]$ such that

$$L(x_t, u_t, d_t) := -h(x_t, u_t, d_t) - \eta\bar{h}(x_t) \leq 0, \tag{4}$$

where $h(x_t, u_t, d_t) := \bar{h}(x_{t+1})) - \bar{h}(x_t)$.

***Remark** 2.5:* The CBF condition in Theorem 2.3 can be appropriately defined to capture commonly encountered uncertainties in system dynamics and operation as follows:

- *Example E1 - Uncertainty in System Dynamics or Environment:* Consider the case where part of the system dynamics is unknown, that is, $d_t \in D$ is the unknown part of the dynamics in (1). A candidate CBF for such a case is an affine CBF $\bar{h}(x) := p^T x + q$, where $p \in \mathbb{R}^n$ and $q \in \mathbb{R}$. Then, the CBF condition in (4) for this case can be written as $L(x_t, u_t, d_t) = -[p^T(f(x_t) + g(x_t)u_t + d_t) + q] + (1 - \eta)(p^T x_t + q) \leq 0$. An identical CBF condition holds when d_t represents an additive exogenous disturbance arising from the interaction of the system with the environment.
- *Example E2 - Obstacle Avoidance:* Consider a navigation problem with obstacle avoidance constraints, where the objective is to maintain a safe distance between an agent (such as a mobile robot or aerial vehicle) and an obstacle

with position $x_t^{obs} \in \mathbb{R}^n$ at time t. Let the obstacle position be stationary and uncertain, i.e. $x_t^{obs} = x_t^o + d_t$ and $x_{t+1}^{obs} = x_t^{obs}$, where x_t^o is known and d_t is unknown. For this case, we may define $\bar{h}(x_t) := \|x_t - x_t^{obs}\|_2^2 - r_s$, where r_s is a user-defined safety margin. Then, the CBF condition in (4) can be written as $L(x_t, u_t, d_t) = -[\|f(x_t)+g(x_t)u_t - x_t^o - d_t\|_2^2 - r_s] + (1-\eta)\|x_t - x_t^o - d_t\|_2^2 - r_s \leq 0$.

C. Control Design Problem

With this uncertain CBF formulation, the goal is to design control inputs u_t that render the system (1) safe $\forall d \in D$. To obtain such control inputs at each time step t, we formulate a robust control design problem with constraints given by condition (4) in Theorem 2.4. Consider the robust control design problem (RCP^t) at time step t expressed as

$$RCP^t : \begin{array}{l} \min\limits_{u_t} C(u_t) \\ \text{s.t. } \; L(x_t, u_t, d_t) \leq 0, \; \forall d_t \in D, u^l \leq u_t \leq u^h, \end{array} \tag{5}$$

where $C(u_t)$ is the cost function.

There are several difficulties involved in solving the problem RCP^t. First, RCP^t involves a possibly infinite number of constraints. Even if the problem is assumed to be convex, this class of problems is, in general, NP-hard [23], [24], [27]. One common approach is to consider the a 'worst-case' solution to the RCP, where the CBF constraint in (5) is replaced by $L(x_t, u_t, d_t^*) \leq 0$, where $d_t^* = \max\{d : d \in D\}$. However, such a design would be overly conservative in many applications, and result in decreased performance metrics such as time-efficiency or control effort. Further, in many applications, a small tolerance towards risk is generally acceptable during operation under uncertainty.

We quantify the risk-tolerance in the safe control design problem in terms of violation probability of the CBF condition as follows.

***Definition** 2.6:* (Violation Probability) The probability of violation under control input u_t is defined as

$$V(u_t) := Prob\{d_t \in D : L(x_t, u_t, d_t) > 0\}. \tag{6}$$

For a given control input u_t, the probability that this input violates the CBF constraint $L(x_t, u_t, d_t) \leq 0$ is given by $V(u_t)$. Assuming a uniform probability density, the violation probability can be interpreted as a measure of the volume of 'unsafe' uncertainty parameters d_t such that the CBF constraint is violated.

Now, select a tunable user-defined risk bound $\epsilon \in (0, 1)$ that quantifies the acceptable violation probability. Note that ϵ can be selected by the designer based on the application. Then, we define an ϵ-level solution as follows:

***Definition** 2.7:* (ϵ-level solution) We say that $u_t \in U$ is an ϵ-level solution, if $V(u_t) \leq \epsilon$, $\epsilon \in (0, 1)$.

With these definitions, we now reformulate the RCP into a chance constrained problem ($CCP^t(\epsilon)$) as follows:

$$CCP^t(\epsilon) : \begin{array}{l} \min\limits_{u_t} C(u_t) \\ \text{s.t. } \; Prob\{d_t \in D : L(x_t, u_t, d_t) \leq 0\} > 1 - \epsilon, \\ \quad\;\; u^l \leq u_t \leq u^h \end{array}$$

***Definition** 2.8:* (ϵ-safety) The dynamical system (1) is said to be ϵ-safe if for all $d_t \in D$, there exists a control input $u_t \in U$ solving the problem CCP_ϵ^t.

We call the problem of designing a control input u_t that solves this chance-constrained problem as the "risk-tunable "control design problem, and formally state it as follows.

Risk-Tunable Control Design Problem $\mathcal{P}_r$: Given a user-defined risk tolerance bound ϵ, find control input u_t solving $CCP^t(\epsilon)$ such that the dynamical system (1) is rendered ϵ-safe at every time t.

III. RISK-TUNABLE CONTROL DESIGN

In this section, we develop an approach to solve the risk-tunable control design problem $\mathcal{P}_r$. We begin by making the following assumptions regarding the convexity of the chance-constrained problem CCP_ϵ^t.

***Assumption** 3.1:* (i) We suppose that the objective function $C(u_t)$ is a convex function in the control input u_t.

(ii) Let $u_t \subset U$ be a convex and closed set, and let $D \subset \mathbb{R}^n$. We assume that $L(x_t, u_t, d_t) : U \times D \to (-\infty, \infty]$ is continuous and convex in U, for any $d_t \in D$.

***Remark** 3.2:* Note that an exact numerical solution of $CCP^t(\epsilon)$ is intractable, see [28], [29]. Moreover, $CCP^t(\epsilon)$ is in general non-convex, even when Assumption 3.1 holds.

There are several ways to solve such chance-constrained problems, including approximating the uncertainty by a known process (e.g., Gaussian process) [13], [14], developing convex relaxations or approximations [19], [30], and sampling-based approaches [10], [11]. In this work, we develop a sampling-based design based on the scenario approach [11]. The key idea is that if a sufficient number of samples of the uncertainty $d_t \in D$ can be extracted, then we can obtain a controller that renders the system safe for most uncertainties up to a risk tolerance threshold.

***Definition** 3.3:* (**Scenario Design**) Assume that N independent identically distributed samples $d_t^1, ..., d_t^N$ are drawn according to probability $Prob$. A scenario design problem is given by the convex optimization problem:

$$RCP_N^t : \begin{array}{l} \min\limits_{u_t} C(u_t) \\ \text{s.t. } \; L(x_t, u_t, d_t^i) \leq 0, i \in \{1, ..., N\}, u^l \leq u_t \leq u^h. \end{array} \tag{7}$$

Note that the convexity of the problem assumed in Assumption 3.1 serves the purpose of enabling the relaxation of CCP_ϵ^t to a finite number of constraints and allows for a generalization of the solution to the CCP_ϵ^t based on the solution of the simpler RCP_N^t.

***Proposition** 3.4:* For the affine CBF defined in Example E1 in Remark 2.5, RCP_N^t is convex.

***Remark** 3.5:* While we present our results for CBF constraints of the form (4) for simplicity of exposition, the following results are generally applicable to other forms of CBF constraints such as exponential CBFs [2], provided that they satisfy Assumption 3.1. Note that Assumption 3.1 does not hold for Example E2 in Remark 2.5 (the CBF constraint, in that case, can in fact be shown to be concave; see Appendix). However, it is possible to pose obstacle avoidance problems in a convex setting in certain cases using an exponential CBF formulation (one such case is presented in our case study in Section IV to illustrate the broader applicability of the results in this section.)

We now have the following result.

***Theorem** 3.6:* For any risk bound $\epsilon \in (0,1)$ and confidence parameter $\beta \in (0,1)$, if

$$N \geq \frac{2}{\epsilon} \ln \frac{1}{\beta} + 2m + \frac{2m}{\epsilon} \ln \frac{1}{\beta}, \tag{8}$$

then, we have that the RCP_N^t is either infeasible, or if feasible, then $Prob^N\{V(u_t^*) < \epsilon\} \geq (1-\beta)$, that is, its solution u_t^* renders the system (1) ϵ-safe as in Definition 2.8 with probability greater than or equal to $1-\beta$.

Theorem 3.6 provides a bound on the number of samples of the uncertainty that are required to guarantee that the control input designed by solving RCP_N^t can render the system ϵ-safe. The confidence parameter β in (8) is the probability $Prob^N(= Prob \times ... \times Prob)$, (N times), of extracting samples of the uncertainty $\{d_t^1, ..., d_t^N\}$ for which the control input u_t^* does not render the system (1) safe.

We now address the question of when the scenario design problem RCP_N^t for for risk-tunable control design is guaranteed to have a solution. We show that, under an additional assumption, RCP_N^t can be shown to always be feasible.

***Assumption** 3.7:* For all $d_t \in D$, there exists $u_t \in U$ such that $\bar{h} \in [m, M]$, $m, M \in \mathbb{R}$, $\forall x \in X$, with $M > m \geq 0$.

With this assumption, we have the following result regarding the solution of RCP_N^t, and therefore, the safe control design problem $CCP^t(\epsilon)$.

***Theorem** 3.8:* Let Assumptions 3.1 and 3.7 hold. Then, for any risk bound $\epsilon \in (0,1)$ and confidence parameter $\beta \in (0,1)$, if $N \geq \frac{2}{\epsilon} \ln \frac{1}{\beta} + 2m + \frac{2m}{\epsilon} \ln \frac{1}{\beta}$, the scenario problem RCP_N^t is always solvable for any N samples of the uncertainty $\{d_t^1, \ldots, d_t^N\}$, the solution u_t^* is unique, and renders the system (1) ϵ-safe in the sense of Definition 2.8.

Theorems 3.6 and 3.8 provide a trade-off between the sample complexity and the achievable risk bound in the safe control design problem, representing an additional handle that can be tuned by designers based on application-specific considerations. Generally, achieving a tighter risk bound will require more samples of the uncertainty.

IV. CASE STUDY

We consider a quadcopter navigation problem with an obstacle whose position is uncertain to illustrate our risk-tunable design. As described in Remark 3.5, the CBF constraints for such obstacle avoidance problems are in general non-convex. However, in some cases, it is possible to develop convex safety conditions. We illustrate one such case here, where the nature of the dynamics arising from the system physics can be exploited to construct convex CBF conditions for the obstacle avoidance problem that are affine in the control input.

We begin with a dynamical model of the quadcopter derived in [31] and summarized here. Let the 3-dimensional position coordinates of the quadcopter along the x-,y-, and z-axis with respect to its body frame $\mathcal{F}_b$ of and the world frame of reference $\mathcal{F}_w$ be given by $x_b := (x_b, y_b, z_b)$ and $r := (r_x, r_y, r_z)$ respectively. The rotation matrix for coordinate transformation from the the body frame $\mathcal{F}_b$ to the world frame $\mathcal{F}_w$ is defined by (9), where ϕ, θ, and ψ denote the Z-X-Y Euler angles corresponding to the roll, pitch, and yaw of the quadcopter. Therefore, $r = \mathcal{R}_{wb} x_b$. Then, the quadrotor dynamics is given by

$$\dot{x} = Ax + Bu, x = \begin{bmatrix} \dot{r} \\ \ddot{r} \end{bmatrix}, A = \begin{bmatrix} \mathbf{0}_{3\times3} & I \\ \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} \end{bmatrix}, B = \begin{bmatrix} \mathbf{0}_{3\times3} \\ \mathbf{1}_{3\times3} \end{bmatrix}, \tag{10}$$

where the control input u comprises of the desired acceleration of the quadcopter. The dynamics of the controller under small angle assumptions on the Euler angles (that is, $\sin \hat{e} \approx \hat{e}, \cos \hat{e} \approx 1, \hat{e} \in \{\phi, \theta, \psi\}$) evolves as [32]:

$$u = \begin{bmatrix} \ddot{r}_1^{des} \\ \ddot{r}_2^{des} \\ \ddot{r}_3^{des} \end{bmatrix} = \begin{bmatrix} g(\theta^{des} \cos \psi^{des} + \phi^{des} \sin \psi^{des}), \\ g(\theta^{des} \sin \psi^{des} - \phi^{des} \cos \psi^{des}) \\ \frac{\sum_{i=1}^4 F_i^{des}}{m} - g \end{bmatrix}, \tag{11}$$

where m is the mass of the quadcopter, g is the acceleration due to gravity, and $\ddot{r}_i^{des}, i \in \{x, y, z\}$ is the desired acceleration component of the quadcopter in the x-,y-, and z-direction respectively, computed using the desired specifications on the Euler angles ϕ^{des}, θ^{des}, and ψ^{des}, and $F_i^{des}, i \in \{1, 2, 3, 4\}$ is the desired thrust on the i-th rotor of the quadcopter. The quadcopter dynamical parameters are set up based on [33].

The objective of the control design is to enable the quadcopter to reach a target position r_{goal}, while avoiding an obstacle with position $r_{obs} = \begin{bmatrix} r_{obs_x} + d & r_{obs_y} + d & r_{obs_z} + d \end{bmatrix}^T$, where $d \in D \subset \mathbb{R}$ is the uncertainty in the obstacle position. For this setting, we choose a safe set $\mathcal{S} = \{r : \bar{h}(r) \geq 0\}$, where

$$\bar{h}(r) = (r_{ex}/a)^4 + (r_{ey}/b)^4 + (r_{ez}/c)^4 - r_s, \tag{12}$$

is the CBF for system (10), where $r_{ex} = r_x - r_{obs_x} - d, r_{ey} = r_y - r_{obs_y} - d, r_{ez} = r_z - r_{obs_z} - d$, with $a, b, c \in \mathbb{R}_+$ can be chosen to represent the shape parameters of a super-ellipsoidal obstacle, and r_s is the safe distance from the obstacle to be maintained by the controller.

Now, from (10) and (12), notice that $\dot{\bar{h}}$ will not depend on the control input u, implying that the CBF constraint will be independent of the design variable (the control input). A standard approach to develop a CBF-based safety condition for such a system involves constructing an Exponential Control Barrier Function (ECBF) condition [1] of the form

$$\ddot{\bar{h}} + K \cdot [\bar{h} \quad \dot{\bar{h}}]^T \geq 0, \tag{13}$$

where $K = [K_1 \quad K_2], K_1, K_2 \in \mathbb{R}$, is a design parameter that can be chosen based on the application. Now, we can rewrite (13) as a convex constraint in u as follows.

***Proposition** 4.1:* The barrier condition in (13) for the quadrotor can be setup as the affine inequality $L(x, u, d) := -Pu - Q \leq 0$ with $P = \begin{bmatrix} \frac{4r_{ex}^3}{a^4} & \frac{4r_{ey}^3}{b^4} & \frac{4r_{ez}^3}{c^4} \end{bmatrix}$, and $Q = K_2 P \dot{r} - K_1 \bar{h}(r) + \dot{r}^T \begin{bmatrix} \frac{12r_{ex}^2}{a^4} & 0 & 0 \\ 0 & \frac{12r_{ey}^2}{b^4} & 0 \\ 0 & 0 & \frac{12r_{ez}^2}{c^4} \end{bmatrix} \dot{r}$, The constraint $L(x, u, d) \leq 0$ is convex in the control input u.

$$\mathcal{R}_{wb} := \begin{bmatrix} \cos\psi\cos\theta - \sin\phi\sin\psi\sin\theta & -\cos\phi\sin\psi & \cos\psi\sin\theta + \cos\theta\sin\phi\sin\psi \\ \cos\theta\sin\psi + \cos\psi\sin\phi\sin\theta & \cos\phi\cos\psi & \sin\psi\sin\theta - \cos\psi\cos\theta\sin\phi \\ -\cos\phi\sin\theta & \sin\phi & \cos\phi\cos\theta \end{bmatrix} \tag{9}$$

The formulation in Proposition 4.1 can be implemented in discrete-time by solving the following at each time step t:

$$(RCP_N^t)_q : \begin{aligned} &\min_{u_t} (r - r_{goal})^T F (r - r_{goal}) + u^T G u \\ &\text{s.t.} \ \ L(x_t, u_t, d_t^i) \leq 0, \ \forall i \in \{1, ..., N\}, \\ &u^l \leq u_t \leq u^h, \end{aligned} \tag{14}$$

where $F, G \in \mathbb{R}^3$ are positive semi-definite weighting matrices. Note that $(RCP_N^t)_q$ satisfies Assumption 3.7. Therefore, we extract samples $\{d_i^t\}$ of the uncertain obstacle position at time t according to Theorem 3.8. For our case study, the additional parameters pertaining to $(RCP_N^t)_q$ are: $d_t \in [-0.1, 0.1]$, $r_{goal} = (7.9, 8.1)$, $r_{obs} = (7.5, 7.5)$, $r_s = 0.4$, $(K_1, K_2) = (6, 8)$, $(a, b) = 0.4$, $\beta = 0.01$. The discretization time is chosen to be 0.1 sec. Note that we only control the quadcopter along the x- y axis, i.e. $m = 2$ in Theorem 3.8.

With these parameters, we study the impact of the tunable risk tolerance ϵ on the performance of the control design. As the risk tolerance is increased (Fig. 1), the quadcopter takes a more direct path towards the goal, with some instances where it crosses into the safety margin r_s around the obstacle. With a lower risk tolerance ($\epsilon = 0.001$ in Fig. 1), the quadcopter takes a much longer duration to reach the goal, following a more circuitous path around the obstacle. Thus, Fig. 1 illustrates how the risk in the design can be traded off for the time performance of the system. Fig. 1 also illustrates the probabilistic nature of the safety guarantees and the role of the uncertainty in the obstacle position in this design, with the same risk bound $\epsilon = 0.01$ resulting in two different trajectories with varying levels of safety violations.

We now examine how the sample complexity of our design based on Theorem 3.6 varies with the risk tolerance bound. Table I lists the number of samples of the uncertainty chosen for each of the risk tolerance bounds ϵ illustrated in Fig. 1. It is observed that the sample complexity increases exponentially as the the risk tolerance bound is decreased. For this case study, we find that the risk tolerance bound $\epsilon = 0.05$ provides represents an ideal design choice, bounding the risk of safety violations to under 5%, while maintaining a reasonable trajectory to reach the goal.

TABLE I: SAMPLE COMPLEXITY VS RISK TOLERANCE WITH $\beta = 0.01$

Risk bound ϵ	Number of samples N
0.1	216
0.05	484
0.01	3045
0.001	39618

V. CONCLUSION

We develop a safe control design approach where the probability of violation of a CBF-based safety constraint is bounded by a tunable user-defined risk, and demonstrated the design through simulations on a quadcopter navigation problem with obstacle avoidance constraints. Future directions include extensions to non-convex safety constraints and learning-based control designs.

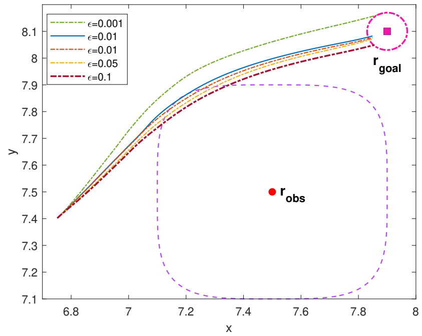

Fig. 1. Impact of risk tolerance bound on controller safety and performance.

VI. APPENDIX

1) *Proofs of Theorems 2.3 and 2.4*: These results arise directly from the standard definitions of CBFs [2], [26].
2) *Proof of Proposition 3.4 and non-convexity of the CBF condition in Example E2 in Remark 2.5*: These proofs follow directly from the definition of convexity.
3) *Proof of Theorem 3.6:* The proof is along the lines of [11]. We omit the dependence of all variables on time t for simplicity. Define $\mathcal{X}_i{:=}\{u \in U : L(x, u, d^i) \leq 0\}$. From Assumption 3.1, $\{\mathcal{X}_i\}$, $\forall i \in [1, N + 2m]$ are the convex sets defined by the $2m$ actuator constraints $u \in U = [u^l, u^h]$ and the N CBF constraints in RCP_N^t. Define convex optimization problems $\mathcal{P}$ and $\mathcal{P}_k$, $k{\in}[1, N{+}2m]$, obtained by removing the k^{th} constraint as:

$$\mathcal{P} : \min_{u_t} C(u_t), \quad s.t. \ u_t{\in} \bigcap_{i=\{1,...,N+2m\}} \mathcal{X}_i,$$

$$\mathcal{P}_k : \min_{u_t} C(u_t), \quad s.t. \ u_t \in \bigcap_{i=\{1,...,N+2m\}\setminus k} \mathcal{X}_i$$

Suppose RCP_N^t is feasible, and u_t^* is the optimal solution to $\mathcal{P}$, and u_k^* is the optimal solution to $\mathcal{P}_k$. Then, the k^{th} constraint is a *support constraint* if $C(u_k^*){<}C(u^*)$. The number of support constraints for problem $\mathcal{P}$ is at most m [11, Theorem 3]. Given N scenarios $\{d^1, ..., d^N\}$, select a subset $\mathcal{I} = \{i_1, ..., i_m\}$ of m indices from $1, ..., N{+}2m$ and let $\hat{u}_I^*$ be the optimal solution of RCP_I^t defined as

$$RCP_I^t : \begin{aligned} &\min_{u_t} C(u_t) \\ &s.t. \ L(x, u, d^i) \leq 0, \ \forall i \in \{1, ..., m\}, \\ &u^l \leq u \leq u^h. \end{aligned} \tag{15}$$

Let $\Delta^N{:=}\{d^i\}_{i=1,...,N}$ be the set of all possible N samples drawn from set D. Define $\Delta_I^N{\subset}\Delta^N$ as $\Delta_I^N{=}\{d^1, ..., d^N{:}\hat{u}_I^*{=}\hat{u}_N^*\}$ where $\hat{u}_N^*$ is the optimal solution with all N constraints corresponding to $\{d^1, ..., d^N\}$. Let $\mathcal{I}$ be a collection of all possible choices of m indices from $1, ..., N + 2m$, then $\mathcal{I}$ contains $\begin{pmatrix} N+m \\ m \end{pmatrix}$ sets and $\Delta^N{=}\bigcup_{I\in\mathcal{I}} \Delta_I^N$. Now suppose, $B{:=}\{d^1, ..., d^N \ : \ V(\hat{u}_N^*){>}\epsilon\}$ and $B_I{:=}\{d^1, ..., d^N \ :$

$V(\hat{u}_I^*)>\epsilon\}$. Then, $B = \bigcup_{I\in\mathcal{I}}(B_I \bigcap \Delta_I^N)$. A bound for $Prob^N(B)$ is now obtained by bounding $Prob(B_I \bigcap \Delta_I^N)$ and then summing over $I\in\mathcal{I}$. Following a similar argument as in the proof in [11, Appendix B], we have $Prob^N(B)\leq \sum_{I\in\mathcal{I}} Prob^N(B_I \bigcap \Delta_I^N)$ which can further be bounded as $\sum_{I\in\mathcal{I}} Prob^N(B_I \bigcap \Delta_I^N)< \begin{pmatrix} N+m \\ m \end{pmatrix}(1-\epsilon)^{N+m}$, since $\mathcal{I}$ has $\begin{pmatrix} N+m \\ m \end{pmatrix}$ sets. Then, following the algebraic manipulations in [11, Appendix B], from (8), we have $\begin{pmatrix} N+m \\ m \end{pmatrix}(1-\epsilon)^{N+m} \leq \beta$, that is, $Prob^N(B) < \beta$. Now, if RCP_N^t is only feasible on a subset $F_s\subset\Delta^N$, the same arguments hold to prove that $Prob^N(B)<\beta$. holds in the set F_s, with $B:=\{(d^1,...,d^N)\in F_s : V(\hat{u}_N^*) > \epsilon\}$.

4) *Proof of Theorem 3.8*: Since $h \in [m, M]$, $\forall u \in [u^l, u^h]$, we have $-L(x_t, u_t, d_t) \geq m - (1-\eta)M$, $\forall d \in D, \forall t \in \mathbb{R}_+$. Then, we can always select η, such that $1 \geq \eta \geq 1 - \frac{m}{M}$ to ensure $L(x_t, u_t, d_t) \leq 0$.
5) *Proof of Proposition 4.1*: The proof follows from differentiating (12), substituting in (13), collecting the terms with the control input u, and invoking Proposition (3.4).

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, 2016.

[2] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, “Control barrier functions: Theory and applications,” in *2019 18th European control conference (ECC)*. IEEE, 2019, pp. 3420–3431.

[3] J. J. Choi, D. Lee, K. Sreenath, C. J. Tomlin, and S. L. Herbert, “Robust control barrier–value functions for safety-critical control,” in *2021 60th IEEE Conference on Decision and Control (CDC)*. IEEE, 2021, pp. 6814–6821.

[4] J. Buch, S.-C. Liao, and P. Seiler, “Robust control barrier functions with sector-bounded uncertainties,” *IEEE Control Systems Letters*, vol. 6, pp. 1994–1999, 2021.

[5] S. Sadraddini, S. Sivaranjani, V. Gupta, and C. Belta, “Provably safe cruise control of vehicular platoons,” *IEEE Control Systems Letters*, vol. 1, no. 2, pp. 262–267, 2017.

[6] T. Gurriet, A. Singletary, J. Reher, L. Ciarletta, E. Feron, and A. Ames, “Towards a framework for realizable safety critical control through active set invariance,” in *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2018, pp. 98–106.

[7] R. Cheng, M. J. Khojasteh, A. D. Ames, and J. W. Burdick, “Safe multi-agent interaction through robust control barrier functions with learned uncertainties,” in *2020 59th IEEE Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 777–783.

[8] 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)*. IEEE, 2021, pp. 6286–6291.

[9] M. Santillo and M. Jankovic, “Collision free navigation with interacting, non-communicating obstacles,” in *2021 American Control Conference (ACC)*. IEEE, 2021, pp. 1637–1643.

[10] M. C. Campi, S. Garatti, and M. Prandini, “The scenario approach for systems and control design,” *Annual Reviews in Control*, vol. 33, no. 2, pp. 149–157, 2009.

[11] G. C. Calafiore and M. C. Campi, “The scenario approach to robust control design,” *IEEE Transactions on automatic control*, vol. 51, no. 5, pp. 742–753, 2006.

[12] M. C. Campi and S. Garatti, *Introduction to the scenario approach*. SIAM, 2018.

[13] L. Hewing, J. Kabzan, and M. N. Zeilinger, “Cautious model predictive control using gaussian process regression,” *IEEE Transactions on Control Systems Technology*, vol. 28, no. 6, pp. 2736–2743, 2019.

[14] E. Bradford and L. Imsland, “Stochastic nonlinear model predictive control using gaussian processes,” in *2018 european control conference (ECC)*. IEEE, 2018, pp. 1027–1034.

[15] R. Cheng, G. Orosz, R. M. Murray, and J. W. Burdick, “End-to-end safe reinforcement learning through barrier functions for safety-critical continuous control tasks,” in *Proceedings of the AAAI conference on artificial intelligence*, vol. 33, no. 01, 2019, pp. 3387–3395.

[16] Y. Hu, J. Fu, and G. Wen, “Safe reinforcement learning for model-reference trajectory tracking of uncertain autonomous vehicles with model-based acceleration,” *IEEE Transactions on Intelligent Vehicles*, 2023.

[17] W. Luo, W. Sun, and A. Kapoor, “Sample-efficient safe learning for online nonlinear control with control barrier functions,” in *Algorithmic Foundations of Robotics XV: Proceedings of the Fifteenth Workshop on the Algorithmic Foundations of Robotics*. Springer, 2022, pp. 419–435.

[18] C. Wang, M. Bahreinian, and R. Tron, “Chance constraint robust control with control barrier functions,” in *2021 American Control Conference (ACC)*. IEEE, 2021, pp. 2315–2322.

[19] L. Blackmore, H. Li, and B. Williams, “A probabilistic approach to optimal robust path planning with obstacles,” in *2006 American Control Conference*. IEEE, 2006, pp. 7–pp.

[20] Y. K. Nakka, A. Liu, G. Shi, A. Anandkumar, Y. Yue, and S.-J. Chung, “Chance-constrained trajectory optimization for safe exploration and learning of nonlinear systems,” *IEEE Robotics and Automation Letters*, vol. 6, no. 2, pp. 389–396, 2020.

[21] I. Salehi, T. Taplin, and A. P. Dani, “Learning discrete-time uncertain nonlinear systems with probabilistic safety and stability constraints,” *IEEE Open Journal of Control Systems*, vol. 1, pp. 354–365, 2022.

[22] M. J. Khojasteh, V. Dhiman, M. Franceschetti, and N. Atanasov, “Probabilistic safety constraints for learned high relative degree system dynamics,” in *Learning for Dynamics and Control*. PMLR, 2020, pp. 781–792.

[23] A. Ben-Tal and A. Nemirovski, “Robust convex optimization,” *Mathematics of operations research*, vol. 23, no. 4, pp. 769–805, 1998.

[24] ——, “On tractable approximations of uncertain linear matrix inequalities affected by interval uncertainty,” *SIAM Journal on Optimization*, vol. 12, no. 3, pp. 811–833, 2002.

[25] P. Akella and A. D. Ames, “A barrier-based scenario approach to verifying safety-critical systems,” *IEEE Robotics and Automation Letters*, vol. 7, no. 4, pp. 11 062–11 069, 2022.

[26] A. Agrawal and K. Sreenath, “Discrete control barrier functions for safety-critical control of discrete systems with application to bipedal robot navigation.” in *Robotics: Science and Systems*, vol. 13. Cambridge, MA, USA, 2017.

[27] L. El Ghaoui, F. Oustry, and H. Lebret, “Robust solutions to uncertain semidefinite programs,” *SIAM Journal on Optimization*, vol. 9, no. 1, pp. 33–52, 1998.

[28] A. Prékopa, *Stochastic programming*. Springer Science & Business Media, 2013, vol. 324.

[29] S. Vajda, *Probabilistic programming*. Academic Press, 2014.

[30] A. Nemirovski and A. Shapiro, “Convex approximations of chance constrained programs,” *SIAM Journal on Optimization*, vol. 17, no. 4, pp. 969–996, 2007.

[31] B. Xu and K. Sreenath, “Safe teleoperation of dynamic uavs through control barrier functions,” in *2018 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 2018, pp. 7848–7855.

[32] D. Mellinger, N. Michael, and V. Kumar, “Trajectory generation and control for precise aggressive maneuvers with quadrotors,” *The International Journal of Robotics Research*, vol. 31, no. 5, pp. 664–674, 2012.

[33] C. Ho, K. Shih, J. Grover, C. Liu, and S. Scherer, “”provably safe” in the wild: Testing control barrier functions on a vision-based quadrotor in an outdoor environment,” in *RSS 2020 Workshop in Robust Autonomy*, 2020. [Online]. Available: https://openreview.net/pdf?id=CrBJIgBr2BK