Risk-bounded Control using Stochastic Barrier Functions

Shakiba Yaghoubi, Keyvan Majd, Georgios Fainekos, Tomoya Yamaguchi, Danil Prokhorov, Bardh Hoxha

***Abstract*— In this paper, we design real-time controllers that react to uncertainties with stochastic characteristics and bound the probability of a failure in finite-time to a given desired value. Stochastic control barrier functions are used to derive sufficient conditions on the control input that bound the probability that the states of the system enter an unsafe region within a finite time. These conditions are combined with reachability conditions and used in an optimization problem to find the required control actions that lead the system to a goal set. We illustrate our theoretical development using a simulation of a lane-changing scenario in a highway with dense traffic.**

***Index Terms*— Barrier Function, Uncertainty, Robotics**

I. Introduction

In motion planning, an Autonomous Mobile System (AMS) is required to move from a start location to a goal location while avoiding collisions with other agents, dynamic and static. In this work, we provide a method for control synthesis to solve this start-to-goal motion problem while bounding "the probability of a collision in finite-time (risk)". We utilize a Barrier Function (BF) candidate whose level set of value one contains the unsafe set of the AMS and other agents' states [18]. The probabilistic nature of the behavior of agents is modeled using Stochastic Differential Equations (SDEs) [16]. Conditions on the BF candidate that bound its expected value over a finite-time horizon are derived based on the model of the AMS and the stochastic model of other agents. These conditions can be used to compute an upper bound on the risk [12], [19]. The upper bounds depend on the state of the system and the parameters used in the conditions that control the evolution of the expected value of the BF candidate. As a result, in a given state, we can bound the risk to a desired threshold by constraining the aforementioned parameters. We use these constraints to choose the values of the parameters and the control input. To lead the AMS to a goal location, our method unifies the conditions imposed by the BF for bounding the risk, with the conditions imposed by a Lyapunov function in a Quadratic Program (QP) which can be solved in real-time. The obtained sub-optimal control input will lead the AMS to the goal set while bounding the probability of entering the unsafe set in a finite time.

In many applications, safe motion planning is carried out based on forward reachable sets [1], [15]. Despite the efforts for finding more efficient methods for their computation [10], reachable sets are still difficult to compute in real-time.

S. Yaghoubi, T. Yamaguchi, D. Prokhorov, and B. Hoxha (<first_name.last_name>@toyota.com) are with the Toyota Research Institute of North America, Ann Arbor, MI, USA.

K. Majd and G. Fainekos ({majd,fainekos}@asu.edu) are with CIDSE, Arizona State University, Tempe, AZ, USA.

This research was partially funded by NSF OIA 1936997

On the other hand, Lyapunov functions have been widely used in literature to verify stability properties of systems without the need for computing their exact solutions. Inspired by Lyapunov functions, barrier certificates have been used recently for both safety verification and control design of safety-critical systems without the need for the difficult task of computing the system's reachable sets [23]. Since they do not require computation of reachable sets, barrier functions present a viable alternative for generating control inputs in real-time. Many recent works have used BFs in a deterministic setting to guarantee safe operating conditions. For instance BFs are used in [2] for designing adaptive cruise controls, in [22] for merging control in a traffic network, in [21] for finite-time convergence in a multi-agent system, and in [3] for obstacle avoidance for low-speed autonomous vehicles. Recently, BFs have been used with learning methods to achieve probabilistic safety for the learned dynamics [5], or controllers [9]. In the presence of uncertainty with hard bounds on its magnitude, BFs can verify input-to state safety [11] or safety in the worst case [24]. However, when the disturbance has stochastic characteristics, BFs should be considered in a stochastic setting. In [13], authors design BFs for nonholonomic systems in unknown environments modeled using stochastic semantic maps. Stochastic Barrier Functions (SBF) have been used in [18], [6] for verification of safety and temporal logic properties of stochastic systems. The authors in [19] use SBFs for finite-time stochastic system verification and feedback control design through solving sum-of-squares programs. However, finding such a closed-loop controller for more complicated systems and environments, and when uncertainty is higher, is not possible. To handle these cases, researchers consider the real-time computation of control inputs based on SBFs and using optimization methods. For instance, using QPs to design real-time control inputs for stochastic systems that maximize the probability of invariance of a set C has been studied in [4] using CBFs for complete and incomplete information and in [20] using high-relative degree SBFs. However, these works derive conditions that phase out the probability of eventually entering the unsafe set. Such a control input, if it exists, may be very conservative in many applications. Hence, in this work, we consider the real-time design of control inputs that bound the probability of a finite-time failure.

The main contributions of this paper are as follows: 1) In Section III-A, we develop the theoretical framework for the composition of conditions that control the finite-time growth of BFs with risk-bounds to derive sufficient conditions for risk-bounded control. The advantage of the the risk-based formulation of the conditions is that it allows for a less conservative control design framework. 2) In Section IV, we combine the aforementioned conditions with Lyapunov conditions in a QP whose on-the-fly solution solves the risk-bounded start-to-goal problem. 3) As discussed in Section V, this framework allows practitioners to specify bounds on the required level of safety guarantees. These bounds can differ when one safety requirement is more critical than another. 4) In Section VI, the proposed framework is demonstrated on a lane-changing scenario in a highway with dense traffic.

II. Problem Formulation

Consider a deterministic nonlinear affine control system as described in the following ordinary differential equation

$$\dot{x}_r(t) = f_r(x_r(t)) + g_r(x_r(t))u(t), \tag{1}$$

where $x_r(t) \in X_r \subseteq \mathbb{R}^{n_r}$ is the system state, $u(t) \in U \subseteq \mathbb{R}^l$ is the control input, and $f_r : \mathbb{R}^{n_r} \to \mathbb{R}^{n_r}$ and $g_r : \mathbb{R}^{n_r} \to \mathbb{R}^{n_r \times l}$ are locally Lipschitz continuous functions.

Also, consider a probability space $(\Omega, \mathcal{F}, P)$, and a standard Wiener process $w(t)$ defined on this space. A stochastic system is defined using the following Stochastic Differential Equation (SDE)

$$dx_o(t) = f_o(x_o(t), t)dt + g_o(x_o(t), t)dw(t), \tag{2}$$

where $x_o(t) \in X_o \subseteq \mathbb{R}^{n_o}$ is a stochastic process, and f_o and g_o are locally Lipschitz continuous functions of appropriate dimensions. Since in general the process $x_o(t)$ is not guaranteed to always lie inside the set X_o. the stopped process corresponding to $x_o(t)$ and X_o is defined as follows:

Definition 1 (Stopped Process [12])**.** *Assume that τ is the first time that $x_o(t)$ exits the interior of the set X_o. Then the stopped process $\tilde{x}_o(t)$ is defined as*

$$\tilde{x}_o(t) = \begin{cases} x_o(t) & if \quad t < \tau \\ x_o(\tau) & if \quad t \geq \tau \end{cases} \tag{3}$$

Remark 1. *The subscripts r, and o are used in the paper to indicate the quantities corresponding to the deterministic system, and the stochastic system, respectively.*

Assume that $\zeta : X_r \to \mathbb{R}_+$ is a function that defines the goal set of the system (1), as follows

$$X_{\mathsf{g}} = \{x_r \in X_r \,|\zeta(x_r) \leq 0\}. \tag{4}$$

Also, let us define the stopped process $\tilde{x}(t) = [x_r(t), \tilde{x}_o(t)]^\top$ corresponding to the augmented state $x(t) = [x_r(t), x_o(t)]^\top$, and an unsafe region on the augmented space $X_r \times X_o$. We denote this unsafe region with $X_{\mathsf{u}} \subset X_r \times X_o$ and define it using a function $h : X_r \times X_o \to \mathbb{R}_+$ as follows

$$X_{\mathsf{u}} =: \{\tilde{x} \in X_r \times X_o \mid h(\tilde{x}) \leq 0\}. \tag{5}$$

Given the state of the system at time t, $\tilde{x}(t) = [x_r(t), \tilde{x}_o(t)]^\top$, and a planning time horizon T, we define p_{u} as the probability that the process enters the unsafe set during this planning horizon, namely,

$$p_{\mathsf{u}} = P\{\tilde{x}(\tau) \in X_{\mathsf{u}} \;\text{ for some } t \leq \tau \leq t+T \mid \tilde{x}(t) \in X_r {\times} X_o\}. \tag{6}$$

Here, we use the term "risk" informally to refer to this event's probability (p_{u}) (see [14] for a more formal discussion about risk metrics).

A desired control input signal u steers the trajectory of the system (1) to X_g while bounding p_{u} for all $t \geq 0$ to a given desired threshold $\bar{p}$. Hence the problem we need to address is formalized as follows:

Problem 1. *Find a control input signal $u : \mathbb{R}_+ \to U$ for the system (1), s.t. 1) there exists some time $t_{\mathsf{g}} > 0$ for which $\zeta(x_r(t_{\mathsf{g}})) \leq 0$, and 2) at any time t which satisfies $0 \leq t \leq t_g$, given $x_r(t)$ of system (1) and $x_o(t)$ of system (2), the control input $u(t)$ bounds the risk p_{u} by the desired upper threshold $\bar{p}$, i.e., $p_{\mathsf{u}} \leq \bar{p}$.*

III. Stochastic Control Barrier Functions

In this section, we first review some background information about stochastic systems and processes, and then derive conditions on a BF candidate to bound the risk.

The evolution of a function of a deterministic system's state can be characterized using Lie derivatives. The stochastic analog of the Lie derivatives are infinitesimal generators which characterise the evolution of the expectation of functions of the stochastic system's state $x_o(t)$ [18]:

Definition 2 (Infinitesimal generator)**.** *The infinitesimal generator A of a stochastic process $x_o(t)$ on $\mathbb{R}^{n_o}$ is defined by*

$$AB(x_0) = \lim_{t \to 0} \frac{E[B(x_o(t)) \mid x_o(0){=}x_0] - B(x_0)}{t},$$

for all the functions $B : \mathbb{R}^{n_o} \to \mathbb{R}$ for which the above limit exists for all x_0 [16].

Let $x_o(t)$ be a stochastic process satisfying Eq. (2). The generator A of a twice differentiable function $B : \mathbb{R}^{n_o} \to \mathbb{R}$ is given by [16]

$$AB(x_o) = \frac{\partial B}{\partial x_o} f_o(x_o, t) + \frac{1}{2} tr\Big(g_o(x_o, t)^\top \frac{\partial^2 B}{\partial {x_o}^2} g_o(x_o, t)\Big).$$

where $tr(.)$ computes the trace of a square matrix.

The stopped process $\tilde{x}_o(t)$ in Eq. (3) inherits the right continuity and strong Markovian property of $x_o(t)$. It also shares the same infinitesimal generator corresponding to $x_o(t)$ on X_o.

A. Bounded Risk Using Stochatic Control Barrier Functions

In the following, we derive the conditions on the control input s.t. the risk is bounded from above by the desired upper threshold. We build upon the idea of [18] to define a BF whose level set of value one contains X_{u} so that the evolution of the BF's expected value can be used to compute upper bounds on p_{u}. These bounds have been proved to exist in [12] and are collected in [19] for finite-time stochastic system verification and feedback control design. We use the computed upper bounds to establish conditions on the evolution of the BF s.t. p_{u} is bounded to $\bar{p}$, and choose control actions according to these conditions in real-time.

Definition 3. *A twice differentiable function $B : X_r \times X_o \to \mathbb{R}_+$ is a Barrier Function (BF) candidate w.r.t the sets*

X_r, X_o, X_{u}, *if*

$$B(x) \geq 0 \quad \forall x \in X_r \times X_o, \text{ and} \tag{7}$$

$$B(x) \geq 1 \quad \forall x \in X_{\mathsf{u}}. \tag{8}$$

Example 1. *If h is a differentiable function, $B(x) = e^{-\gamma h(x)}$ is a BF candidate for $\gamma > 0$ w.r.t X_{u} as defined in (5).*

In what follows we assume that solutions to Eq. (1) are guaranteed to exist until at least t_g. As an example, a locally Lipschitz continuous state feedback control $u(t) = u(x)$ or a piecewise continuous time-varying control $u(t)$ can guarantee the existence of solutions to Eq (1) [8].

Definition 4. *Consider the system of Eq. (1) with a control input $u(t) = u(x)$, augmented with the stochastic system in Eq. (2). A BF candidate B is a Stochastic Barrier Function (SBF) for this augmented system, if there exist $a \geq 0, b \geq 0$ s.t. the following condition on the infinitesimal generator of B is satisfied $\forall x \in X_r \times X_o$,*

$$\frac{\partial B}{\partial x} F_{cl}(x) + \frac{1}{2} tr(g_o(x_o,t)^\top \tfrac{\partial^2 B}{\partial {x_o}^2} g_o(x_o,t)) \leq -aB(x) + b,$$

where $F_{cl}(x) = [f_r(x_r) + g_r(x_r)u(x)), f_o(x_o,t)]^\top$.

Given the current state of the defined augmented system $x(t)$, an SBF provides a bound on p_{u} (probability of entering the unsafe set during the planning horizon T):

Theorem 1. *Consider the stopped process $\tilde{x}(t)$ w.r.t the augmented system state $x(t)$, define $B_0 = B(x(t))$, and $p_B = P\{\sup_{t \leq \tau \leq t+T} B(\tilde{x}(\tau)) \geq 1 \mid \tilde{x}(t) \in X_r \times X_o\}$. Then:*

$$\text{If } a = 0: \quad p_{\mathsf{u}} \leq p_B \leq B_0 + bT. \tag{9}$$

$$\text{If } a > 0,\ b \leq a: \quad p_{\mathsf{u}} \leq p_B \leq 1 - (1 - B_0)e^{-bT}. \tag{10}$$

$$\text{If } a > 0,\ a \leq b: \quad p_{\mathsf{u}} \leq p_B \leq \tfrac{B_0 + (e^{bT} - 1)\frac{b}{a}}{e^{bT}}. \tag{11}$$

Proof. The bounds are immediate corollaries of [12, Ch. 3, Thrm. 1, and Cor. 1-1]. □

Remark 2. *Note that for $B(\tilde{x}(t)) = B_0 \neq 0$, and $T = 0$, the right hand side of inequalities in Thrm. 1 do not reduce to zero. The reason is that the method of proof for finding the bounds in [12] does not distinguish between the fixed/deterministic initial conditions for $B(\tilde{x})$ and initial conditions which are random variables with expected value $B(\tilde{x}(t))$. Hence, the results remain valid for the case of nonanticipative initial conditions with mean $B(\tilde{x}(t))$.*

The definition of a SBF is more suitable for verifying stochastic safety properties of a system with a closed form state feedback control $u(x)$. When solving a control synthesis problem, additional conditions on a BF candidate should depend on the choice of the control input:

Definition 5. *A BF candidate B is a Stochastic Control Barrier Function (SCBF) for the augmented system of Eq. (1), and (2), if there exist a control input $u \in U$ s.t. for all $x \in X_r \times X_o$ the following condition is satisfied for some $a \geq 0, b \geq 0$.*

$$\frac{\partial B}{\partial x}(F_{ol}(x) + e_r g_r(x_r)u) + \frac{1}{2} tr(g_o(x_o,t)^\top \tfrac{\partial^2 B}{\partial {x_o}^2} g_o(x_o,t)) \leq -aB(x) + b, \tag{12}$$

where $F_{ol}(x) = [f_r(x_r), f_o(x_o,t)]^\top$, and $e_r = [I_{n_r}, 0_{n_r \times n_o}]^\top$, in which I_n is an $n \times n$ identity matrix, and $0_{n \times m}$ is an $n \times m$ zero matrix.

While Thrm. 1 provides us with bounds on the risk as functions of a, b, B_0, T, we still need to provide conditions on a, b (B_0 given $\tilde{x}(t)$, and T are fixed) and the control input u to guarantee that the risk is always bounded by $\bar{p}$. We derive these conditions using SCBFs below:

Theorem 2. *Suppose that there exists a SCBF B for the augmented system of Eq. (1), and (2). If at each visited state $\tilde{x}(t)$, the control input $u \in U$ satisfies the conditions of Def. 5 for some $a \geq 0, b \geq 0$ s.t. one of the conditions*

$$a = 0, b \leq (\bar{p} - B_0)/T, \tag{13}$$

$$a > 0, b \leq \min(a, -\tfrac{1}{T} \ln \tfrac{1-\bar{p}}{1-B_0}), \text{ or} \tag{14}$$

$$a > 0, \tfrac{b(e^{bT}-1)}{\bar{p}e^{bT} - B_0} \leq a \leq b \tag{15}$$

hold, then for all $t \geq 0$, $p_{\mathsf{u}} \leq \bar{p}$ holds.

Proof. Based on the assumptions, the function B becomes a SBF for the system in Eq. (1) in closed loop with a control input u that satisfies the conditions of Thrm. (2), hence the bounds in (9)-(11) are valid. Since the extra conditions on a, b in inequalities (13)-(14) based on which the control is chosen bound the right hand sides of (9)-(11) to $\bar{p}$, we have $p_{\mathsf{u}} \leq \bar{p}$, and the proof is complete. □

IV. Risk Bounded Optimization-Based Control Design

In this section, we use the properties of SCBFs for synthesizing risk-based control inputs. We use the constraint in Eq. (12) combined with the constraints on a, b in Eq. (9), (10), or (11) in an optimization problem with a quadratic cost in u to find an optimal control input that bounds the risk. Such an optimization problem has an objective function:

$$J(u) = (u - u_d)^T Q (u - u_d), \tag{16}$$

where u_d is a desired value which is set to zero if input minimization is desired, and Q is a diagonal matrix with non-negative elements. Hence, given $\bar{p}$, the following optimization problem can be solved each time new information about the states x_r, x_o is received, and the obtained control value u^* can be used to bound the risk until new information is received and a new control value is computed.

$$\min_{u \in U, a, b} J(u) \tag{17}$$

$$\text{s.t.} \begin{cases} \text{Ineq. (12)} \\ \text{Ineq. (13), or (14), or (15)} \end{cases}.$$

Note that in the above program the objective function and the first constraint are respectively quadratic and linear in the search parameters u, a, b. However, the second constraint imposed by Eq. (14), or (15) are nonlinear in either a or b.

Hence, in order to transform the program (17) to a quadratic program (QP) for which efficient solvers exist, one can fix a in (13) or b in (14) to positive values, and find the other parameter to satisfy the second constraint along with an optimal control u that bounds the risk to $\bar{p}$. Also, in order to minimize the risk when possible, parameters a and b can be included in the objective function with negative and positive multipliers respectively (note the inverse relationship of the upper bound in Eq. (11) with a and the direct relationship of the upper bounds in equations (9)-(11) with b).

A. Goal Set Reachability

Recall that a solution to Prob. 1 should lead the states of the system (1) to a goal set while bounding the risk. An advantage of using BF methods for safety is that they can be combined with methods that seek other objectives like reachability. In this section, we derive the conditions under which the control input of the system (1) lead the states x_r to a goal set X_{g} as in Eq. (4).

Definition 6 (Control Lyapunov like Function (CLF))**.** *A differentiable function $V : X_r \to \mathbb{R}$ is a Control Lyapunov like[1] function (CLF), if it satisfies the following conditions*

$$V(x_r) > 0 \quad \forall x_r \in X_r/X_g, \tag{18}$$

$$V(x_r) \leq 0 \quad \forall x_r \in X_g, \tag{19}$$

$$\forall x_r \in X_r,\ \exists u \in U \text{ s.t: } \frac{\partial V}{\partial x_r}(f_r(x_r) + g_r(x_r)u) \leq 0. \tag{20}$$

If the control input u satisfies Ineq. (20) for all $x_r \in X_r$, then $V(x)$ decreases in value until eventually $V(x) \leq 0$ and hence the goal set X_{g} is reached. Hence, the reachability objective can be unified with safety objectives by considering the program (17) with an additional constraint imposed by a CLF $V(x)$ as defined in Def. 6, as follows

$$\min_{u \in U, a, b, \delta} J(u) + k\delta \tag{21}$$
$$\text{s.t.} \begin{cases} \text{Ineq. (12)} \\ \text{Ineq. (13), or (14), or (15)} \\ \frac{\partial V}{\partial x_r}(f_r(x_r) + g_r(x_r)u) \leq \delta \end{cases} .$$

where k is a positive constant. A candidate for the function $V(x)$ when ζ is a differentiable function is $V(x) = \zeta(x)$ (see the definition of X_{g} in Eq. (4)).

As in [2], in the above program, the CLF constraint (20) is relaxed through δ. By adding δ to the objective function, we allow for control inputs that minimally violate the Lyapunov constraint (20) when instantaneous improvement toward the goal set contradicts safety conditions. Since δ is considered in the objective function when safety and reachability constraints do not conflict, they will be satisfied at the same time, and Prob. 1 can be solved by iteratively solving program (21).

Program (21) can also be transformed into a QP by fixing either a or b. Also, these parameters can be included in the objective function to scale down the risk when possible, and to increase the chance of finding an admissible control u that satisfies the constraints at a later time. Whereas, if the inequality constraints are always satisfied with equality, the chance of not finding an effective reaction to the stochastic process x_o through an admissible control $u \in U$ increases in the next iterations. But also note that the hard constraint on a or b prevents choosing riskier actions that possibly decrease the total objective function by an immediate movement toward the goal set or by reducing the control cost $J(u)$.

[1]Despite conventional Lyapunov functions the positive definiteness of $V(x)$ is not neccessary since reachability (and not stability) is the objective.

V. Control Design in the Presence of Multiple Unsafe regions

When designing a real-time control input for the system (1) by iteratively solving an optimization problem, it may be required to consider safety w.r.t a varying number of stochastic processes at each iteration. Furthermore, different bounds may be needed on their associated risks. For instance, system (1) can describe the model of a vehicle that needs to be driven/controlled in presence of a varying number of other vehicles with stochastic characteristics, and the risk bounds corresponding to larger, or emergency agent vehicles may need to be set to smaller values too. In this case, the control action should satisfy a a varying number of safety constraints related to the agents.

Assume that in an specific iteration, M stochastic processes $x_{o,i}, i = 1, 2, ..., M$ defined using SDEs of the form (2) - with $f_o = f_{o,i}$, $g_o = g_{o,i}$, $w = w_i$ - need to be considered in the control design. We denote the corresponding unsafe sets with $X_{\mathsf{u},i}$s. Each of these sets is defined on the space of the augmented state $\tilde{x}_i = [x_r, \tilde{x}_{o,i}]^\top$ using a relation over a function $h_i(\tilde{x}_i)$, like in Eq. (5). In order to bound $p_{\mathsf{u},1}, ..., p_{\mathsf{u},M}$ (the probabilities of entering the unsafe sets $X_{\mathsf{u},i}$ within a given time-horizon) to $\bar{p}_1, ..., \bar{p}_M$, we need to consider M BF candidates B_i for each unsafe set $X_{\mathsf{u},i}$ based on the Def. 3. Note that one can consider a smaller value for $\bar{p}_i$, if entering the unsafe set $X_{\mathsf{u},i}$ has a more severe impact on the system. The BFs then can be used to find a series of M conditions formed based on Thrm. 2. These conditions can be added to program (21) to find a sub-optimal control input that bounds the risks $p_{\mathsf{u},i}$ while reaching the goal set. Note that even with our framework that allows for designing less conservative controllers, when multiple safety constraints are present or $U \neq \mathbb{R}^l$, feasibility of program (21) cannot be assured. In fact, such a framework needs to be considered as part of a larger architecture wherein a backup controller is implemented if no feasible solution to program (21) is found.

A. Application to Nonholonomic Systems

The deterministic system (1) can describe a unicycle model that can be considered as a simplified model of an AMS, i.e $x_r = [\mathsf{p}_r^x, \mathsf{p}_r^y, \theta_r]^\top$, $u = [u_1, u_2]^\top$, where $\mathsf{p}_r^x, \mathsf{p}_r^y, \theta_r$ describe the x and y position of the robot and its heading angle respectively, and u_1, u_2 are the linear and angular velocities of the robot. Also $f_r = [0, 0, 0]^\top$, and

$$\dot{x}_r(t) = g_r(x_r(t))u(t) = \begin{bmatrix} \cos(\theta_r) & 0 \\ \sin(\theta_r) & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}. \tag{22}$$

In this case, the projection of X_r into its first and second dimentions represents the AMS's work space, i.e, the environment in which it is moving, and its projection into its third dimension is $[-\pi, \pi]$. The goal set of the AMS can describe a set of position states in $\mathbb{R}^2$:

$$X_{\mathsf{g}} =: \{x_r \in X_r \mid ([\mathsf{p}_r^x, \mathsf{p}_r^y] - x_g)^2 - r_g^2 \le 0\}, \quad (23)$$

where x_g is the center and r_g is radius of the goal set.

There are M agents around the AMS whose stochastic behavior can be modelled using SDEs of the form (2). Assuming that each agent $i \in 1, ..., M$ is moving in direct line with slope γ_i, it can be modelled as

$$dx_{o,i}(t) = [v_{c,i} \quad \gamma_i v_{c,i}]^\top dt + c_i[1 \quad \gamma_i]^\top dw_i, \quad (24)$$

where c_i is a constant, $x_{o,i} = [\mathsf{p}_{o,i}^x, \mathsf{p}_{o,i}^y]^\top$ is the agent i's position, $v_i = v_{c,i} + w_i$ is its velocity where $v_{c,i}$ is a constant value and w_i is a stochastic Wiener process representing the stochastic changes in agent i's velocity.

AMS's collisions with moving agents are undesirable, hence one can define the unsafe sets as

$$X_{u,i} =: \{\tilde{x}_i \in X_r \times X_{o,i} \mid ([\mathsf{p}_r^x, \mathsf{p}_r^y] - [\mathsf{p}_{o,i}^x, \mathsf{p}_{o,i}^y])^2 - r_i^2 \le 0\}, \quad (25)$$

where $\tilde{x}_i = [x_r, \tilde{x}_{o,i}]$ is the stopped process corresponding to the augmentation of the AMS's state and the obstacle i's state, $x_i = [x_r, x_{o,i}]$, and r_i depends on the width/length/radius of the AMS and the agent i.

To find a control input u that leads the AMS to the goal set while bounding the probabilities of collisions with agents $1, ..., M$ in finite-time T to $\bar{p}_1, ..., \bar{p}_M$, program (21) with conditions based on BFs w.r.t $X_{u,i}$s can be solved.

B. SCBFs and CLFs for Nonholonomic Systems

For the non-holonomic system of Eq. (22), with an unsafe set of the form (25) which represents a set of position states of the system, the control inputs u_1 and u_2 (the linear and angular velocities) have different relative degrees w.r.t the BF candidate $B_i(x_i) = e^{-\gamma_i h_i(x_i)}$. The consequence is that while u_1 appears in the right hand side of the Ineq. (12), u_2 does not. Hence, u_2 cannot be derived accordingly to help render the system risk-bounded. So the constraint in Thrm. 2 may not be satisfied if $\frac{\partial B_i}{\partial x_i} e_r g_r(x_r) u = \frac{\partial B_i}{\partial \mathsf{p}_r^x} cos(\theta) + \frac{\partial B_i}{\partial \mathsf{p}_r^y} sin(\theta)$ is a zero vector, or if no admissible velocity u_1 in the corresponding bounds in U can satisfy the constraint in Thrm. 2. As in [17], [13], to avoid involved control design methods, we use a near-identity diffeomorphism to solve the problem for a closely related system. Consider $\bar{x}_r = [\bar{\mathsf{p}}_r^x, \bar{\mathsf{p}}_r^y, \bar{\theta}_r]$, and the transformation $\bar{x}_r := x_r + l[R(\theta_r)e_1, 0]^\top$, where $l > 0$ is a small constant that allows for approximating x_r with $\bar{x}_r$ with the needed precision, $R(\theta_r) = \begin{bmatrix} \cos(\theta_r) & -l\sin(\theta_r) \\ \sin(\theta_r) & l\cos(\theta_r) \end{bmatrix}$, and $e_1 = [1, 0]^\top$. Hence:

$$\dot{\bar{x}}_r(t) = \begin{bmatrix} \cos(\theta_r) & -l\sin(\theta_r) \\ \sin(\theta_r) & l\cos(\theta_r) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}. \quad (26)$$

In the full rank system of Eq (26) both u_1, u_2 appear in Ineq. (12), and they can both contribute to satisfaction of the condition. Note that the maximum distance of x_r from $\bar{x}_r$ is l. Hence, defining $\bar{x}_i = (\bar{x}_r, \tilde{x}_{o,i})$, the unsafe sets can be expanded to account for the introduced error as

$$\bar{X}_{u,i} =: \{\bar{x}_i \mid ([\bar{\mathsf{p}}_r^x, \bar{\mathsf{p}}_r^y] - [\mathsf{p}_{o,i}^x, \mathsf{p}_{o,i}^y])^2 - (r_i + l)^2 \le 0\}. \quad (27)$$

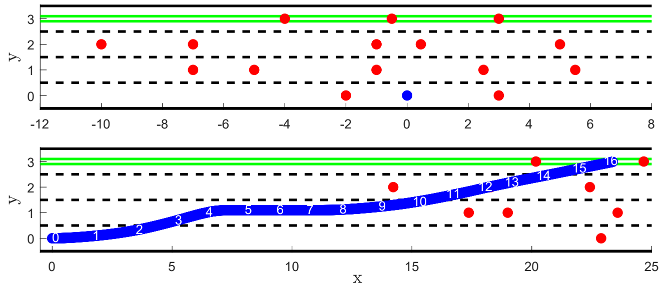

Fig. 1: Top: Initial positions of the ego vehicle and traffic participants. Bottom: Final position of the traffic participants alongside with the time-stamped trajectory of the ego vehicle from start to finish. Simulation video can be found at https://youtu.be/hqGe8h1erzA.

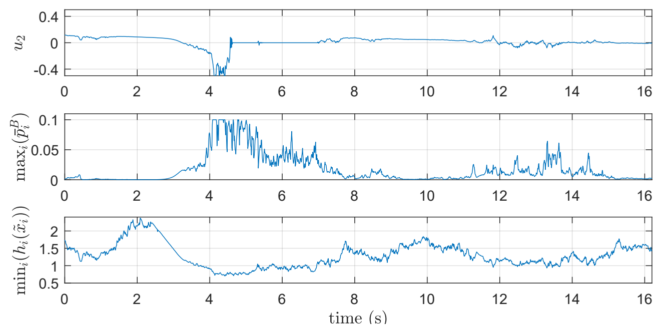

Fig. 2: Figures show control input signals, maximum upper bound to p_i^B over all the traffic participants, minimum $h_i(x)$ over all the traffic participants respectively.

VI. Experimental Results

In this section, we illustrate our method on a reach-avoid problem in a highway scenario. An ego vehicle in the rightmost lane needs to reach the left-most lane while avoiding collisions with other traffic participants. The ego vehicle is modelled using the unicycle model of Eq. (22) with the initial condition $x_r(0) = [0, 0, 0]^\top$. The linear and angular velocities of the vehicle are considered to be in the set $u \in U = \{0 \le u_1 \le 2, \ -\pi/6 \le u_2 \le \pi/6\}$. It is assumed that the traffic participants move in their lanes with stochastic velocities close to the highway's desired speed, and, hence, they are modelled using the SDE in (24) with $v_{c,i} = 1.5, c_i = 0.2$, and $\gamma_i = 0$. We consider a scenario with 15 traffic participants with different initial states $x_{o,i}(0)$. The top subplot in Fig. 1 shows the position of the ego vehicle (in blue) and the traffic participants (in red). The goal set (shown in green) is $X_{\mathsf{g}} = \{x_r | (\mathsf{p}_r^y - 3)^2 \le 0.1^2\}$.

We define the sets $X_{\mathsf{u},i}, \ i = 1, ..., 15$ that include the augmented state of the ego car and the traffic participant i, $\tilde{x}_i$, as in Eq. (25) with $r_i = 0.5$, i.e:

$$X_{\mathsf{u},i} = \{\tilde{x}_i \in X_r \times X_{o,i} \mid ([\mathsf{p}_r^x, \mathsf{p}_r^y] - [\mathsf{p}_{o,i}^x, \mathsf{p}_{o,i}^y])^2 - 0.5^2 \le 0\}.$$

At time t, the control input $u(t)$ should be designed to bound the risks of entering the sets $X_{\mathsf{u},i}$ within a 1-second time horizon ($T = 1$) by $\bar{p}_i = 0.1$ for all $i = 1, ..., 15$. In order to find such a control input using BFs of the form $B_i(x_i) = e^{-\gamma_i h_i(x_i)}$, we transform the model of the ego vehicle using Eq. (26) with $l = 0.01$. In order to compensate for the transformation error, we define new unsafe sets as in Eq. (27). Hence, we define $B_i(\bar{x}_i) = e^{-\gamma_i h_i(\bar{x}_i)}$ with $\gamma_i = 5$ and $h_i(\bar{x}_i) = ([\bar{\mathsf{p}}_r^x, \bar{\mathsf{p}}_r^y] - [\mathsf{p}_{o,i}^x, \mathsf{p}_{o,i}^y])^2 - (0.5 + l)^2$.

At each state $\bar{x}_r$ in order to find a sub-optimal control input u that guides the ego vehicle to reach the goal set in the top lane, while bounding the risk to $\bar{p}_i = 0.1$, we formulate the quadratic program (21), by fixing $a_i = 1$, and using constraints from Ineq. (14), and $V(\bar{x}_r) = (\bar{\mathsf{p}}_r^y - 3)^2 - (0.1 + l)^2$. To guide the program to minimize the risk when possible and avoid a risky action when it is not necessary, we will add the variables b_i to the objective function. Also, at each state $\bar{x}_r$, to improve the efficiency, we only consider the SCBF constraints related to the traffic participants that are in a distance 3 or less of the ego vehicle. Finally, we add an additional soft constraint to the QP to encourage smaller input changes from iteration to iteration. The bottom subplot in Fig. 1, shows the resulting - time-stamped - trajectory of the ego vehicle and the final positions of the traffic participants. The computed control inputs u_1 and u_2 are admissible and lie in the corresponding bounds of U. The control input related to the angular velocity (u_2) is shown in the top subplot in Fig. 2. The middle subplot shows the maximum $\bar{p}_i^B$ over all the traffic participants, where $\bar{p}_i^B = 1 - (1 - B_0)e^{-b_i T}$ is the upper bound to the risk p_i^u (see Eq. (10)). The bottom subplot shows the minimum $h_i(\bar{x}_i)$ over all the traffic participants. From the figures, we can see that $\bar{p}_i^B$, and, hence the chance of an upcoming collision in the next 1 second is bounded to 0.1. The correlation between the bottom two subplots shows that as expected, the risk increases as the distance between the ego vehicle and some traffic participant $(\min_i(h_i(\bar{x}_i)))$ is about to decrease. Another observation is that when risk increases and approaching the goal set conflicts with risk-related constraints, the computed angular velocity (u_2) steers the ego vehicle away from the traffic participants in the opposite direction of the goal set. So, when necessary reachability objective is postponed until it can be satisfied with the safety constraints at the same time. Note that our experiments show that the task cannot be completed if the risk is not tolerated and the input u is expected to make the probability of the undesired event zero as required in previous works like [4, Cor. 1].

VII. Conclusion

This paper presented the conditions under which the system's probability of failure in a finite time becomes bounded to desired thresholds. These conditions depend on BF candidates that contain the unsafe operating conditions and constrain the growth of their expected value to bound the probability of failure. These constraints combined with constraints based on Lyapunov functions are used in a QP to design safe sub-optimal control inputs that stabilize the system or lead the system to a set of goal states, online. Our case study uses the proposed constrained QP to successfully drive a vehicle that needs to change lanes in a crowded highway while bounding the risk of collisions. In the future, we consider using the work in [7] to modify our proposed QPs to achieve guaranteed asymptotic convergence rate.

References

[1] Matthias Althoff, Olaf Stursberg, and Martin Buss. Stochastic reachable sets of interacting traffic participants. In *2008 IEEE Intelligent Vehicles Symposium*, pages 1086–1092. IEEE, 2008.

[2] Aaron D Ames, Jessy W Grizzle, and Paulo Tabuada. Control barrier function based quadratic programs with application to adaptive cruise control. In *53rd IEEE Conference on Decision and Control*, 2014.

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

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

[5] David D Fan et al. Bayesian learning-based adaptive control for safety critical systems. In *2020 IEEE International Conference on Robotics and Automation (ICRA)*, pages 4093–4099. IEEE, 2020.

[6] Pushpak Jagtap, Sadegh Soudjani, and Majid Zamani. Temporal logic verification of stochastic systems using barrier certificates. In *International Symposium on Automated Technology for Verification and Analysis*, pages 177–193. Springer, 2018.

[7] Mrdjan Jankovic. Robust control barrier functions for constrained stabilization of nonlinear systems. *Automatica*, 96:359–367, 2018.

[8] Hassan K Khalil. Nonlinear systems. *Upper Saddle River*, 2002.

[9] Mohammad Javad Khojasteh, Vikas Dhiman, Massimo Franceschetti, and Nikolay Atanasov. Probabilistic safety constraints for learned high relative degree system dynamics. In *Learning for Dynamics and Control*, pages 781–792, 2020.

[10] Niklas Kochdumper, Bastian Schürmann, and Matthias Althoff. Utilizing dependencies to obtain subsets of reachable sets. In *Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control*, pages 1–10, 2020.

[11] Shishir Kolathaya and Aaron D Ames. Input-to-state safety with control barrier functions. *IEEE control systems letters*, 3(1), 2018.

[12] Harold J Kushner. Stochastic stability and control. Technical report, Brown Univ Providence RI, 1967.

[13] Lars Lindemann, George J Pappas, and Dimos V Dimarogonas. Control barrier functions for nonholonomic systems under risk signal temporal logic specifications. *arXiv preprint arXiv:2004.02111*, 2020.

[14] Anirudha Majumdar and Marco Pavone. How should a robot assess risk? towards an axiomatic theory of risk in robotics. In *Robotics Research*, pages 75–84. Springer, 2020.

[15] Nick Malone et al. Hybrid dynamic moving obstacle avoidance using a stochastic reachable set-based potential field. *IEEE Transactions on Robotics*, 33(5):1124–1138, 2017.

[16] Bernt Øksendal. Stochastic differential equations. In *Stochastic differential equations*, pages 65–84. Springer, 2003.

[17] Reza Olfati-Saber. Near-identity diffeomorphisms and exponential e-tracking and 6-stabilization of first-order nonholonomic se (2) vehicles.

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

[19] Cesar Santoyo, Maxence Dutreix, and Samuel Coogan. A barrier function approach to finite-time stochastic system verification and control. *arXiv preprint arXiv:1909.05109*, 2019.

[20] Meenakshi Sarkar, Debasish Ghose, and Evangelos A Theodorou. High-relative degree stochastic control lyapunov and barrier functions. *arXiv preprint arXiv:2004.03856*, 2020.

[21] Mohit Srinivasan, Samuel Coogan, and Magnus Egerstedt. Control of multi-agent systems with finite time control barrier certificates and temporal logic. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 1991–1996. IEEE, 2018.

[22] Wei Xiao, Calin Belta, and Christos G Cassandras. Decentralized merging control in traffic networks: A control barrier function approach. In *Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems*, pages 270–279, 2019.

[23] Xiangru Xu, Paulo Tabuada, Jessy W Grizzle, and Aaron D Ames. Robustness of control barrier functions for safety critical control. *IFAC-PapersOnLine*, 48(27):54–61, 2015.

[24] Shakiba Yaghoubi, Georgios Fainekos, and Sriram Sankaranarayanan. Training neural network controllers using control barrier functions in the presence of disturbances. *2020 IEEE Intelligent Transportation Systems Conference (ITSC)*, 2020.