Safety Assurance System Utilizing Visual Attention for Advanced Driver-Assistance Systems

Haoming Jing (https://orcid.org/0009-0009-9324-2669)
Zhuoyuan Wang (https://orcid.org/0000-0002-1360-6218)
Yorie Nakahira (PI, https://orcid.org/0000-0003-3324-4602)

FINAL RESEARCH REPORT - July 31, 2023

Contract # 69A3551747111

Contents

Chapter 1

Theoretical Foundation

1.1 Introduction

Autonomous systems (*e.g.,* robots and self-driving vehicles) must make safe control decisions in real-time and in the presence of various uncertainties. The control of such safety- and delay-critical systems relies extensively on barrier function-based approaches. Barrier function-based approaches can provide provable safety with low computation cost within deterministic systems that possess small and bounded noise due to the two features stated below [1,2,3]: computation efficiency arising from a myopic controller (feature 1) and from the use of analytical/affine safety conditions (feature 2). However, these two features did not necessarily translate to stochastic systems whose uncertainty is captured by random variables with unbounded support, as we will discuss below. In this chapter, we overcome this difficulty by characterizing a sufficient condition for 'invariance' in the probability space. This condition is then used to guarantee the unsafe probability to below the tolerable levels without the loss of these two features.

Feature 1: Computation efficiency arising from a myopic controller. In a deterministic system, safety can be guaranteed if the state never moves outside the safe set within an infinitesimal outlook time interval. This property allows a myopic controller, which only evaluates the infinitesimal outlook time interval (immediate future time), to keep the system safe at all times. A myopic evaluation requires much less computation than methods that evaluate a long time horizon since the computational load to evaluate possible future trajectories significantly increases with the outlook time horizon.

In a stochastic whose uncertainty has unbounded support, however, the probability of staying within the safe set in the infinitesimal outlook time interval is strictly less than one. In other words, there will always be a non-zero tail probability to move outside of the safe set. This tail probability can accumulate over time and result in a small long-term safe probability. This suggests the need for a more refined *temporal* characterization of long-term safe/unsafe probabilities.

Feature 2: Computation efficiency arising from the use of analytical/affine safety conditions. In a deterministic system, the condition for the state to stay within the safe set in an infinitesimal time can be translated as requiring the vector field of the state stays within the tangent cone of the safe set [4]. A sufficient condition of this requirement is expressed using analytic inequalities that are affine in the control action and thereby can be can be integrated into quadratic programs (see [5] and references therein).

In a stochastic system, however, constraining the mean trajectory to satisfy this condition, without bounding the higher moments, does not give us control over the tail probability of the state moving outside of the safe region. This suggests the need for a more refined *spatial* characterization of unsafe behaviors and state distribution.

Therefore, ensuring safety in a stochastic system needs more refined temporal and spatial characterization of safe/unsafe behaviors during a long outlook time interval. However, the former requires tracing the long-term evolution of complex dynamics, environmental changes, control actions, as well as their couplings. While the latter requires characterization of the state distribution, tails, and conditional value at risk. Both compromise the above two features and can impose a significant computational burden. Such heavy computation can compromises safety due to slower response, despite the use of more optimized actions.

Prior work has yielded diverse approaches for finer time/space characterization in stochastic systems, but all wrestle with this important safety/reaction time tradeoff. We approximately classify these approaches into three main types based on their choice of tradeoffs: long-term safety with heavy computation (approach A); myopic safety with low computation (approach B) ; and long-term conservative safety with low computation (approach C).

1.1.1 Related Work

Approach A: long-term safety with heavy computation. There exists extensive literature that considers a long time horizon and/or the state distribution (or higher moments of the state distribution) at the expense of high computation costs. For example, various model predictive control (MPC) and chance-constrained optimization include safety constraints in a long time horizon (see [6, 7] and references therein). Reachability-based techniques use the characterization of reachable states over a finite/infinite time horizon to constrain the control action so that the state reaches or avoids certain regions [8]. Within barrier function-based approaches, the safety condition can be formulated as constraints on the control action that involve the conditional value-at-risk (CVaR) of the barrier function values [9]. While these techniques can find more optimal control actions that are safe in the long term, they often come with significant computation costs. The cause is twofold: first, possible trajectories often scale exponentially with the length of the outlook time horizon; and second, tails or CVaR involve the probability and mean of rare events, which are more challenging to estimate than nominal events. Such stringent tradeoffs between estimating longer-term safe probability vs. computation burden limit the utility of these techniques in delay-critical systems for more expansive (longer time scale or precise characterization of the state distribution) control action evaluation.

Approach B: myopic safety with low computation. Motivated by the latency requirement in real-time safety-critical control, a few approaches use myopic controllers that constrain the probability of unsafe events in an infinitesimal time interval. For example, the stochastic control barrier function use a sufficient condition for ensuring that the state, on average, moves within the tangent cone of the safe set [10]. The probabilistic barrier certificate ensures certain conditions of the barrier functions to be satisfied with high probability [11, 12]. The myopic nature of these methods achieves a significant reduction in computational cost but can result in unsafe behaviors in a longer time horizon due to the accumulation of tail probabilities of unsafe events.

Approach C: long-term conservative safety with low computation. To have a faster response but still achieve longer-term safety, other approaches use probability and/or martingale inequalities to derive sufficient

conditions for constraining the evolution of barrier function values in a given time interval [3, 13, 14]. These sufficient conditions are given analytically and are elegantly integrated into the convex optimization problems to synthesize controllers offline or verify control actions online. The controllers based on these techniques often require less online computation to find the action that guarantees longer-term safety. However, due to the approximate nature of the probabilistic inequalities, the control actions can be conservative and unnecessarily compromise nominal performance.

1.1.2 Contributions of This Chapter

In this chapter, we propose an efficient algorithm that ensures safety during a fixed or receding time horizon. The algorithm is based on a new safety condition that is sufficient to control the unsafe probability in a given time interval to stay above the tolerable risk levels.[1] This safety condition is constructed by translating probabilistic safety specifications into a forward invariance condition on the level sets of the safe probability. The use of forward invariance allows safety at all time points to be guaranteed by a myopic controller that only evaluates the state evolution in an infinitesimal future time interval. Moreover, the sufficient condition is affine to the control action and can be used in convex/quadratic programs. The parameters of the sufficient condition are determined from the safe probability, its gradient, and its hessian. These values satisfy certain deterministic convection-diffusion equations (CDEs), which characterize the boundary conditions and the relationship between the safe probabilities of neighboring initial conditions and time horizons. These CDEs can be combined with the Monte Carlo (MC) method to improve the accuracy and efficiency in computing these values.

Below, we summarize the advantages of the proposed algorithms.

Advantage 1 Computation efficiency. The proposed method only myopically evaluates the immediate future using closed-form safety constraints. Thus, it can have reduced computational burdens than approach A.

[1] Here, we consider two types of unsafe probability: the probability of exiting the safe set in a time interval when originated inside and the probability of recovering to the safe set when originated outside.

Advantage 2 Provable guarantee in long-term safe probability. The closed-form safety constraints are derived from the safe probability during a receding or fixed time horizon. Thus, the proposed method can have more direct control over the probability of accumulating tail events than approach B.

Advantage 3 Intuitive parameter tuning using exact safety vs. performance tradeoffs. The proposed method uses exact characterizations of safe probability. Thus, it allows the aggressiveness towards safety to be directly tuned based on the exact probability, as opposed to probabilistic bounds or martingale approximations used in approach C. Moreover, our framework may be useful in characterizing the speed and probability of forward convergence in finite-time Lyapunov analysis of stochastic systems.

1.2 Preliminary

Let $\mathbb{R}$, $\mathbb{R}_+$, $\mathbb{R}^n$, and $\mathbb{R}^{m\times n}$ be the set of real numbers, the set of non-negative real numbers, the set of n-dimensional real vectors, and the set of $m \times n$ real matrices, respectively. Let $x[k]$ be the k-th element of vector x. Let $f : \mathcal{X} \to \mathcal{Y}$ represent that f is a mapping from space $\mathcal{X}$ to space $\mathcal{Y}$. Let $\mathbb{1}\{\mathcal{E}\}$ be an indicator function, which takes 1 when condition $\mathcal{E}$ holds and 0 otherwise. Let $\mathbf{0}_{m\times n}$ be an $m \times n$ matrix with all entries 0. Let $\mathbf{1}_n^{[m]}$ be a length n column vector with the m-th entry 1 and other entries 0. Let $\mathbb{I}_m$ be the $m \times m$ identity matrix. Let $\nabla_x f$ be the gradient of a real valued function f with respect to x. Let $\mathbb{H}_x f$ be the hessian of a real valued function f with respect to x. Given events $\mathcal{E}$ and $\mathcal{E}_c$, let $\mathbb{P}(\mathcal{E})$ be the probability of $\mathcal{E}$ and $\mathbb{P}(\mathcal{E}|\mathcal{E}_c)$ be the conditional probability of $\mathcal{E}$ given the occurrence of $\mathcal{E}_c$. Given random variables X and Y, let $\mathbb{E}[X]$ be the expectation of X and $\mathbb{E}[X|Y = y]$ be the conditional expectation of X given $Y = y$. We use upper-case letters (*e.g.,* Y) to denote random variables and lower-case letters (*e.g.,* y) to denote their specific realizations.

Definition 1 (Infinitesimal Generator)**.** The infinitesimal generator A of a stochastic process $\{Y_t \in \mathbb{R}^n\}_{t\in\mathbb{R}_+}$ is

$$AF(y) = \lim_{h\to 0} \frac{\mathbb{E}[F(Y_h)|Y_0 = y] - F(y)}{h} \tag{1.1}$$

whose domain is the set of all functions $F : \mathbb{R}^n \to \mathbb{R}$ such that the limit of (4.11) exists for all $y \in \mathbb{R}^n$.

1.3 Problem Statement

Here, we introduce the control system in subsection 1.3.1, define the measures to characterize two types of safety in subsection 1.3.2, and state the controller design goals in subsection 1.3.3.

1.3.1 System Model

We consider a time-invariant stochastic control and dynamical system. The system dynamics is given by the stochastic differential equation (SDE)

$$dX_t = (f(X_t) + g(X_t)U_t)\,dt + \sigma(X_t)dW_t, \tag{1.2}$$

where $X_t \in \mathbb{R}^n$ is the system state, $U_t \in \mathbb{R}^m$ is the control input, and $W_t \in \mathbb{R}^\omega$ captures the system uncertainties. Here, X_t can include both the controllable states of the system and the uncontrollable environmental variables such as moving obstacles. We assume that W_t is the standard Wiener process with 0 initial value, *i.e.,* $W_0 = 0$. The value of $\sigma(X_t)$ is determined based on the size of uncertainty in unmodeled dynamics and environmental variables.

The control action U_t is determined at each time by the control policy. We assume that accurate information of the system state can be used for control. The control policy is composed of a nominal controller and additional modification scheme to ensure the safety specifications illustrated in subsections 1.3.2 and 1.3.3. The nominal controller is represented by

$$U_t = N(X_t), \tag{1.3}$$

which does not necessarily account for the safety specifications defined below. To adhere to the safety specifications, the output of the nominal controller is then modified by another scheme. The overall control policy involving the nominal controller and the modification scheme is represented by

$$U_t = K_N(X_t, L_t, T_t), \tag{1.4}$$

where $K_N : \mathbb{R}^n \times \mathbb{R} \times \mathbb{R} \to \mathbb{R}^m$ is a deterministic function of the current state X_t, safety margin L_t, and time horizon T_t to the current control action U_t. The policy of the form (1.4) assumes that the decision rule is time-invariant,[2] and that the control action can be uniquely determined for each (X_t, L_t, T_t).

[2] The functions N, K_N do not change over time

This policy is also assumed to be memory-less in the sense that it does not use the past history of the state $\{X_\tau\}_{\tau<t}$ to produce the control action U_t. The assumption for memory-less controller is reasonable because the state evolution dX_t of system (2.2) only depends on the current system state X_t.[3] We restrict ourselves to the settings when f, g, σ, N, and K_N have sufficient regularity conditions such that both the closed loop system of (2.2) and (1.4) have unique strong solutions.[4]

The safe region of the state is specified by the zero super level set of a continuously differentiable barrier function $\phi(x) : \mathbb{R}^n \to \mathbb{R}$, *i.e.,*

$$\mathcal{C}(0) = \{x \in \mathbb{R}^n : \phi(x) \geq 0\}. \tag{1.5}$$

We use

$$\mathcal{C}(L) := \{x \in \mathbb{R}^n : \phi(x) \geq L\} \tag{1.6}$$

to denote the set with safety margin L. Accordingly, we use $\operatorname{int}\mathcal{C}(0) = \{x \in \mathbb{R}^n : \phi(x) > 0\}$ to denote the interior of the safe set, $\mathcal{C}(0)^c = \{x \in \mathbb{R}^n : \phi(x) < 0\}$ to denote the unsafe set, $\partial\mathcal{C}(L) = \{x \in \mathbb{R}^n : \phi(x) = L\}$ to denote the boundary of L super level set.

1.3.2 Probabilistic Characterization of Safe Behaviors

The system must satisfy the following two types of probabilistic safety specifications: forward invariance and forward convergence.

Forward Invariance

The forward invariance property refers to the system's ability to keep its state within a set when the state originated from the set. The probabilistic forward invariance to a set $\mathcal{C}(L)$ can be quantified using

$$\mathbb{P}\left(X_\tau \in \mathcal{C}(L), \forall \tau \in [t, t+T] \mid X_t = x \right) \tag{1.7}$$

for some time interval $[0, T]$ conditioned on an initial condition $x \in \mathcal{C}(L)$. Probability (1.7) can be computed from the distribution of the following two

[3] Note that $f(X_t)$, $g(X_t)$, and $\sigma(X_t)$ are time-invariant functions of the system state.

[4] Conditions required to have a unique strong solution can be found in [15, Chapter 5], [16, Chapter 1], [17, Chapter II.7] and references therein.

random variables:[5]

$$\Phi_x(T) := \inf\{\phi(X_t) \in \mathbb{R} : t \in [0,T], X_0 = x\}, \tag{1.8}$$
$$\Gamma_x(L) := \inf\{t \in \mathbb{R}_+ : \phi(X_t) < L, X_0 = x\}. \tag{1.9}$$

Here, $\Phi_x(T)$ is the worst-case safety margin from the boundary of the safe set $\partial\mathcal{C}(0)$ during $[0,T]$, and $\Gamma_x(L)$ is the time when the system exit from $\mathcal{C}(L)$ for the first time. We can rewrite (1.7) using the two random variables (1.8) and (1.9) as

$$\mathbb{P}\left(X_\tau \in \mathcal{C}(L), \forall \tau \in [t, t+T] \mid X_t = x \right) \tag{1.10}$$
$$= \mathbb{P}\left(X_\tau \in \mathcal{C}(L), \forall \tau \in [0,T] \mid X_0 = x\right) \tag{1.11}$$
$$= \mathbb{P}(\Phi_x(T) \geq L) \tag{1.12}$$
$$= \mathbb{P}(\Gamma_x(L) > T) = 1 - \mathbb{P}(\Gamma_x(L) \leq T). \tag{1.13}$$

Here, equality (1.11) holds due to the time-invariant nature of the system[3] and control policies[2].

Forward Convergence

The forward convergence property indicates the system's capability for its state to enter a set when the state originated from outside the set. This probabilistic forward convergence can be quantified using

$$\mathbb{P}\left(\exists \tau \in [t, t+T] \text{ s.t. } X_\tau \in \mathcal{C}(L) \mid X_t = x \right) \tag{1.14}$$

for some time interval $[0,T]$ conditioned on an initial condition $x \in \mathcal{C}(L)^c$. Similar to the case of forward invariance, probability (1.14) can also be computed from the distribution of the following two random variables:[5]

$$\Theta_x(T) := \sup\{\phi(X_t) \in \mathbb{R} : t \in [0,T], X_0 = x\}, \tag{1.15}$$
$$\Psi_x(L) := \inf\{t \in \mathbb{R}_+ : \phi(X_t) \geq L, X_0 = x\}. \tag{1.16}$$

Here, $\Theta_x(T)$ indicates the distance to the boundary of the safe set $\partial\mathcal{C}(0)$, and $\Psi_x(L)$ is the duration for the state to enter the set $\mathcal{C}(L)$ for the first time.

[5] These random variables are previously introduced and analyzed in [18].

We can also rewrite (1.14) using the two random variables (1.15) and (1.16) as

$$\begin{aligned}
&\mathbb{P}\left(\exists \tau \in [t, t+T] \text{ s.t. } X_\tau \in \mathcal{C}(L) \mid X_t = x\right) && (1.17)\\
&= \mathbb{P}\left(\exists \tau \in [0, T] \text{ s.t. } X_\tau \in \mathcal{C}(L) \mid X_0 = x\right) && (1.18)\\
&= \mathbb{P}(\Theta_x(T) \geq L) && (1.19)\\
&= \mathbb{P}(\Psi_x(L) \leq T). && (1.20)
\end{aligned}$$

1.3.3 Design Goals

In this chapter, we design the control policy with the long-term safety guarantees given in the forms alike (1.7) or (1.14).

When the goal is to guarantee probabilistic forward invariance, we aim to ensure the following condition: for each time $t \in \mathbb{R}_+$,

$$\mathbb{P}\big(X_\tau \in \mathcal{C}(L_t), \forall \tau \in [t, t+T_t]\big) \geq 1 - \epsilon, \tag{1.21}$$

conditioned on the initial condition $X_0 = x$, for some $\epsilon \in (0, 1)$. From now on, all probabilities are conditioned on the initial condition $X_0 = x$ unless otherwise noted. Here, L_t is the desired safety margin, and T_t is the outlook time horizon. For each time t, condition (1.21) constrains the probability of staying within the safe set with margin L_t during the time interval $[t, t+T_t]$ to be above $1-\epsilon$.

When the goal is to guarantee probabilistic forward convergence, we aim to ensure the following condition: for each time $t \in \mathbb{R}_+$,

$$\mathbb{P}\big(\exists \tau \in [t, t+T_t] \text{ s.t. } X_\tau \in \mathcal{C}(L_t)\big) \geq 1 - \epsilon, \tag{1.22}$$

conditioned on the initial condition $X_0 = x$, for some $\epsilon \in (0, 1)$.

In both cases, the value of $\epsilon \in (0, 1)$ is chosen based on risk tolerance. In (1.21) and (1.22), the probabilities are taken over the distribution of X_t and its future trajectories $\{X_\tau\}_{\tau \in (t, t+T_t]}$ conditioned on $X_0 = x$. The distribution of X_t is generated based on the closed-loop system of (2.2) and (1.4), whereas the distribution of $\{X_t\}_{t \in (t, t+T_t]}$ are allowed to be defined in two different ways based on the design choice: the closed-loop system of (2.2) and (1.3) or the closed-loop system of (2.2) and (1.4).

We consider either fixed time horizon or receding time horizon. In the fixed time horizon, safety is evaluated at each time t for a time interval

$[t, t+H]$ of fixed length. In the receding time horizon, we evaluate, at each time t, safety only for the remaining time $[t, H]$ given a fixed horizon. The outlook time horizon for each case is given by

$$T_t = \begin{cases} H, & \text{for fixed time horizon,} \\ H - t, & \text{for receding time horizon.} \end{cases} \tag{1.23}$$

The safety margin is assumed to be either fixed or time varying. Fixed margin refers to when the margin remains constant at all time, *i.e.,* $L_t = \ell$. For time-varying margin, we consider the margin L_t that evolves according to

$$dL_t = f_\ell(L_t),\ L_0 = \ell, \tag{1.24}$$

for some continuously differentiable function f_ℓ.[6] The values of T_t and $\{L_t\}_{t\in[0,\infty)}$ are determined based on the design choice.

1.4 Proposed Method

Here, we present a sufficient condition to achieve the safety requirements in subsection 1.4.1. Based on this condition, we propose two safe control algorithms in subsection 1.4.2 and outline a method to boost algorithm performance in subsection 1.4.3.

Before presenting these results, we first define a few notations. To capture the time-varying nature of T_t and L_t, we augment the state space as

$$Z_t := \begin{bmatrix} T_t \\ L_t \\ \phi(X_t) \\ X_t \end{bmatrix} \in \mathbb{R}^{n+3}. \tag{1.25}$$

The dynamics of Z_t satisfies the following SDE:

$$dZ_t = (\tilde{f}(Z_t) + \tilde{g}(Z_t)U_t)dt + \tilde{\sigma}(Z_t)dW_t. \tag{1.26}$$

[6] This representation also captures fixed margin by setting $f_\ell(L_t) \equiv 0$.

Here, $\tilde{f}$, $\tilde{g}$, and $\tilde{\sigma}$ are defined to be

$$\tilde{f}(Z_t) := \begin{bmatrix} f_T \\ f_\ell(L_t) \\ f_\phi(X_t) \\ f(X_t) \end{bmatrix} \in \mathbb{R}^{(n+3)}, \tag{1.27}$$

$$\tilde{g}(Z_t) := \begin{bmatrix} \mathbf{0}_{2\times n} \\ \mathcal{L}_g\phi(X_t) \\ g(X_t) \end{bmatrix} \in \mathbb{R}^{(n+3)\times m}, \tag{1.28}$$

$$\tilde{\sigma}(Z_t) := \begin{bmatrix} \mathbf{0}_{2\times n} \\ \mathcal{L}_\sigma\phi(X_t) \\ \sigma(X_t) \end{bmatrix} \in \mathbb{R}^{(n+3)\times \omega}. \tag{1.29}$$

In (1.27), the scalar f_T is given by

$$f_T := \begin{cases} 0, & \text{in fixed time horizon,} \\ -1, & \text{in receding time horizon,} \end{cases} \tag{1.30}$$

the function f_ℓ is given by (1.24), and the function f_ϕ is given by

$$f_\phi(X_t) := \mathcal{L}_f\phi(X_t) + \frac{1}{2}\mathrm{tr}\big([\sigma(X_t)]\, [\sigma(X_t)]^\intercal \,\mathrm{Hess}\,\phi(X_t)\big). \tag{1.31}$$

Remark 1. The Lie derivative of a function $\phi(x)$ along the vector field $f(x)$ is denoted as $\mathcal{L}_f\phi(x) = f(x)\cdot\nabla\phi(x)$. The Lie derivative $(\mathcal{L}_g\phi(x))$ along a matrix field $g(x)$ is interpreted as a row vector such that $(\mathcal{L}_g\phi(x))\, u = (g(x)u)\cdot\nabla\phi(x)$.

1.4.1 Conditions to Assure Safety

We consider one of the following four types of probabilistic quantities:[7]

$$\mathbf{F}(Z_t) := \begin{cases} \mathbb{P}\left(\Phi_{X_t}(T_t) \geq L_t\right) & \text{for type I,} \\ \mathbb{P}\left(\Gamma_{X_t}(L_t) > T_t\right) & \text{for type II,} \\ \mathbb{P}\left(\Theta_{X_t}(T_t) \geq L_t\right) & \text{for type III,} \\ \mathbb{P}\left(\Psi_{X_t}(L_t) \leq T_t\right) & \text{for type IV,} \end{cases} \tag{1.32}$$

[7]Recall from Section 1.3.3 that whenever we take the probabilities (and expectations) over paths, we assume that the probabilities are conditioned on the initial condition $X_0 = x$.

where the probability is taken over the same distributions of $\{X_\tau\}_{\tau\in[t,T_t]}$ that are used in the safety requirement (1.21) and (1.22). The values of T_t and L_t (known and deterministic) are defined in (1.23) and (1.24) depending on the design choice of receding/fixed time-horizon and fixed/varying margin.

Additionally, we define the mapping $D_{\mathbf{F}} : \mathbb{R}^{n+3} \times \mathbb{R}^m \to \mathbb{R}$ as[8]

$$\begin{aligned} D_{\mathbf{F}}(Z_t, U_t) := \mathcal{L}_{\tilde{f}}\mathbf{F}(Z_t) + (\mathcal{L}_{\tilde{g}}\mathbf{F}(Z_t))\, U_t \\ + \frac{1}{2}\mathrm{tr}\left([\tilde{\sigma}(Z_t)]\,[\tilde{\sigma}(Z_t)]^\intercal \,\mathrm{Hess}\,\mathbf{F}(Z_t)\right). \end{aligned} \tag{1.33}$$

From Itô's Lemma,[9] the mapping (1.33) essentially evaluates the value of the infinitesimal generator of the stochastic process Z_t acting on $\mathbf{F}$: *i.e.,* $A\mathbf{F}(Z_t) = D_{\mathbf{F}}(z, u)$ when the control action $U_t = u$ is used when $Z_t = z$.

We propose to constrain the control action U_t to satisfy the following condition at all time t:

$$D_{\mathbf{F}}(Z_t, U_t) \geq -\alpha\left(\mathbf{F}(Z_t) - (1-\epsilon)\right). \tag{1.34}$$

Here, $\alpha : \mathbb{R} \to \mathbb{R}$ is assumed to be a monotonically-increasing, concave or linear function that satisfies $\alpha(0) \leq 0$. From (1.33), condition (2.10) is affine in U_t. This property allows us to integrate condition (2.10) into a convex/quadratic program.

Theorem 1. *Consider the closed-loop system of* (2.2) *and* (1.4).[10] *Assume that* $\mathbf{F}(z)$ *in* (1.32) *is a continuously differentiable function of* $z \in \mathbb{R}^{n+3}$ *and* $\mathbb{E}[\mathbf{F}(Z_t)]$ *is differentiable in* t. *If system* (2.2) *originates at* $X_0 = x$ *with* $\mathbf{F}(z) > 1 - \epsilon$, *and the control action satisfies* (2.10) *at all time, then the following condition holds:*[11]

$$\mathbb{E}\left[\mathbf{F}(Z_t)\right] \geq 1 - \epsilon \tag{1.35}$$

for all time $t \in \mathbb{R}_+$.

[8] See Remark 1 for the notation for Lie derivative.

[9] Itô's Lemma is stated as below: Given a n-dimensional real valued diffusion process $dX = \mu dt + \sigma dW$ and any twice differentiable scalar function $f : \mathbb{R}^n \to \mathbb{R}$, one has $df = \left(\mathcal{L}_\mu f + \frac{1}{2}\,\mathrm{tr}\,(\sigma\sigma^\intercal\,\mathrm{Hess}\,f)\right)dt + \mathcal{L}_\mu \sigma dW$.

[10] Recall from subsection 1.3.1 that f, g, σ, N, and K_N are assumed to have sufficient regularity conditions.

[11] Here, the expectation is taken over X_t conditioned on $X_0 = x$, and $\mathbf{F}$ in (1.32) gives the probability of forward invariance/convergence of the future trajectories $\{X_\tau\}_{(t,t+T_t]}$ starting at X_t.

Proof (theorem 1). First, we show that

$$\mathbb{E}[\mathbf{F}(Z_\tau)] \leq 1 - \epsilon \tag{1.36}$$

implies

$$\mathbb{E}\left[\alpha\left(\mathbf{F}(Z_\tau) - (1-\epsilon)\right)\right] \leq 0. \tag{1.37}$$

Let τ is the time when (1.36) holds. We first define the events D_i and a few variables $v_i, q_i,$ and δ_i, $i \in \{0, 1\}$, as follows:

$$D_0 = \left\{\mathbf{F}(Z_\tau) < 1 - \epsilon\right\}, \tag{1.38}$$
$$D_1 = \left\{\mathbf{F}(Z_\tau) \geq 1 - \epsilon\right\}, \tag{1.39}$$
$$v_0 = \mathbb{E}\left[\mathbf{F}(Z_\tau) \mid D_0\right] = 1 - \epsilon - \delta_0, \tag{1.40}$$
$$v_1 = \mathbb{E}\left[\mathbf{F}(Z_\tau) \mid D_1\right] = 1 - \epsilon + \delta_1, \tag{1.41}$$
$$q_0 = \mathbb{P}(D_0), \tag{1.42}$$
$$q_1 = \mathbb{P}(D_1). \tag{1.43}$$

The left hand side of (1.36) can then be written as

$$\begin{aligned}\mathbb{E}[\mathbf{F}(Z_\tau)] &= \mathbb{E}\left[\mathbf{F}(Z_\tau) \mid D_0\right]\mathbb{P}(D_0) + \mathbb{E}\left[\mathbf{F}(Z_\tau) \mid D_1\right]\mathbb{P}(D_1) \\ &= v_0 q_0 + v_1 q_1. \end{aligned} \tag{1.44}$$

From

$$\begin{aligned}\mathbb{E}\left[\mathbf{F}(Z_\tau) \mid D_0\right] &< 1 - \epsilon, \\ \mathbb{E}\left[\mathbf{F}(Z_\tau) \mid D_1\right] &\geq 1 - \epsilon,\end{aligned} \tag{1.45}$$

we obtain

$$\delta_0 \geq 0 \quad \text{and} \quad \delta_1 \geq 0. \tag{1.46}$$

Moreover, $\{q_i\}_{i\in\{0,1\}}$ satisfies

$$\mathbb{P}(D_0) + \mathbb{P}(D_1) = q_0 + q_1 = 1. \tag{1.47}$$

Combining (1.36) and section 3.3.3 gives

$$v_0 q_0 + v_1 q_1 \leq 1 - \epsilon. \tag{1.48}$$

Applying (3.56) and (3.57) to (3.65) gives

$$(1-\epsilon-\delta_0)\,q_0+(1-\epsilon+\delta_1)\,q_1\le 1-\epsilon, \tag{1.49}$$

which, combined with (3.64), yields

$$\delta_1 q_1-\delta_0 q_0\le 0. \tag{1.50}$$

On the other hand, we have

$$\begin{aligned}
&\mathbb{E}\left[\alpha\left(\mathbf{F}(Z_\tau)-(1-\epsilon)\right)\right]\\
&\quad=\ \mathbb{P}(D_0)\left(\mathbb{E}\left[\alpha\left(\mathbf{F}(Z_\tau)-(1-\epsilon)\right)\mid D_0\right]\right)\\
&\qquad+\mathbb{P}(D_1)\left(\mathbb{E}\left[\alpha\left(\mathbf{F}(Z_\tau)-(1-\epsilon)\right)\mid D_1\right]\right) &(1.51)\\
&\quad=\ q_0\left(\mathbb{E}\left[\alpha\left(\mathbf{F}(Z_\tau)-(1-\epsilon)\right)\mid D_0\right]\right)\\
&\qquad+q_1\left(\mathbb{E}\left[\alpha\left(\mathbf{F}(Z_\tau)-(1-\epsilon)\right)\mid D_1\right]\right) &(1.52)\\
&\quad\le\ q_0\left(\alpha\left(\mathbb{E}\left[\mathbf{F}(Z_\tau)-(1-\epsilon)\mid D_0\right]\right)\right)\\
&\qquad+q_1\left(\alpha\left(\mathbb{E}\left[\mathbf{F}(Z_\tau)-(1-\epsilon)\mid D_1\right]\right)\right) &(1.53)\\
&\quad=\ q_0\left(\alpha\left(-\delta_0\right)\right)+q_1\left(\alpha\left(\delta_1\right)\right) &(1.54)\\
&\quad\le\ \alpha\left(-q_0\delta_0+q_1\delta_1\right) &(1.55)\\
&\quad\le\ 0. &(1.56)
\end{aligned}$$

Here, section 3.3.3 is due to (3.58) and (3.59); section 3.3.3 is obtained from Jensen's inequality [19] for concave function α; section 3.3.3 is based on (3.56) and (3.57); section 3.3.3 is given by assumption A2; and section 3.3.3 is due to (3.67). Thus, we showed that (1.36) implies (1.37).

Using Dynkin's formula, given a time-invariant control policy, the sequence $\mathbb{E}[\mathbf{F}(Z_t)]$ takes deterministic value over time where the dynamics is given by

$$\frac{d}{d\tau}\mathbb{E}[\mathbf{F}(Z_\tau)]=\mathbb{E}[A\mathbf{F}(Z_\tau)]. \tag{1.57}$$

Condition (2.10) implies

$$\mathbb{E}[A\mathbf{F}(Z_\tau)]\ge-\mathbb{E}\left[\alpha\left(\mathbf{F}(Z_\tau)-(1-\epsilon)\right)\right]. \tag{1.58}$$

Therefore, we have

$$\frac{d}{d\tau}\mathbb{E}[\mathbf{F}(Z_\tau)]\ge 0\quad\text{whenever }\mathbb{E}[\mathbf{F}(Z_\tau)]\le 1-\epsilon. \tag{1.59}$$

This condition implies

$$\mathbb{E}[\mathbf{F}(Z_t)] \geq 1 - \epsilon \quad \text{for all } t \in \mathbb{R}_+. \tag{1.60}$$

due to lemma 1, which is given below. ■

Lemma 1. *Let $y\colon \mathbb{R}_+ \to \mathbb{R}$ be a real-valued differentiable function that satisfies*

$$\frac{d}{dt} y_t \geq 0 \quad \textit{whenever } y_t \leq L. \tag{1.61}$$

Additionally, we assume $y_0 > L$. Then

$$y_t \geq L \quad \textit{for all } t \in \mathbb{R}_+. \tag{1.62}$$

Proof. Suppose there exists $b \in \mathbb{R}_+$ such that $y_b < L$. By the intermediate value theorem, there exists $a \in (0, b)$ such that $y_a = L$, and $y_t < L$ for all $t \in (a, b]$. Next, by the mean value theorem, there exists $\tau \in (a, b)$ such that $(dy_t/dt)|_{t=\tau} = (y_b - y_a)/(b - a) < 0$. This contradicts condition (1.61). ■

Corollary 1. *Consider the closed-loop system of* (2.2) *and* (1.4) *with the assumptions stated in theorem 1. Let* $\mathbf{F}$ *be defined as type I or II in* (1.32)*. If the system state originates at $X_0 = x$ with $\mathbf{F}(z) > 1 - \epsilon$, and the control action satisfies* (2.10) *at all time $t \in \mathbb{R}_+$, then condition* (1.21) *holds.*

Proof (corollary 1). From (1.11), (1.32), and theorem 1, we have

$$\begin{aligned} &\mathbb{P}\left(X_\tau \in \mathcal{C}(L_t), \forall \tau \in [t, t + T_t]\right) \\ &= \mathbb{E}\left[\mathbf{F}(Z_\tau)\right] \\ &\geq 1 - \epsilon, \end{aligned}$$

which yields (1.21). ■

Corollary 2. *Consider the closed-loop system of* (2.2) *and* (1.4) *with the assumptions stated in theorem 1. Let* $\mathbf{F}$ *be defined as type III or IV in* (1.32)*. If the system state originates at $X_0 = x$ with $\mathbf{F}(z) > 1 - \epsilon$, and the control action satisfies* (2.10) *at all time $t \in \mathbb{R}_+$, then condition* (1.22) *holds.*

Proof (corollary 2). From (1.17) and (1.32), we have

$$\begin{aligned} &\mathbb{P}\left(\exists \tau \in [t, t + T_t] \text{ s.t. } X_\tau \in \mathcal{C}(L_t)\right) \\ &= \mathbb{E}\left[\mathbf{F}(Z_\tau)\right] \\ &\geq 1 - \epsilon, \end{aligned}$$

which yields (1.22). ■

1.4.2 Safe Control Algorithms

Here, we propose two safe control algorithms based on the safety conditions introduced in subsection 1.4.1. In both algorithms, the value of $\mathbf{F}$ is defined as type I or II in (1.32) when the safety specification is given as forward invariance condition, and as type III or IV when the safety specification is given as forward convergence condition.

Additive modification

We propose a control policy of the form

$$K_N(X_t, L_t, T_t) = N(X_t) + \kappa(Z_t)(\mathcal{L}_{\tilde{g}}\mathbf{F}(Z_t))^\intercal. \tag{1.63}$$

Here, N is the nominal control policy defined in (1.3).

The mapping $\kappa : \mathbb{R}^{n+3} \to \mathbb{R}_+$ is chosen to be a non-negative function that are designed to satisfy the assumptions of theorem 1 and makes $U_t = K_N(X_t, L_t, T_t)$ to satisfy (2.10) at all time. Then, the control action $U_t = K_N(X_t, L_t, T_t)$ yields

$$\begin{aligned} &\mathbb{E}[d\mathbf{F}(Z_t)] = A\mathbf{F}(Z_t) \\ &= \mathcal{L}_{\tilde{f}}\mathbf{F} + (\mathcal{L}_{\tilde{g}}\mathbf{F})N + \kappa\mathcal{L}_{\tilde{g}}\mathbf{F}\,(\mathcal{L}_{\tilde{g}}\mathbf{F})^\intercal + \frac{1}{2}\mathrm{tr}\left(\tilde{\sigma}\tilde{\sigma}^\intercal \,\mathrm{Hess}\,\mathbf{F}\right). \end{aligned} \tag{1.64}$$

As κ is non-negative, the term $\kappa\mathcal{L}_{\tilde{g}}\mathbf{F}\,(\mathcal{L}_{\tilde{g}}\mathbf{F})^\intercal$ in (1.64) takes non-negative values. This implies that the second term additively modify the nominal controller output $N(X_t)$ in the ascending direction of the forward invariance probability (1.21) or forward convergence probability (1.22).

Constrained optimization

We propose a control policy of the form

$$\begin{aligned} K_N(X_t, L_t, T_t) = \quad &\arg\min_{u} \quad J(N(X_t), u) \\ &\text{s.t.} \quad (2.10), \end{aligned} \tag{1.65}$$

Here, $J : \mathbb{R}^m \times \mathbb{R}^m \to \mathbb{R}$ is an objective function that penalizes the deviation from the desired performance, the nominal control action, and/or the costs. It is also designed to satisfy the assumptions of theorem 1 to comply with the safety specification (1.21) or (1.22). The constraint of (1.65) imposes

that (2.10) holds at all time t, and can additionally capture other design restrictions.[12] When $(\mathcal{L}_{\tilde{g}}\mathbf{F}(z)) \neq 0$ for any z, there always exists u that satisfy the constraint (2.10).

Both additive modification and conditioning structures are commonly used in the safe control of deterministic systems (see [20, subsection II-B] and references therein). These existing methods are designed to find control actions so that the vector field of the state does not point outside of the safe set around its boundary. In other words, the value of the barrier function will be non-decreasing in the infinitesimal future outlook time horizon whenever the state is close to the boundary of the safe set. However, such myopic decision-making may not account for the fact that different directions of the tangent cone of the safe set may lead to vastly different long-term safety. In contrast, the proposed control policies (1.63) and (1.65) account for the long-term safe probability in $\mathbf{F}$, and are guaranteed to steer the state toward the direction with non-decreasing long-term safe probability when the tolerable long-term unsafe probability is about to be violated. When $\mathbf{F}$ is defined based on the closed-loop system involving (2.2) and (1.3), its value can be computed offline. In such cases, the controller only needs to myopically evaluate the addition (1.63) or closed-form inequality conditions (1.65) in real time execution. In both cases, the computation efficiency is comparable to common myopic barrier function-based methods in a deterministic system.

1.4.3 Improving the Accuracy of Gradient Estimation

The safety condition (2.10) requires us to evaluate $\mathbf{F}$, $\partial\mathbf{F}/\partial z$, and $\operatorname{Hess}\mathbf{F}$. These values can be estimated by applying Monte-Carlo methods on finite difference approximation formulas. However, for some systems and parameter ranges, naive sampling can produce noisy estimate of the probabilities and their gradients [18]. At a high spatial frequency, the randomness due to sampling can have a relatively larger impacts than the infinitesimal changes in the initial state.

Such drawback in naive sampling can be complemented using additional information about the conditions that must be satisfied by the probabilities and their gradients. Here, we derive the safe/recovery probabilities as the solution to certain convection diffusion equations. The solution of the

[12] For example, K_N is Lipschitz continuous when $J(N(x), u) = u^\intercal H(x)u$ with $H(x)$ being a positive definite matrix (pointwise in x).

convection diffusion equations are guaranteed to be smooth and satisfy the neighbor relations of probabilities (see [21, Section 7.1] and reference therein for the regularity of convection diffusion). Such characterization allows the well-established numerical analysis techniques to be used to improve the accuracy of these estimates [22].

Below, we present the convection diffusion equations. To emphasize the qualitatively different roles of T_t and $(L_t, \phi(X_t), X_t)$, we introduce another state variable

$$Y_t := \begin{bmatrix} L_t \\ \phi(X_t) \\ X_t \end{bmatrix} \in \mathbb{R}^{n+2}. \tag{1.66}$$

Theorem 2. *Let $S = \tilde{\sigma}\tilde{\sigma}^\intercal$. Let $\rho = \tilde{f} + \tilde{g}N$ if $\mathbf{F}$ in (1.32) is defined for the closed-loop system of (2.2) and (1.3), and $\rho = \tilde{f} + \tilde{g}K_N$ if $\mathbf{F}$ is defined for the closed-loop system of (2.2) and (1.4). The variable $\tilde{\mathbf{F}}(Y_t, T_t) := \mathbf{F}(Z_t)$ for types I-IV satisfies the following convection diffusion equation [18, Theorems 1–4]:*

$$\frac{\partial \tilde{\mathbf{F}}}{\partial T} = \frac{1}{2}\nabla\cdot(S\nabla\tilde{\mathbf{F}}) + \mathcal{L}_{\rho - \frac{1}{2}\nabla\cdot S}\tilde{\mathbf{F}},\ y[2] \geq y[1], T > 0. \tag{1.67}$$

For types I and II, the boundary condition satisfies

$$\begin{cases} \tilde{\mathbf{F}}(y, T) = 0, & y[2] < y[1], T > 0, \\ \tilde{\mathbf{F}}(y, 0) = \mathbb{1}\{y[2] \geq y[1]\}(y), & y \in \mathbb{R}^{n+2}. \end{cases} \tag{1.68}$$

For types III and IV, the boundary condition satisfies

$$\begin{cases} \tilde{\mathbf{F}}(y, T) = 1, & y[2] < y[1], T > 0, \\ \tilde{\mathbf{F}}(y, 0) = \mathbb{1}\{y[2] \geq y[1]\}(y), & y \in \mathbb{R}^{n+2}. \end{cases} \tag{1.69}$$

The methods to compute the values of $\mathbf{F}$, $\partial\mathbf{F}/\partial z$, and $\operatorname{Hess}\mathbf{F}$ are thorough and diverse. The characterization from Theorem 2 can be exploited for improve the computation accuracy and efficiency. Examples of such techniques (non-mutually exclusive) are:

- Directly run Monte Carlo for neighboring states and approximate the gradient using finite difference methods.

- Evaluate the values of a boundary, and diffusing the boundary values to the interior/remaining areas. The boundary can be defined by the boundary condition given in (1.68) or (1.69). It can also be certain areas in (1.67), whose values can be evaluated using the MC method.

- Use the relation in (1.67) to derive the subspace that must be satisfied by $\mathbf{F}(z)$ and its neighbors $\mathbf{F}(z + \Delta z)$. This relation can be used to smooth out the results from the MC method: *e.g.,* the obtained probability can be projected onto the lower-dimensional subspace defined by (1.67).

- Use condition (1.67) to further derive the conditions that must be satisfied by $\partial\mathbf{F}/\partial z$ and $\operatorname{Hess}\mathbf{F}$.

A review on the available methods and their tradeoffs is beyond the scope of this chapter. The proposed approach do not constrain the computation of $\mathbf{F}$, $\partial\mathbf{F}/\partial z$, and $\operatorname{Hess}\mathbf{F}$ to be limited to any specific methods.

1.5 Deployment and Experiment

In this section, we show the efficacy of our proposed method in an example use case.

1.5.1 Algorithms for Comparison

We compare our proposed controller with three existing safe controllers designed for stochastic systems. Below, we present their simplified versions.

- Proposed controller: The safety condition is given by

$$D_{\mathbf{F}}(Z_t, U_t) \geq -\alpha(\mathbf{F}(Z_t) - (1 - \epsilon)), \tag{1.70}$$

  where $\alpha > 0$ is a constant. We choose type I in (1.32) with fixed time horizon and time-invariant zero margin, *i.e.,* $\mathbb{P}\left(\Phi_{X_t}(H) \geq 0\right)$.

- Stochastic control barrier functions (StoCBF) [10]: The safety condition is given by

$$D_{\phi}(X_t, U_t) \geq -\eta\phi(X_t), \tag{1.71}$$

where $\eta > 0$ is a constant. Here, the mapping $D_\phi : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ is defined as the infinitesimal generator of the stochastic process X_t acting on the barrier function ϕ, *i.e.,*

$$\begin{aligned} D_\phi(X_t, U_t) :=& A\phi(X_t) \\ =& \mathcal{L}_f\phi(X_t) + \mathcal{L}_g\phi(X_t)U_t \\ &+ \frac{1}{2}\mathrm{tr}\left(\left[\sigma(X_t)\right]\left[\sigma(X_t)\right]^\intercal \mathrm{Hess}\,\phi(X_t)\right). \end{aligned} \tag{1.72}$$

This condition constrains the average system state to move within the tangent cone of the safe set.

- Probabilistic safety barrier certificates (PrSBC) [11]: The safety condition is given by

$$\mathbf{P}\left(D_\phi(X_t, U_t) + \eta\phi(X_t) \geq 0\right) \geq 1 - \epsilon, \tag{1.73}$$

where $\eta > 0$ is a constant. This condition constrains the state to stay within the safe set in the infinitesimal future interval with high probability.

- Conditional-value-at-risk barrier functions (CVaR) [9]: The safety condition is given by

$$\mathrm{CVaR}_\beta\left(\phi(X_{t_{k+1}})\right) \geq \gamma\phi(X_{t_k}) \tag{1.74}$$

where $\gamma \in (0, 1)$ is a constant, $\{t_0 = 0, t_1, t_2, \cdots\}$ is a discrete sampled time of equal sampling intervals. This is a sufficient condition to ensure the value of $\mathrm{CVaR}^k_\beta(\phi(X_{t_k}))$ conditioned on $X_0 = x$ to be non-negative at all sampled time $t_{k\in\mathbb{Z}_+}$. The value of $\mathrm{CVaR}^k_\beta(\phi(X_{t_k}))$ quantifies the evaluation made at time $t_0 = 0$ about the safety at time t_k.

1.5.2 Settings

We consider the control affine system (2.2) with $f(X_t) \equiv A = 2$, $g(X_t) \equiv 1$, $\sigma(X_t) \equiv 2$. The safe set is defined as

$$\mathcal{C}(0) = \left\{x \in \mathbb{R}^n : \phi(x) \geq 0\right\}, \tag{1.75}$$

with the barrier function $\phi(x) := x - 1$. The safety specification is given as the forward invariance condition. The nominal controller is a proportional controller $N(X_t) = -KX_t$ with $K = 2.5$. The closed-loop system with this controller has an equilibrium at $x = 0$ and tends to move into the unsafe set in the state space. We consider the following two settings:

Table 1.1: parameters used in simulation

Controller	Parameters
Proposed controller	$\alpha = 1$, $\epsilon = 0.1$, $H = 10$
StoCBF	$\eta = 1$
PrSBC	$\eta = 1$, $\epsilon = 0.1$
CVaR	$\gamma = 0.65$, $\beta = 0.1$

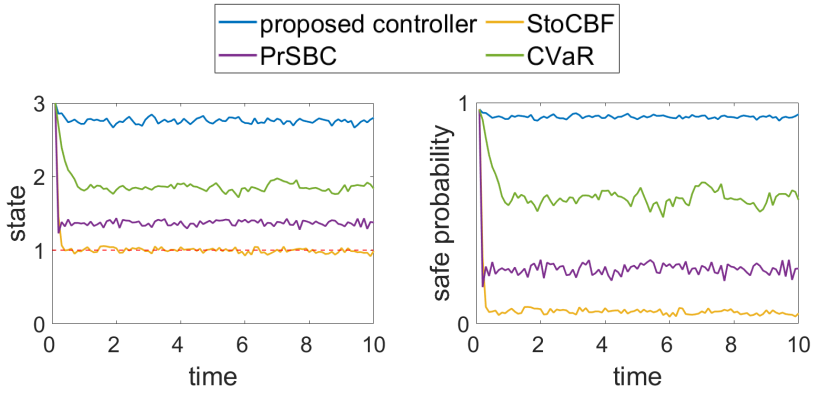
- **Worst-case safe control:** We use the controller that satisfies the safety condition with equality at all time to test the safety enforcement power of these safety constraint. Such control actions are the riskiest actions that are allowed by the safety condition. The use of such control actions allows us to evaluate the safety conditions separated from the impact of the nominal controllers. Here we want to see whether our proposed controller can achieve non-decreasing expected safety as intended.
- **Switching control:** We impose safe controller only when the nominal controller does not satisfy the safety constraint. Here we want to see how the proposed controller performs in practical use, where typically there is a control goal that is conflicting with safety requirements.

We run simulations with $dt = 0.1$ for all controllers. The initial state is set to $x_0 = 3$. For our controller, each Monte Carlo approximation uses 10000 sampled trajectories. The parameters used are listed in Table 1.1. Since the parameter α in the proposed controller has a similar effect as η in StoCBF and PrSBC, we use the same values for these parameters in those controllers. The parameter ϵ is the tolerable probability of unsafe events both in the proposed controller and PrSBC, so we use the same values of ϵ for both algorithms for a fair comparison.

1.5.3 Results

Fig. 1.1 shows the results in the worst-case setting. The proposed controller can keep the expected safe probability $\mathbb{E}[\mathbf{F}(X_t)]$ close to 0.9 all the time, while others fail to keep it at a high level with used parameters. A major cause of failure is due to the accumulation of rare event probability, leading to unsafe

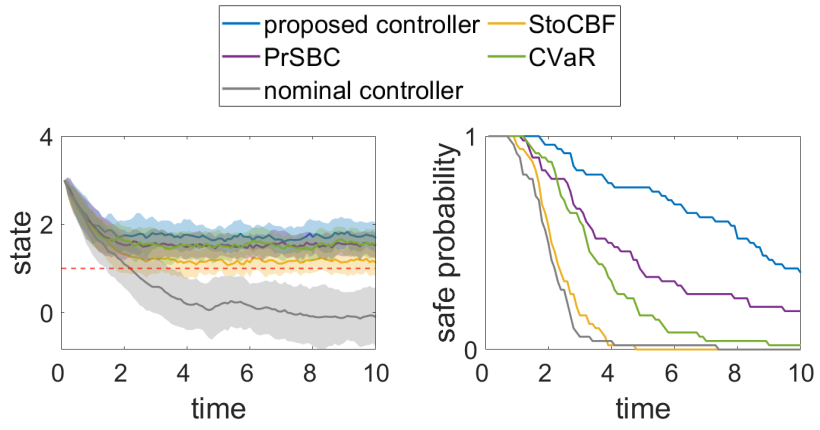
behaviors. This shows the power of having a provable performance for non-decreasing long-term safe probability over time. For comparable parameters, the safety improves from StoCBF to PrSBC to CVaR. This is also expected as constraining the expectation has little control of higher moments, and constraining the tail is not as strong as constraining the tail and the mean values of the tail.



(a) average state (b) expected safe probability

Figure 1.1: Results in the worst-case setting where **(a)** shows the average system state over 50 trajectories and **(b)** shows the expected safe probability (1.21).

Fig. 1.2 shows the results in the switching control setting. We obtained the empirical safe probability by calculating the number of safe trajectories over the total trials. In this setting, the proposed controller can keep the state within the safe region with the highest probability compared to other methods, even when there is a nominal control that acts against safety criteria. This is because the proposed controller directly manipulates dynamically evolving state distributions to guarantee non-decreasing safe probability when the tolerable unsafe probability is about to be violated, as opposed to when the state is close to an unsafe region. Our novel use of forward invariance condition on the safe probability allows a myopic controller to achieve long-term safe probability, which cannot be guaranteed by any myopic controller that directly imposes forward invariance on the safe set.



(a) average state (b) empirical safe probability

Figure 1.2: Results in the switching control setting where **(a)** shows the averaged system state of 50 trajectories with its standard deviation and **(b)** shows the empirical safe probability.

1.6 Summary

In this chapter, we considered the problem of ensuring long-term safety with high probability in stochastic systems. We proposed a sufficient condition to control the long-term safe probability of forward invariance (staying within the safe region) and forward convergence (recovering to the safe region). We then integrated the proposed sufficient condition into a myopic controller which is computationally efficient. We additionally outline possible techniques to improve the computation accuracy and efficiency in evaluating the sufficient condition. Finally, we evaluated the performance of our proposed controller in a numerical example. Although beyond the scope of this chapter, the proposed framework can also be used to characterize the speed and probability of system convergence and may be useful in finite-time Lyapunov analysis in stochastic systems.

Bibliography

[1] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *European control conference*. IEEE, 2019, pp. 3420–3431.

[2] O. Khatib, "Real-time obstacle avoidance for manipulators and mobile robots," in *Autonomous robot vehicles*. Springer, 1986, pp. 396–404.

[3] 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*, vol. 52, no. 8, pp. 1415–1428, 2007.

[4] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, nov 1999. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0005109899001132

[5] 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.

[6] M. Farina, L. Giulioni, and R. Scattolini, "Stochastic linear Model Predictive Control with chance constraints – A review," *Journal of Process Control*, vol. 44, pp. 53–67, aug 2016. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0959152416300130

[7] L. Hewing, K. P. Wabersich, M. Menner, and M. N. Zeilinger, "Learning-Based Model Predictive Control: Toward Safe Learning in Control," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 3, no. 1, pp. 269–296, may 2020. [Online]. Available: https://www.annualreviews.org/doi/10.1146/annurev-control-090419-075625

[8] M. Chen and C. J. Tomlin, "Hamilton–Jacobi Reachability: Some Recent Theoretical Advances and Applications in Unmanned Airspace Management," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, no. 1, pp. 333–358, may 2018. [Online]. Available: https://www.annualreviews.org/doi/10.1146/annurev-control-060117-104941

[9] M. Ahmadi, X. Xiong, and A. D. Ames, "Risk-sensitive path planning via cvar barrier functions: Application to bipedal locomotion," *arXiv preprint arXiv:2011.01578*, 2020.

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

[11] W. Luo, W. Sun, and A. Kapoor, "Multi-robot collision avoidance under uncertainty with probabilistic safety barrier certificates," *arXiv preprint arXiv:1912.09957*, 2019.

[12] Y. Lyu, W. Luo, and J. M. Dolan, "Probabilistic safety-assured adaptive merging control for autonomous vehicles," in *2021 IEEE International Conference on Robotics and Automation (ICRA)*, 2021, pp. 10 764–10 770.

[13] S. Yaghoubi, K. Majd, G. Fainekos, T. Yamaguchi, D. Prokhorov, and B. Hoxha, "Risk-bounded control using stochastic barrier functions," *IEEE Control Systems Letters*, 2020.

[14] C. Santoyo, M. Dutreix, and S. Coogan, "A barrier function approach to finite-time stochastic system verification and control," *Automatica*, p. 109439, 2021.

[15] G. P. Moustris, S. C. Hiridis, K. M. Deliparaschos, and K. M. Konstantinidis, "Evolution of autonomous and semi-autonomous robotic surgical systems: a review of the literature," *The international journal of medical robotics and computer assisted surgery*, vol. 7, no. 4, pp. 375–392, 2011.

[16] B. Øksendal, *Stochastic Differential Equations: An Introduction with Applications*, 6th ed., ser. Universitext. Berlin Heidelberg: Springer-Verlag, 2003.

[17] A. N. Borodin, *Stochastic processes*. Springer, 2017.

[18] A. Chern, X. Wang, A. Iyer, and Y. Nakahira, "Safe control in the presence of stochastic uncertainties," *Accepted to 2021 60th Conference on Decision and Control*, 2021.

[19] J. L. W. V. Jensen, "Sur les fonctions convexes et les inégalités entre les valeurs moyennes," *Acta Mathematica*, vol. 30, pp. 175–193, 1906. [Online]. Available: http://projecteuclid.org/euclid.acta/1485887155

[20] A. Chern, X. Wang, A. Iyer, and Y. Nakahira, "Safe control in the presence of stochastic uncertainties," *arXiv preprint arXiv:2104.01259*, 2021.

[21] L. C. Evans, "Partial differential equations and monge-kantorovich mass transfer," *Current developments in mathematics*, vol. 1997, no. 1, pp. 65–126, 1997.

[22] R. J. LeVeque *et al.*, *Finite volume methods for hyperbolic problems*. Cambridge university press, 2002, vol. 31.

[23] Q. Lu, A. Sorniotti, P. Gruber, J. Theunissen, and J. De Smet, "H loop shaping for the torque-vectoring control of electric vehicles: Theoretical design and experimental assessment," *Mechatronics*, vol. 35, pp. 32–43, 2016.

[24] H.-S. TAN and Y.-K. CHIN, "Vehicle antilock braking and traction control: a theoretical study," *International journal of systems science*, vol. 23, no. 3, pp. 351–365, 1992.

[25] L. Zhang, H. Ding, J. Shi, Y. Huang, H. Chen, K. Guo, and Q. Li, "An adaptive backstepping sliding mode controller to improve vehicle maneuverability and stability via torque vectoring control," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 2598–2612, 2020.

[26] M. Bauer and M. Tomizuka, "Fuzzy logic traction controllers and their effect on longitudinal vehicle platoon systems," *Vehicle system dynamics*, vol. 25, no. 4, pp. 277–303, 1996.

[27] A. Parra, A. Zubizarreta, J. Pérez, and M. Dendaluce, "Intelligent torque vectoring approach for electric vehicles with per-wheel motors," *Complexity*, vol. 2018, 2018.

[28] X. Wu, C. Ma, M. Xu, Q. Zhao, and Z. Cai, "Single-parameter skidding detection and control specified for electric vehicles," *Journal of the Franklin Institute*, vol. 352, no. 2, pp. 724–743, 2015.

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

[30] 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, 2018.

[31] M. Wielitzka, M. Dagen, and T. Ortmaier, "Sensitivity-based road friction estimation in vehicle dynamics using the unscented kalman filter," in *2018 Annual American Control Conference (ACC)*. IEEE, 2018, pp. 2593–2598.

[32] S. Jung and T. C. Hsia, "Explicit lateral force control of an autonomous mobile robot with slip," in *2005 IEEE/RSJ International Conference on Intelligent Robots and Systems*. IEEE, 2005, pp. 388–393.

[33] S. De Pinto, C. Chatzikomis, A. Sorniotti, and G. Mantriota, "Comparison of traction controllers for electric vehicles with on-board drivetrains," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 6715–6727, 2017.

[34] L. De Novellis, A. Sorniotti, P. Gruber, J. Orus, J.-M. R. Fortun, J. Theunissen, and J. De Smet, "Direct yaw moment control actuated through electric drivetrains and friction brakes: Theoretical design and experimental assessment," *Mechatronics*, vol. 26, pp. 1–15, 2015.

[35] Y. Wang, L. Yuan, H. Chen, P. Du, and X. Lian, "An anti-slip control strategy with modifying target and torque reallocation for heavy in-wheel motor vehicle," *Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering*, p. 09544070211063086, 2021.

[36] J. Zhou, H. Yue, J. Zhang, and H. Wang, "Iterative learning double closed-loop structure for modeling and controller design of output stochastic distribution control systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 6, pp. 2261–2276, 2014.

[37] C. Yin, J.-X. Xu, and Z. Hou, "A high-order internal model based iterative learning control scheme for nonlinear systems with time-iteration-varying parameters," *IEEE Transactions on Automatic Control*, vol. 55, no. 11, pp. 2665–2670, 2010.

[38] K.-H. Park, "An average operator-based pd-type iterative learning control for variable initial state error," *IEEE Transactions on Automatic Control*, vol. 50, no. 6, pp. 865–869, 2005.

[39] I. D. Landau, R. Lozano, M. M'Saad, and A. Karimi, *Adaptive control: algorithms, analysis and applications*. Springer Science & Business Media, 2011.

[40] G. Bai, Y. Meng, L. Liu, W. Luo, and Q. Gu, "Review and comparison of path tracking based on model predictive control," *Electronics*, vol. 8, no. 10, p. 1077, 2019.

[41] F. Borrelli, A. Bemporad, M. Fodor, and D. Hrovat, "An mpc/hybrid system approach to traction control," *IEEE Transactions on Control Systems Technology*, vol. 14, no. 3, pp. 541–552, 2006.

[42] P. Falcone, F. Borrelli, J. Asgari, H. E. Tseng, and D. Hrovat, "Predictive active steering control for autonomous vehicle systems," *IEEE Transactions on control systems technology*, vol. 15, no. 3, pp. 566–580, 2007.

[43] O. Barbarisi, G. Palmieri, S. Scala, and L. Glielmo, "Ltv-mpc for yaw rate control and side slip control with dynamically constrained differential braking," *European Journal of Control*, vol. 15, no. 3-4, pp. 468–479, 2009.

[44] B. Leng, L. Xiong, Z. Yu, K. Sun, and M. Liu, "Robust variable structure anti-slip control method of a distributed drive electric vehicle," *IEEE Access*, vol. 8, pp. 162 196–162 208, 2020.

[45] T. Brüdigam, M. Olbrich, D. Wollherr, and M. Leibold, "Stochastic model predictive control with a safety guarantee for automated driving," *IEEE Transactions on Intelligent Vehicles*, pp. 1–1, 2021.

[46] A. Carvalho, Y. Gao, S. Lefevre, and F. Borrelli, "Stochastic predictive control of autonomous vehicles in uncertain environments," in *12th International Symposium on Advanced Vehicle Control*, 2014, pp. 712–719.

[47] G. Siddharth, Z. Wang, H. Jing, and Y. Nakahira, "Adaptive safe control for driving in uncertain environments," *arXiv preprint*, 2022.

[48] W. Luo, W. Sun, and A. Kapoor, "Multi-robot collision avoidance under uncertainty with probabilistic safety barrier certificates," *Advances in Neural Information Processing Systems*, vol. 33, pp. 372–383, 2020.

[49] P. Falcone, H. Eric Tseng, F. Borrelli, J. Asgari, and D. Hrovat, "Mpc-based yaw and lateral stabilisation via active front steering and braking," *Vehicle System Dynamics*, vol. 46, no. S1, pp. 611–628, 2008.

[50] H. Zhao, B. Ren, H. Chen, and W. Deng, "Model predictive control allocation for stability improvement of four-wheel drive electric vehicles in critical driving condition," *IET Control Theory & Applications*, vol. 9, no. 18, pp. 2688–2696, 2015.

[51] E. Siampis, E. Velenis, S. Gariuolo, and S. Longo, "A real-time nonlinear model predictive control strategy for stabilization of an electric vehicle at the limits of handling," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 6, pp. 1982–1994, 2017.

[52] J. Yoon, W. Cho, J. Kang, B. Koo, and K. Yi, "Design and evaluation of a unified chassis control system for rollover prevention and vehicle stability improvement on a virtual test track," *Control Engineering Practice*, vol. 18, no. 6, pp. 585–597, 2010.

[53] M. Ataei, A. Khajepour, and S. Jeon, "Model predictive control for integrated lateral stability, traction/braking control, and rollover prevention of electric vehicles," *Vehicle system dynamics*, vol. 58, no. 1, pp. 49–73, 2020.

[54] M. Isaksson Palmqvist, "Model predictive control for autonomous driving of a truck," https://www.diva-portal.org/smash/get/diva2:930995/FULLTEXT01.pdf, 2016.

[55] U. Kiencke and L. Nielsen, "Automotive control systems: for engine, driveline, and vehicle," 2000.

[56] P. Falcone, M. Tufo, F. Borrelli, J. Asgari, and H. E. Tseng, "A linear time varying model predictive control approach to the integrated vehicle dynamics control problem in autonomous systems," in *2007 46th IEEE Conference on Decision and Control*. IEEE, 2007, pp. 2980–2985.

[57] J. A. Andersson, J. V. Frasch, M. Vukov, and M. Diehl, "A condensing algorithm for nonlinear mpc with a quadratic runtime in horizon length," *Automatica*, pp. 97–100, 2013.

[58] L. T. Biegler, "Efficient solution of dynamic optimization and nmpc problems," in *Nonlinear model predictive control*. Springer, 2000, pp. 219–243.

[59] H. Zhu, B. Brito, and J. Alonso-Mora, "Decentralized probabilistic multi-robot collision avoidance using buffered uncertainty-aware voronoi cells," *Autonomous Robots*, pp. 1–20, 2022.

[60] D. Claes, D. Hennes, K. Tuyls, and W. Meeussen, "Collision avoidance under bounded localization uncertainty," in *2012 IEEE/RSJ International Conference on Intelligent Robots and Systems*. IEEE, 2012, pp. 1192–1198.

[61] L. Lindemann and D. V. Dimarogonas, "Control barrier functions for signal temporal logic tasks," *IEEE control systems letters*, vol. 3, no. 1, pp. 96–101, 2018.

[62] 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.

[63] M. Farina, L. Giulioni, and R. Scattolini, "Stochastic linear model predictive control with chance constraints–a review," *Journal of Process Control*, vol. 44, pp. 53–67, 2016.

[64] L. Hewing, K. P. Wabersich, M. Menner, and M. N. Zeilinger, "Learning-based model predictive control: Toward safe learning in control," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 3, pp. 269–296, 2020.

[65] M. Chen and C. J. Tomlin, "Hamilton–jacobi reachability: Some recent theoretical advances and applications in unmanned airspace management," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, pp. 333–358, 2018.

[66] V. Dhiman, M. J. Khojasteh, M. Franceschetti, and N. Atanasov, "Control barriers in bayesian learning of system dynamics," *IEEE Transactions on Automatic Control*, 2021.

[67] K. P. Wabersich, L. Hewing, A. Carron, and M. N. Zeilinger, "Probabilistic model predictive safety certification for learning-based control," *IEEE Transactions on Automatic Control*, vol. 67, no. 1, pp. 176–188, 2021.

[68] Z. Wang, H. Jing, C. Kurniawan, A. Chern, and Y. Nakahira, "Myopically verifiable probabilistic certificate for long-term safety," in *2022 American Control Conference (ACC)*. IEEE, 2022, pp. 4894–4900.

[69] M.-Y. Yu, R. Vasudevan, and M. Johnson-Roberson, "Occlusion-aware risk assessment for autonomous driving in urban environments," *Robotics and Automation Letters*, vol. 4, no. 2, pp. 2235–2241, 2019.

[70] R. Poncelet, A. Verroust-Blondet, and F. Nashashibi, "Safe geometric speed planning approach for autonomous driving through occluded intersections," in *International Conference on Control, Automation, Robotics and Vision*. IEEE, 2020, pp. 393–399.

[71] Z. Zhang and J. Fisac, F, "Safe occlusion-aware autonomous driving via game-theoretic active perception," in *Robotics: Science and Systems*. RSS, 2021.

[72] M. Koç, E. Yurtsever, K. Redmill, and Ü. Özgüner, "Pedestrian emergence estimation and occlusion-aware risk assessment for urban autonomous driving," in *International Intelligent Transportation Systems Conference*. IEEE, 2021, pp. 292–297.

[73] M. Kahn, A. Sarkar, and K. Czarnecki, "I know you can't see me: Dynamic occlusion-aware safety validation of strategic planners for autonomous vehicles using hypergames," in *International Conference on Robotics and Automation*. IEEE, 2022, pp. 11 202–11 208.

[74] Y. Lyu, W. Luo, and J. M. Dolan, "Probabilistic safety-assured adaptive merging control for autonomous vehicles," in *International Conference on Robotics and Automation*. IEEE, 2021, pp. 10 764–10 770.

[75] T. Brüdigam, M. Olbrich, D. Wollherr, and M. Leibold, "Stochastic model predictive control with a safety guarantee for automated driving," *Transactions on Intelligent Vehicles*, 2021.

[76] J. Müller, J. Strohbeck, M. Herrmann, and M. Buchholz, "Motion planning for connected automated vehicles at occluded intersections with infrastructure sensors," *Transactions on Intelligent Transportation Systems*, 2022.

[77] D. Isele, R. Rahimi, A. Cosgun, K. Subramanian, and K. Fujimura, "Navigating occluded intersections with autonomous vehicles using deep reinforcement learning," in *International Conference on Robotics and Automation*. IEEE, 2018, pp. 2034–2039.

[78] K. Sama, Y. Morales, H. Liu, N. Akai, A. Carballo, E. Takeuchi, and K. Takeda, "Extracting human-like driving behaviors from expert driver data using deep learning," *Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9315–9329, 2020.

[79] C. Hubmann, N. Quetschlich, J. Schulz, J. Bernhard, D. Althoff, and C. Stiller, "A pomdp maneuver planner for occlusions in urban scenarios," in *Intelligent Vehicles Symposium*. IEEE, 2019, pp. 2172–2179.

[80] S. Gangadhar, Z. Wang, H. Jing, and Y. Nakahira, "Adaptive safe control for driving in uncertain environments," in *Intelligent Vehicles Symposium*. IEEE, 2022, pp. 1662–1668.

[81] K. Ogata, *Discrete-time control systems*. Prentice-Hall, Inc., 1995.

[82] C.-Y. Liang and H. Peng, "String stability analysis of adaptive cruise controlled vehicles," *International Journal Series C Mechanical Systems, Machine Elements and Manufacturing*, vol. 43, no. 3, pp. 671–677, 2000.

[83] A. Rasouli and J. K. Tsotsos, "Autonomous vehicles that interact with pedestrians: A survey of theory and practice," *Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 900–918, 2019.

[84] P. Kielar, M, O. Handel, D. Biedermann, H, and A. Borrmann, "Concurrent hierarchical finite state machines for modeling pedestrian behavioral tendencies," *Transportation Research Procedia*, vol. 2, pp. 576–584, 2014.

[85] C. Hubmann, J. Schulz, G. Xu, D. Althoff, and C. Stiller, "A belief state planner for interactive merge maneuvers in congested traffic," in *International Conference on Intelligent Transportation Systems*. IEEE, 2018, pp. 1617–1624.

[86] C. Burger, T. Schneider, and M. Lauer, "Interaction aware cooperative trajectory planning for lane change maneuvers in dense traffic," in *International Conference on Intelligent Transportation Systems*. IEEE, 2020, pp. 1–8.

[87] A. Rasouli, I. Kotserub, and J. Tsotsos, K, "Are they going to cross? a benchmark dataset and baseline for pedestrian crosswalk behavior," in *International Conference on Computer Vision Workshops*. IEEE, 2017.

[88] D. Helbing and P. Molnár, "Social force model for pedestrian dynamics," *Physical Review E*, vol. 51, no. 5, pp. 4282–4286, 1995.

[89] F. Camara, N. Bellotto, S. Cosar, F. Weber, D. Nathanael, M. Althoff, J. Wu, J. Ruenz, A. Dietrich, G. Markkula *et al.*, "Pedestrian models for autonomous driving part ii: high-level models of human behavior," *Transactions on Intelligent Transportation Systems*, vol. 22, no. 9, pp. 5453–5472, 2020.

[90] O. Johnson, *Information theory and the central limit theorem*. World Scientific, 2004.

[91] A. H. Lang, S. Vora, H. Caesar, L. Zhou, J. Yang, and O. Beijbom, "Pointpillars: Fast encoders for object detection from point clouds," in *Conference on Computer Vision and Pattern Recognition*, 2019, pp. 12 697–12 705.

[92] X. Zhang, H. Fu, and B. Dai, "Lidar-based object classification with explicit occlusion modeling," in *International Conference on Intelligent Human-Machine Systems and Cybernetics*. IEEE, 2019.

[93] H. Jing and Y. Nakahira, "Probabilistic safety certificate for multi-agent systems," in *2022 IEEE 61st Conference on Decision and Control (CDC)*. IEEE, 2022, pp. 5343–5350.

[94] Z. Wang, H. Jing, C. Kurniawan, A. Chern, and Y. Nakahira, "Myopically verifiable probabilistic certificate for long-term safety," *arXiv preprint arXiv:2110.13380*, 2021.

[95] P. Onelcin and Y. Alver, "The crossing speed and safety margin of pedestrians at signalized intersections," *Transportation Research Procedia*, vol. 22, pp. 3–12, 2017.

[96] D. R. Cox, *Queues*. Chapman and Hall/CRC, 2020.

[97] J. D. Lartey *et al.*, "Predicting traffic congestion: A queuing perspective," *Open Journal of Modelling and Simulation*, vol. 2, no. 02, p. 57, 2014.

[98] M. O'Kelly, H. Zheng, A. Jain, J. Auckley, K. Luong, and R. Mangharam, "Tunercar: A superoptimization toolchain for autonomous racing," in *International Conference on Robotics and Automation*, 2020, pp. 5356–5362.

[99] J. Kong, M. Pfeiffer, G. Schildbach, and F. Borrelli, "Kinematic and dynamic vehicle models for autonomous driving control design," in *Intelligent Vehicles Symposium*, 2015, pp. 1094–1099.

[100] Z. Wang, H. Jing, A. Chern, and Y. Nakahira, "Myopically verifiable probabilistic certificate for long-term safety," *Under Review*, 2023.

[101] S. Gangadhar, Z. Wang, K. Poku, N. Yamada, K. Honda, Y. Nakahira, H. Okuda, and T. Suzuki, "An occlusion- and interaction-aware safe control strategy for autonomous vehicles," in *2023 22nd IFAC World Congress*, 2023.

Chapter 2

Dealing with Extreme Driving Conditions

2.1 Background

Driving in adverse conditions (e.g. icy roads with low traction) is challenging for both human drivers and autonomous vehicles. The vehicle parameters can vary by operating conditions, and the control strategy must adapt to changes quickly. These parameters may have significant uncertainties before their changes can be accurately estimated. The uncertainties due to unmodeled dynamics and noise in sensing, localization, and estimation can be substantial. Moreover, the vehicles' states can have unsafe regions of attractions, in which controllability and stability are significantly reduced. The likelihood of entering such regions depends on the future road condition (traction, curvature, etc.), planned maneuvers and actions, predictions of the environments, and their levels of uncertainty. Therefore, it is critical for an autonomous vehicle to adapt to changes, mediate behaviors based on uncertainties, exploit predictions, and do them in an integrated manner.

2.1.1 Related Work

Various techniques have been developed for advanced driving assistance systems (ADASs) and autonomous vehicles (AVs). Many of these techniques are developed in deterministic worst-case frameworks: H-infinity controllers [23], robust sliding mode controllers [24,25], fuzzy logic controllers [26,27,28], and control barrier functions [29, 30]. These techniques can often be efficiently

computed but require full system models and small bounded uncertainties (errors). In large uncertainties, these techniques may not perform well. Ensuring safety for all possible errors may be infeasible. The performance may not degrade gracefully for increasing uncertainties due to overly conservative actions.

When there are unknown parameters or changes in the internal and external parameters, techniques have been developed for parameter estimation and fast adaptation. Some combine parameter estimates (e.g., Kalman filter, Bayesian filter) and additional modifications in control to account for uncertainties [31, 32, 33]. The modification in control techniques is often built on worst-case frameworks and similarly assumes the availability of accurate estimates. Others direct estimate the control parameters using PID tuning [34,35], interactive learning methods [36,37,38], adaptive control [39]. These methods' performance guarantees (convergence) often require the system dynamics to take some specific structures, and they often do not exploit future predictions.

Various model predictive control (MPC) techniques have been developed to better exploit future predictions and balance different performance objectives [40, 41, 42, 43, 44]. These methods look into future time horizons and use predictions to achieve better performance. As the number of possible trajectories grows exponentially to the outlook time horizon, there are often stringent tradeoffs between outlook time horizon and computation burdens.

To better account for uncertainties, many methods use stochastic frameworks. Examples of these techniques are stochastic MPC [45] and chance-constrained MPC [46]. Control of distributions and constraints of probability can be efficiently computed under certain assumptions such as linear dynamics and Gaussian disturbances. However, for general (nonlinear) systems, there do not exist lightweight algorithms suitable for online or onboard computation. The tradeoff between outlook time horizon and computation load can be even more stringent because constraining long-term probability requires characterizing the evolution of complex state distributions over time.

2.1.2 Contributions of This Chapter

Motivated by these challenges, we propose a stochastic adaptive safe control technique that accounts for internal parameter changes, planned vehicle control, and the prediction of environmental factors. The technique efficiently (myopically) finds a control action with ensured long-term safe probability.

The method can both flexibly adapt to changes and remain robust in a steady state by mediating behaviors based on the levels of parameter uncertainties. The long-term safe probability can represent a variety of performance/safety specifications, and its probability measure can be continuously learned based on driving data.

Specifically, we derive a sufficient condition for controlling the safe probability within a desirable range. The safety condition is then used to construct a safe control algorithm that can be efficiently computed in real-time and modularly embedded into existing decision-making processes. The algorithm accounts for the distribution of uncertainties and finds appropriate control actions even in the presence of large uncertainties. Such features allow safer and faster responses to changes before sufficient samples become available or before the parameter estimates converge. Moreover, it can be modularly added into an existing decision-making process: for example, it can be incorporated into the MPCs to balance multiple objectives while ensuring chance-constrained safety conditions for nonlinear affine control systems without the assumption of Gaussian distributions. The resulting algorithms can properly control the long-term safe probabilities, which are defined based on future trajectories and intended control action, allowing that information to be used for producing more stable and safer action. Furthermore, the long-term safe probability can be learned continuously using past driving data, which allows the control policy to be individually fine-tuned based on its common driving conditions. By extending the outlook time horizon, preventive control actions can be executed before the system reaches a state where maintaining safety is no longer possible. Finally, the framework requires few assumptions in the choice of models: it can be adapted to different vehicle dynamics or tire models, ranging from white-box to gray-box to black-box models. The model also does not need to be differentiable—a common requirement when deterministic safe control algorithms that involve the computation of (Lie) derivatives to be applied.

The rest of this chapter is organized as follow. We first present the vehicle dynamics, controller structures, and design objectives in Section 4.2. Then, we present the proposed safe control framework and prove its performance guarantees in Section 2.3. Finally, we present a few case studies of autonomous driving in Section 2.4 and discuss the advantages of the proposed approaches.

2.2 Problem Statement

In this section, we introduce the generic vehicle dynamics in section 2.2.1, controller in section 2.2.2, and the safety specifications in section 2.2.3.

2.2.1 System Model

We use $x \in \mathbb{R}^m$ to represent the state of the vehicle and $u \in \mathbb{R}^n$ to represent the control action. The dynamics of x depends on the physics and mechanics of the vehicle and the control action. We use

$$\dot{x} = F_x(x, \xi) + F_u(x)u, \tag{2.1}$$

with some possibly nonlinear functions F_x, F_u to represent the dynamics. The vehicle dynamics are parameterized by $\xi \in \mathbb{R}^l$. The values of ξ can change over time, so its exact values may not be accessible by the controller. The system dynamics in (2.1) is affine to the control action u. The proposed technique is agnostic to the choice of vehicle models, and thus F_x and F_u can be high-dimensional and highly nonlinear functions and/or built from data.

In order to implement the controller in digital systems, we discretize (2.1) as follows.

$$x_{k+1} = F(x_k, u_k, \xi_k). \tag{2.2}$$

Let (2.2) be the discretized system dynamics, where F is a function derived from (2.1). Let x_k and u_k be the value of x_t and u_t evaluated at the discrete time point $t = k\Delta t$, respectively, where Δt is the sampling time of the digital controller.

2.2.2 Nominal Controller

We assume the existence of an estimator for the vehicle parameters ξ. Let $\hat{\xi}_k$ denote the latest estimate of ξ available at time step k. We allow the estimator to operate in different time scale from the controller or be updated intermittently. We additionally assume that the estimator gives the posterior of the estimate. Let z denote the vehicle state and estimated parameter at time k, *i.e.,*

$$z_k = \left[x_k^T,\ \hat{\xi}_k\right]^T \in \mathbb{R}^{m+l}. \tag{2.3}$$

The distribution of z_k is determined from the vehicle dynamics, the estimator, and environmental changes.

The system is equipped with a nominal optimization-based (MPC) controller of the following form:

$$u_{k:k+H} = \underset{u_{k:k+H} \in \mathcal{U}}{\arg\min} \quad J(x_{k:k+H}, u_{k:k+H}) \tag{2.4a}$$

$$\text{s.t.} \quad C(x_{k:k+H}, u_{k:k+H}) \succeq 0 \tag{2.4b}$$

$$x_{i+1} = \hat{F}(x_i, u_i, \hat{\xi}_k), i = k, \cdots, k+H \tag{2.4c}$$

where $x_{k:k+H} = \{x_k, x_{k+1}, \cdots, x_{k+H}\}$, and $u_{k:k+H} = \{u_k, u_{k+1}, \cdots, u_{k+H}\}$. Here, H is the MPC outlook horizon, and the optimization domain $\mathcal{U}$ is the admissible set of control actions. In this optimization problem, the cost function $J(x_{k:k+H}, u_{k:k+H})$ for system state and control is minimized. Condition (2.4b) represents the constraints in the vehicle states and controls (*e.g.,* steering angle limits). The left hand side of (2.4b), $C(x_{k:k+H}, u_{k:k+H})$, is a vector valued function of $x_{k:k+H}, u_{k:k+H}$, and the inequality of (2.4b) is taken point-wise. Condition (2.4c) accounts for the knowledge of the system dynamics, which approximates the original dynamics (2.2), *i.e.,* $F \approx \hat{F}$. This controller is designed based on the performance specifications of the system and does not necessarily account for the safety specifications, which is described in the next subsection.

2.2.3 Safety Specifications

We represent the safe event using a set $\mathcal{S} \in \mathbb{R}^m$ defined as the 0-superlevel set of a function $\phi : \mathbb{R}^m \times \mathbb{R}^l \to \mathbb{R}$, *i.e.,*

$$\mathcal{S}(\xi) = \{x : \phi(x, \xi) \geq 0\}, \tag{2.5}$$

where the function $\phi(x, \xi)$ involves the internal state of the vehicle x and external/environmental variables ξ (*e.g.,* friction coefficients). The safety specifications is then given by the following condition: the vehicle state stays within the safe set, *i.e.,*

$$x \in \mathcal{S}(\xi). \tag{2.6}$$

A major challenge to ensure (2.6) arises from the uncertainties in the system. For example, safety depends on ξ, and when it changes, the controller must

adapt its action before an accurate estimate of ξ can be constructed from samples. When the uncertainty of ξ is large, it can be impossible to have (2.6) with probability 1. Moreover, ensuring (2.6) for all possible worst cases may not be feasible and/or leads to unnecessarily conservative control actions, which compromise the robustness and performance of the system. Instead, we aim to control the safety probability defined below.

Specifically, we want to ensure $x \in \mathcal{S}(\xi)$ during an outlook time window $\mathcal{T}(k) = \{k, k+1, \cdots, k+T\}$ with probability $1-\epsilon$: *i.e.,* at any time $k \in \mathbb{Z}_+$,

$$\mathbb{P}(x_\tau \in \mathcal{S}(\xi_\tau), \forall \tau \in \mathcal{T}(k)) \geq 1 - \epsilon. \tag{2.7}$$

Here ϵ can be interpreted as the tolerance level for unsafe events. The outlook time horizon T should be sufficiently long to avoid myopic behaviors that are unsafe. Note that the outlook time horizon T does not need to be identical to the outlook horizon H of the MPC controller (2.4). The benefit of choosing different T and H will be explained later in Remark 3.

2.3 Proposed Method

In this section, we present the proposed safety condition in section 2.3.1, and the proposed safe adaptation algorithm in section 2.3.2.

2.3.1 Proposed Safety and Recovery Condition

In this subsection, we propose an adaptive safe control method that exploits prediction and mediates behaviors based on the level of uncertainties. We first derive a sufficient condition that ensures safe probability based on a novel probabilistic forward invariance condition. The key novelty of this condition is that it can ensure long-term safety probability to be ensured using a myopic controller that can be computed in real-time onboard computation, while standard control barrier function (CBF) based methods often lead to unsafe behaviors because of the long tail distribution of the unsafe events. The long-term safety probability can be computed offline and be continuously learned using the driving history. The controller only needs to myopically evaluate the immediate control action using a linear constraint, which can be easily integrated into optimization-based planning and control processes (*e.g.,* MPC [40, 41, 42, 45, 46]).

Let A denote the following discrete-time generator.

Definition 2 (Discrete-time Generator)**.** The discrete-time generator A of a discrete-time stochastic process $\{y_k \in \mathbb{R}^n\}_{k\in\mathbb{Z}_+}$ with sampling interval Δt evaluated at time k is given by

$$AG(y_k) = \frac{\mathbb{E}[G(y_{k+1})|y_k] - G(y_k)}{\Delta t} \tag{2.8}$$

whose domain is the set of all functions $G : \mathbb{R}^n \to \mathbb{R}$ of the stochastic process.

The discrete-time generator can be considered as the discrete-time counterpart of the infinitesimal generator for a continuous-time process.

Let $\mathbf{F}(z)$ be the probability of the vehicle originating from state $z_k = z$ at time k to remain safe during outlook time horizon $\mathcal{T}(k)$, *i.e.,*

$$\mathbf{F}(z) := \mathbb{P}(x_\tau \in \mathcal{S}(\xi_\tau), \forall \tau \in \mathcal{T}(k)|z_k = z). \tag{2.9}$$

Note that, conditioned on $z_k = z$, this probability does not depend on k.[1] In order to ensure safety of the system, we propose to constrain the control action u_k to satisfy the following conditions at all time $k \in \mathbb{Z}_+$:

$$A\mathbf{F}(z_k) \geq -\gamma(\mathbf{F}(z_k) - (1-\epsilon)). \tag{2.10}$$

Here, $\gamma : \mathbb{R} \to \mathbb{R}$ is a function of $\mathbf{F}(z_k) - (1-\epsilon)$. When $\mathbf{F}(z_k) \leq 1-\epsilon$, the value of $A\mathbf{F}(z_k)$, if positive, can be interpreted as the the recovery rate. Condition (2.10) essentially constrains the discrete-time generator of $\mathbf{F}(z_k)$ to be lower bounded by $-\gamma(\mathbf{F}(z_k) - (1-\epsilon))$.

Remark 2. Since function $\mathbf{F}(z_k)$ gives the safety probability of the system in the time horizon $\mathcal{T}(k)$, it encodes information of prediction on the future as well as the level of uncertainties.

We impose the following two conditions for $\gamma(q)$:

Requirement 1: $\gamma(q)$ is strictly concave or linear in q.

Requirement 2: $\gamma(q) \leq q$, $\forall q \in \mathbb{R}$.

Condition (2.10) with design requirements 1 and 2 guarantees the safe probability condition (2.7) to hold, as stated below.

[1]This property holds because the system dynamics in (2.2) is time-invariant. The functions F_x and F_u do not depend on time.

Theorem 3. *Consider the open-loop system* (2.2)*. Let* $\gamma(q)$ *satisfy requirements 1 and 2. If the state and parameter estimation originate at* $z_0 = z$ *with* $\mathbf{F}(z) > 1-\epsilon$*, and the control action satisfies* (2.10) *at all time, then the following condition holds:*

$$\mathbb{P}(x_\tau \in \mathcal{S}(\xi_\tau), \forall \tau \in \mathcal{T}(k)) \geq 1 - \epsilon \tag{2.11}$$

for all time $k \in \mathbb{Z}_+$*. Here, the probability is taken over* z_k *conditioned on* $z_0 = x$*, and* $\mathbf{F}$ *in* (2.9) *gives the probability of safety of the future trajectories* $\{z_\kappa\}_{\{k+1,k+2,\cdots,k+T\}}$ *conditioned on* z_k*.*

Proof. See [47].

Note that the left hand side of (2.11) is equivalent to $\mathbb{E}\left[\mathbb{P}(x_\tau \in \mathcal{S}(\xi_\tau), \forall \tau \in \mathcal{T}(k))\right]$, where the expectation is taken over z_k conditioned on $z_0 = x$, and $\mathbf{F}$ in (2.9) gives the probability of safety of the future trajectories $\{z_\kappa\}_{\{k+1,k+2,\cdots,k+T\}}$ conditioned on z_k.

2.3.2 Proposed Safe Adaptation Algorithm

Next, we show that $A\mathbf{F}(z_k)$ can be approximated using a linear function of u_k when the sampling interval Δt is sufficiently small. With z defined in (2.3), let $D(z)$ denote the first m entries of the gradient of $\mathbf{F}(z)$ evaluated at z, *i.e.,*

$$D(z) = [D^{(1)}(z), D^{(2)}(z), \cdots, D^{(m)}(z)]^T \in \mathbb{R}^m, \tag{2.12}$$

where

$$D^{(i)}(z) = \frac{\mathbf{F}(z + \Delta^{(i)}) - \mathbf{F}(z - \Delta^{(i)})}{2\Delta}. \tag{2.13}$$

Here, Δ is the step size to calculate the finite difference of the safety probability, $\Delta^{(i)}$ denotes a vector that takes a scalar value of Δ in i-th entry and 0 otherwise. Note that $D(z)$ has the same dimension with the state x.

We make the following assumptions:

$$\lim_{\Delta t \to 0} \mathbb{E}\left[\frac{z_{k+1} - z_k}{\Delta t}\right] = \begin{bmatrix} F_x(x_k, u_k, \hat{\xi}_k) + F_u(x_k)u_k \\ 0 \end{bmatrix} \tag{2.14}$$

$$\lim_{\Delta t \to 0} \frac{1}{2\Delta t} \mathbb{E}\left[(z_{k+1} - z_k)^T M (z_{k+1} - z_k) \mid z_k\right] = c_k \tag{2.15}$$

$$\lim_{\Delta t \to 0} \frac{1}{\Delta t} \mathbb{E}\left[R_2(z_k, z_{k+1}) \mid z_k\right] = 0. \tag{2.16}$$

Here, M is a matrix of appropriate dimension, c_k is a constant c_k, and R_2 denotes the terms with order greater than 2 in the Taylor expansion of Ψ, *i.e.,* $R_2\left(z_k, z_{k+1}\right) = o\left(\|z_{k+1} - z_k\|^2\right)$. Condition (2.14) assumes the limit of the derivative of x equals to the dynamics with the estimated parameter, and the estimated parameter is not changing in the infinitesimal time. This holds for ordinary differential equation (ODE) systems with additive Gaussian noise, which is commonly assumed in stochastic safe control community [10,48]. It is assumed in (2.14) that information about the future value of $\hat{\xi}$ is not available. Condition (2.15) says the second order term in the Taylor expansion of Ψ equals to some constant c_k. Note that this term does not necessarily vanish (*e.g.,* Ito's calculus), but it will not depend on u. Condition (2.16) implies that terms higher than third order will vanish.

Lemma 2. *Assume* (2.14)–(2.16) *hold. Then, the following condition holds.*

$$\lim_{\Delta t \to 0} A\mathbf{F}(z_k) = D(z_k) \cdot (F_x(x_k, \hat{\xi}_k) + F_u(x_k)u_k + c_k). \tag{2.17}$$

Proof. See [47]

From Lemma 2, we can use sufficiently small sampling interval Δt and evaluate condition (2.10) using

$$D(z_k) \cdot (F_x(x_k, \hat{\xi}_k) + F_u(x_k)u + c_k) \geq -\gamma(\mathbf{F}(z_k) - (1 - \epsilon)). \tag{2.18}$$

Since D, F_x, F_u and $\mathbf{F}$ are all constant given x_k and $\hat{\xi}_k$, condition (2.18) is linear in u, thus can be used in LQ or convex problem without losing convexity. Therefore, it can be easily integrated into existing optimization-based controllers (*e.g.,* [49,50,51,52]) without much extra computational [40, 53]. For example, we can impose (2.18) as an addition constraints in the nominal MPC controller (2.4), *i.e.,*

$$u_{k:k+H} = \underset{u_{k:k+H} \in \mathcal{U}}{\arg\min} \quad J(x_{k:k+H}, u_{k:k+H}), \tag{2.19a}$$

$$\text{s.t.} \quad \text{(2.4b), (2.4c) and (2.18).} \tag{2.19b}$$

This controller exploits prediction through both MPC forward rollout and the long-term safety probability function $\mathbf{F}(z)$ in (2.9), with different outlook horizon H and T, respectively.

Remark 3. The computation load of the MPC controller (2.4) often scales exponentially with its time horizon H. Interestingly, the safety condition (2.10)

can be used to ensure safety during horizon T without requiring the MPC controller to extend its outlook horizon to T. Thus, if the value D in (2.12)-(2.13) is computed offline, the computation load of the MPC controller only needs to scale with $H(\ll T)$.

The overall safe control strategy is given by Algorithm 2. At each time step k, Algorithm 2 functions as follows. In line 5, it obtains from the estimator the latest estimate $\hat{\xi}_k$ for the system parameter ξ. In line 6, it evaluates the functions $\mathbf{F}$ and D at z_k either using online or offline computation. These values can be obtained by sampling the system dynamics (2.1) or (2.2), or can be continuously learned from the past driving data. In line 7, it finds an control action u_k either using the optimization problem (2.19). This control action u_k is executed in line 8, and its impact on x_{k+1} is observed in line 4 at the next time step.

Algorithm 1 Safe control algorithm

```
1: Initialize Δz
2: k ← 0
3: while k < K_max do
4:     Observe x_k
5:     Obtain ξ̂_k from the estimator
6:     Obtain F(z_k) and D(z_k)
7:     Find u_k ← solve {u_k in (2.19)}
8:     Execute action u_k
9:     k ← k + 1
10: end while
```

2.4 Deployment and Experiment

We evaluated the efficacy of the proposed adaptive safe control method with simulation on a four-wheel 3-DoF vehicle. The design goal is to track a reference path without slipping. We present the vehicle dynamics in section 2.4.1, the controller and the design specification in section 2.4.2, and the results and discussions in section 2.4.3.

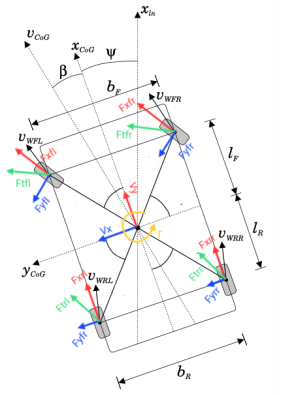


Figure 2.1: Freebody diagram of the vehicle.

2.4.1 Vehicle Model

We consider the vehicle model presented in [54] and Burckhardt's tire model based on the Kamm friction circle [55].

Fig. 2.1 shows the diagram of the vehicle model. In this model, each tire is associated with a longitudinal and lateral force. We use F_t to denote the total tire force on each of the four wheels, calculated as the squared sum of the lateral and longitudinal tire force. The saturated tire grip force is given by

$$F_{\text{sat}} = \mu m g/4, \tag{2.20}$$

where m is the vehicle mass, and g is gravitational acceleration constant, μ is the friction coefficient between the tire and road (referred to as c_1 in Burckhardt's tire model). The vehicle system's state and control actions are

$$x = [x_{\text{CoG}},\, y_{\text{CoG}},\, \psi,\, v_x,\, v_y,\, r,\, \omega_{fr},\, \omega_{fr},\, \omega_{rl},\, \omega_{rr},\, \delta]^T \tag{2.21}$$

$$u = \left[T_e,\, \dot{\delta}\right]^T, \tag{2.22}$$

where x_{CoG}, y_{CoG}, and ψ are the vehicle's inertial pose, v_x and v_y are the vehicle's frame velocities, r is the yaw rate, ω_{fl}, ω_{fr}, ω_{rl}, and ω_{rr} are the tire angular rates, δ is the steering angle, T_e is the input torque from the differential and $\dot{\delta}$ is the steering rate. The specific choice of parameters for simulation are summarized in Table 2.1. The friction coefficient μ is the unknown parameter ξ in our simulation, by adding an additive zero-mean Gaussian noise with variance σ^2 to μ. Please see [47] for more details of the vehicle model.

Table 2.1: Simulation Parameters

Parameter	Definition	Value
C_f	cornering stiffness for front tire	6680 N/rad
C_r	cornering stiffness for rear tire	6680 N/rad
b_a	aerodynamic drag coefficient	100 Ns/m
b_r	tire drag coefficient	100 Ns/m
μ	tire to road friction coefficient	0.03
m	mass of the vehicle	1500 kg
g	gravitational acceleration	9.8 $\mathrm{m/s^2}$
L_f	front wheel distance to vehicle center	1.070 m
L_r	rear wheel distance to vehicle center	1.605 m
W	width of the vehicle	1.517 m
I_z	rotational inertia about the center	2600 $\mathrm{kgm^2}$

2.4.2 Controllers and Design Specifications

The performance specification is to track a reference trajectory. This can be achieved by a linear time-varying MPC controller (LTV-MPC) of the form (2.4) with

$$\hat{F}(x,u) = A_{\text{lin}}\, x_e + B_{\text{lin}}\, u_e, \tag{2.23a}$$

$$J(x,u) = \frac{1}{2} x_e^T Q x_e + \frac{1}{2} u_e^T R u_e, \tag{2.23b}$$

$$C(x,u) \leq 0, \tag{2.23c}$$

where $x_e = x - x_r$, $u_e = u - u_r$ with $[x_r, u_r]$ be the reference trajectory, A_{lin} and B_{lin} are the Jacobian of a reduced-order linearized vehicle dynamics at each time step, with states $x = [x_{\text{CoG}},\, y_{\text{CoG}},\, \psi,\, v_x,\, v_y,\, r]^T$ and controls $u = [\dot{v}_x,\, \delta]^T$ [56]. The reference trajectories $[x_r, u_r]$ are obtained from a B-spline based planner and reference generator demonstrated in [54]. The objective J is the weighted quadratic penalties on the trajectory tracking error x_e and the difference between the actual control and the reference control u_e. Constraint function C limits the control inputs of the vehicle system within a certain range. LTV-MPC linearizes the system at each time step, and predicatively optimize the control input in a given horizon H to make sure the vehicle

is tracking the reference trajectory while satisfying necessary constraints. However, we do not add any safety specific constraints in LTV-MPC. This is because LTV-MPC uses a reduced state space model of the vehicle and the tire force dynamic is highly nonlinear and under-actuated in this state space. Moreover, the nonlinearity of tire-force dynamics and the under-actuated nature of the safety specification prevents control barrier function methods to be used for constructing a linear constraint.

The safety specification is to limit each tire's total force within a certain percentage $\eta \in (0, 1)$ of the maximum tire force F_{sat}, beyond which the vehicle starts to slip. The safety condition is defined by (2.5) with

$$\begin{aligned}\phi(x, \xi) = \min\Bigg\{1 - \left(\frac{4F_{tfl}}{\eta\xi mg}\right)^2, 1 - \left(\frac{4F_{tfr}}{\eta\xi mg}\right)^2, \\ 1 - \left(\frac{4F_{trl}}{\eta\xi mg}\right)^2, 1 - \left(\frac{4F_{trr}}{\eta\xi mg}\right)^2\Bigg\},\end{aligned} \tag{2.24}$$

where $\xi = \mu$ is the friction coefficient, F_{tfl} and F_{trr}, etc, are the tire forces on front left wheel, rear right wheel, etc. With this definition, if any of the four tire's total force F_t exceed ηF_{sat}, function $\phi(x, \xi)$ in (2.24) will become negative indicating that safety is being compromised. Accordingly, the proposed controller is given by (2.19) whose parameters are defined by (2.23). This controller essentially add to LTV-MPC a linear constraint (2.18) that ensures the long-term safe probability and probabilistic recovery speed.

2.4.3 Results

Impact of uncertainty on safety and performance. Fig 2.2 shows the safety and performance for varying levels of uncertainties for the proposed method and the LTV-MPC. The safety is measured by the averaged value of the safety specification function (2.24), the performance is measured by the averaged cost function value, and the level of uncertainty is measured by σ. In contrast to LTV-MPC, the proposed method has a more graceful degradation in safety and performance. With the proposed method, the tire force always stayed within 85% of its saturation (Fig. 2.3) and produced stable trajectories (Fig. 2.4 left). This can be achieved because the proposed controller will look into the future and impose a more effective safe control on the system once the safety probability has an tendency of dropping, i.e., the system state is getting close to some potentially unsafe regions. With LTV-MPC,

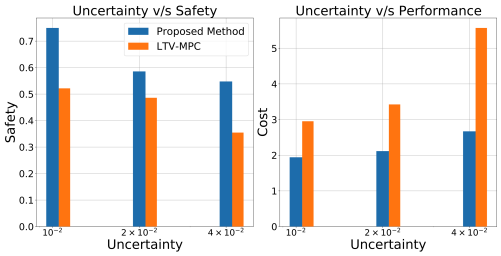


Figure 2.2: Impact of uncertainty on safety (left) and performance (right).

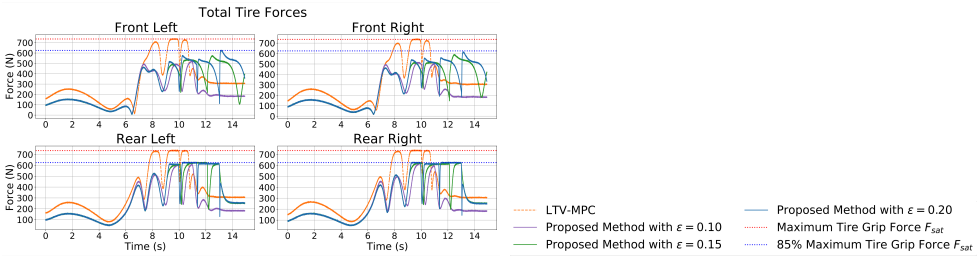


Figure 2.3: Total tire force of each wheel.

the total tire force started to exceed the maximum desired saturation rate from around 8 seconds. This is because LTV-MPC can not directly account for the safety specifications in its constraints, as mentioned in the previous section.

Safety versus performance tradeoffs. Fig. 2.5 shows the tradeoffs between the safety and performance for the proposed method and the LTV-MPC. The proposed methods have an improved tradeoff than LTV-MPC.

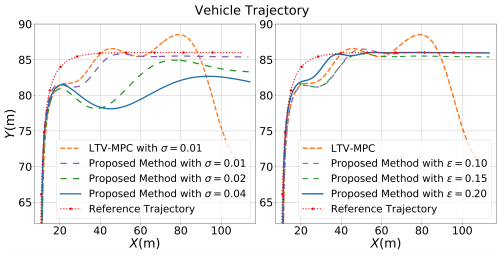


Figure 2.4: Trajectory of the vehicle for varying uncertainty σ (left) and tolerance ϵ (right).

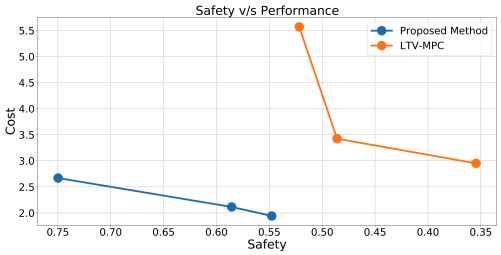


Figure 2.5: Safety v.s. performance tradeoffs.

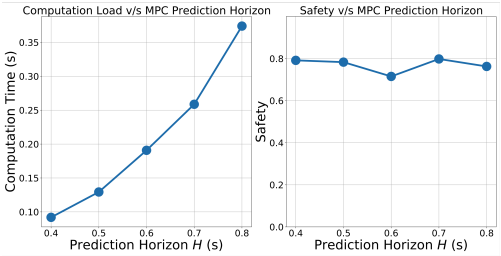


Figure 2.6: Impact of MPC time horizon H on computation load (left) and safety (right).

This is achieved because it can systematically trade-off long-term safety vs performance by varying the tolerance level ϵ. With a looser safety requirement, more aggressive control was produced to improve performance (Fig. 2.4 right).

Time horizon, computation load, and safety. Fig. 2.6 shows the effect of the MPC outlook time horizon H and resulting computation load and safety. The computation load grows with H in the order of $O(H^3)$ [57,58]. However, reducing H does not compromise safety because the proposed methods only requires myopic evaluation to achieve long-term safety.

2.5 Summary

This chapter proposes a stochastic adaptive safe control technique for adverse driving conditions that can exploit prediction, mediate behaviors based on uncertainty, and adapt to changes. We demonstrate its reliability, efficiency, and modularity through theoretical and numerical studies. The reliability is due to its provable guarantee of long-term safe probability or probabilistic

recovery speeds. The computational efficiency of imposing chance constraints in nonlinear systems is achieved through a novel use of probabilistic forward invariance conditions. Finally, the derived safety condition can be modularly integrated into existing controllers, which largely improves its applicability.

Chapter 3

Dealing with Other Agents on the Road

3.1 Background

Multi-agent autonomous systems must balance safety and performance specifications in uncertain environments with distributed control in real-time. There can be information sharing constraints between agents due to limited communication or the scale of the network. In such systems, an agent may only have access to the information of a small subset of the whole network or its neighboring agents. Despite the information sharing constraints, the safety and performance specifications are often given as global specifications that need to be ensured in the long-term. For example, swarms of autonomous agents must collaboratively achieve some common goal (*e.g.,* when a swarm of surveillance drones need to collectively cover the search areas, and when at least one robot should reach a target area to perform some tasks). Safety (*e.g.,* collision avoidance, stability) must also be satisfied at all times. Nonlinear systems can have an unsafe (unstable) region of attractions, which often cannot be avoided by myopically moving away from unsafe regions. Moreover, the environments in which these agents operate can be highly uncertain and dynamic. These uncertainties can come from a multitude of factors, arising from human and other agents' behaviors, disturbance and noise, limited communications, and unmodeled dynamics. Due to the highly dynamic nature, agents must have a fast feedback loop and respond quickly. Such latency requirements may prohibit the use of cloud

computation and delayed communication, and the agents' control actions often need to be computed using onboard hardware. To tackle these challenges, this chapter studies how to ensure long-term global objectives with information sharing constraints and limited online computation in uncertain environments.

3.1.1 Related Work

There has been great advancement in safe control techniques for uncertain or multi-agent systems in the past decade. When the control objective is to avoid obstacles (one agent crashes into another), the existing literature has proposed to use a distance-based barrier function that can be evaluated using local information [59, 60]. This approach is based on the idea that one only needs to know the distance between two agents to control their possibility of crashes. More generally, this approach works when a control objective can be translated into a local condition whose safe set is defined by a level set of decomposable Barrier or Lyapunov functions [1, 61, 62]. Here, decomposable functions refer to the ones that can be evaluated using only the information available to each agent. Although global objectives are quite common in many multi-agent systems (as stated above), this approach cannot account for global objectives that cannot be represented by non-decomposable Barrier/Lyapunov functions.

There often exists stringent tradeoffs between assuring long-term behaviors vs. computational efficiency. On one hand, there exist model prediction control and reachability-based techniques that account for future trajectories of long time horizon to ensure long-term safety [63, 64, 65]. These techniques are often computationally expensive because the space of possible trajectories exponentially increases with the horizon. To reduce the computation burden, various techniques based on barrier function approaches have been proposed to ensure short-term safety conditions myopically [9, 10, 11]. On the other hand, approaches such as stochastic control barrier functions achieve a significant reduction in computational cost due to their use of myopic controllers, but can result in unsafe behaviors in a longer time horizon due to the compounding probabilities of unsafe events [1, 14, 66, 67]. These approaches cannot control the accumulation of tail distribution and may result in small long-term safe probability. To better account for tradeoffs, we have proposed a framework to ensure long-term safe probability using myopic evaluation for fully observable centralized systems [68]. In this chapter, we will generalize

our prior work to distributed systems with information sharing constraints.

3.1.2 Contributions of This Chapter

In this chapter, we propose a stochastic safe control technique that can ensure multiple global objectives for multi-agent systems in uncertain environments. We first define a new notion of probabilistic forward invariance and forward convergence which can represent the satisfaction of safety and operational specifications with high probability. The specifications can be given global specifications in the form of unions and intersections of forward invariance and forward convergence conditions. Then, we show a sufficient condition for the probability of the control objectives to be within a desired range. This sufficient condition has two features. First, it can achieve all global objectives using local computation. The global objectives can be something that cannot be represented by decomposable barrier functions. At the same time, the condition can be used by each agent with only local information to certify the safety of an existing action or modify it to satisfy the safety and operational specifications. Second, it can achieve long-term safety or performance specifications using myopic evaluation. The specification can be defined as satisfying forward invariance condition (safety) or forward convergence condition (operational) through an outlook time horizon, while its condition can be evaluated using future evolution of an immediate next step. When the sampling frequency is sufficiently high, the certification and modification scheme can be done using a linear constraint and be integrated into a convex/quadratic program. Using this condition, we propose a distributed control algorithm for each agent: Each agent solves an optimization problem with the linear constraints; the information sharing structure or the decision of control actions has a tree structure that can accommodate the relative priority (power) between agents.

The proposed methods have the following advantages.

Advantage 1: The proposed methods can use local information to ensure global safety and performance specifications. The proposed method can be implemented in a decentralized manner: Each agent can use its local information to certify or modify its control actions based on the sufficient condition described above. If all agents can find a feasible action, the global safety or operational specifications will be satisfied with desired probabilities, even global specifications which are represented using non-decomposable Barrier or Lyapunov functions.

Advantage 2: The proposed methods can ensure long-term safety using myopic evaluation. The proposed method embeds the probability of long-term safety or performance into a Barrier-like function. This embedding allows a new notion of conditional forward invariance to be applied on the long-term probability. This new notion allows each agent to typically evaluate the outcome of the immediate future horizon, only using its local information, to ensure long term probability.

To achieve advantages 1 and 2, our novel definition of conditional probabilistic forward invariance and forward convergence condition (see section 3.2.3 for detail) is critical to achieve this property. To the best of our knowledge, there does not exist any existing methods that can achieve advantages 1 and 2 simultaneously.

3.2 Problem Statement

The notations of this chapter follow the conventions set up in section 1.2.

3.2.1 System Model

We consider a multi-agent time-invariant stochastic dynamical system with M agents. The dynamics of agent i, $i \in \{1, 2, \cdots, M\}$, is given by the stochastic differential equation (SDE):

$$dX^i = (F^i(X^i) + G^i(X^i)U^i)dt + \Sigma^i(X^i)dW^i, \tag{3.1}$$

where $X^i \in \mathbb{R}^{m^i}$ is the system state of agent i, $U^i \in \mathbb{R}^{n^i}$ is the control input of agent i, and $W^i \in \mathbb{R}^{\omega^i}$ captures the system uncertainties of agent i. We assume that W^i is the independent standard Brownian motions with 0 initial value. The value of $\Sigma^i(X^i)$ is determined based on the size of uncertainty in agent i. We assume that the dynamics of agent i does not depend on other agents. Thus, the dynamics of the entire multi-agent system can be written as

$$dX = (F(X) + G(X)U)dt + \Sigma(X)dW, \tag{3.2}$$

where

$$X = \begin{bmatrix} X^1 \\ X^2 \\ \vdots \\ X^N \end{bmatrix}, U = \begin{bmatrix} U^1 \\ U^2 \\ \vdots \\ U^N \end{bmatrix}, W = \begin{bmatrix} W^1 \\ W^2 \\ \vdots \\ W^N \end{bmatrix}, \tag{3.3}$$

and

$$F = \text{diag}(F^1, F^2, \cdots, F^M) \tag{3.4}$$

$$G = \text{diag}(G^1, G^2, \cdots, G^M) \tag{3.5}$$

$$\Sigma = \text{diag}(\Sigma^1, \Sigma^2, \cdots, \Sigma^M). \tag{3.6}$$

Let

$$m = \sum_{i=1}^{M} m^i \tag{3.7}$$

denote the dimension of the state, *i.e.,* $X \in \mathbb{R}^m$. To implement the controller in digital system, we discretize the time into sampled points of equal interval Δt, *i.e.,* $t_k = \Delta t k, \forall k \in \mathbb{Z}_+$. Accordingly, system (3.1) and (3.2) can be written in discrete-time as

$$X^i_{k+1} = \mathcal{F}^i(X^i_k, U^i_k, W^i_k) \tag{3.8}$$

and

$$X_{k+1} = \mathcal{F}(X_k, U_k, W_k), \tag{3.9}$$

respectively. With slight abuse of notation, we use X_k to denote X evaluated at time $k\Delta t$.

We assume that agent i can access the information of its own states and the states and control inputs of a few other agents. Let $\mathcal{A}^i$ be the set of agents whose states and information can be accessed by agent i. Then, the information available to agent i at time k is given by

$$Q^i_k = \{X^j_k, U^l_k : j \in \mathcal{A}^i, l \in \mathcal{A}^i \backslash \{i\}\}. \tag{3.10}$$

3.2.2 Nominal Controller

We assume the existence of a nominal controller

$$U_k^i = N^i(Q_k^i) \tag{3.11}$$

for each agent i. The nominal controller is assumed to satisfy some performance specifications, but not necessarily all safety and operational specifications, as we will introduce in section 3.2.3. The proposed framework does not restrict the choice of nominal controllers, and each agent can have different forms of nominal controllers.

3.2.3 Design Goal

Our goal is to ensure long term safety of all agents as well as satisfaction of operational specifications. We assume that there are B such specifications, indexed by $j = 1, 2, \cdots, B$, and each specification is represented as follows: at time k, specification j is defined by the event

$$\mathcal{C}_k^j = \{x \in \mathbb{R}^m : \phi_k^j(x) \geq 0\}, \tag{3.12}$$

where $\phi_k^j(x) : \mathbb{R}^m \to \mathbb{R}$ is a continuous mapping. Here, B is the number of safety/operational specifications. We consider two forms of conditions: forward invariance and forward convergence, formally defined below.

Forward Invariance

The forward invariance specifications require the condition to continuously hold. If the j-th condition is given as a forward invariance condition, its satisfaction during time horizon T_k^j is given by

$$S_k^j = \{x_\tau \in \mathcal{C}_k^j, \forall \tau \in \{k, k+1, \cdots, k+T_k^j\}\}. \tag{3.13}$$

Forward Convergence

The forward convergence specifications require the system to satisfy the condition eventually. If the j-th condition is given as a forward convergence condition, its satisfaction before time horizon T_k^j is given by

$$S_k^j = \{\exists \tau \in \{k, k+1, \cdots, k+T_k^j\} \text{ s.t. } x_\tau \in \mathcal{C}_k^j\}. \tag{3.14}$$

The overall performance specification can be represented by the intersections and/or unions of condition $S^j, j \in \{1, 2, \cdots, B\}$, denoted by S. The design goal is to satisfy the S with probability above $1 - \epsilon$ at each time k, *i.e.,*

$$\mathbb{P}(S_k) \geq 1 - \epsilon, \ \forall k \geq 0. \tag{3.15}$$

The forward invariance specifications and forward convergence specifications are combined in (4.9). This is different from existing techniques that use two separate processes. In a separate design, the control input calculated based on one specification may compromise other specifications. The advantage of combining them into one condition is to jointly account for multiple specifications of both types and not compromising any specification.

3.3 Proposed Method

Here, we present a sufficient condition to achieve the design goal in section 3.3.1 and prove its performance guarantee in section 3.3.3. Based on this condition, we propose a distributed controller in section 3.3.2.

3.3.1 Conditions to Assure Safety and Operational Specifications

In this subsection, we present a sufficient condition to satisfy the performance and safety specifications. Let

$$\Psi_k(I) := \mathbb{P}(S_k|I) \in \mathbb{R} \tag{3.16}$$

be the sequence of probability of event S_k conditioned on the information I. We define a new notion of conditional discrete-time generator as below.

Definition 3 (Conditional discrete-time generator)**.** The conditional discrete-time generator A of a discrete-time stochastic process $\{x_k\}_{k\in\mathbb{Z}_+}$ conditioned on another process $\{y_k\}_{k\in\mathbb{Z}_+}$ with sampling interval Δt evaluated at time k is given by

$$A\phi(x_k|y_k) = \frac{\mathbb{E}[\phi(x_{k+1})|y_k] - \mathbb{E}[\phi(x_k)|y_k]}{\Delta t} \tag{3.17}$$

whose domain is the set of all functions $\phi : \mathbb{R}^n \to \mathbb{R}$ of the stochastic process.

When $x_k = y_k$, this generator can be considered as the discrete-time counterpart of the continuous-time infinitesimal generator. We additionally add the conditioning of y_k in order to capture the information-sharing constraints. Although the value of $A\phi(y_k)$ depends on both x_k and y_k, with slight abuse of notation, for the rest of the chapter, we will use $A\phi(y_k)$ where the discrete-time stochastic process x_k in Definition 4 is the full state of the system, *i.e.,* X_k in (3.9).

We consider the following condition at all time k:

$$A\Psi_k(Q_k^i) \geq -\gamma(\Psi_k(Q_k^i) - (1-\epsilon)),\ \forall k \geq 0. \tag{3.18}$$

Here, $\gamma : \mathbb{R} \to \mathbb{R}$ is a function that satisfies the following 2 design requirements:

Requirement 1: $\gamma(h)$ is linear and increasing in h.

Requirement 2: $\gamma(h) \leq h$ for any $h \in \mathbb{R}$.

The probability measure of $\mathbb{P}(S_k|I)$ is taken over X, the global state, conditioned on Q^i, the information that can be accessed by agent i. Therefore, the values on both sides of (3.18) can be computed using Q^i. Thus, the form of (3.18) is advantageous in distributed networks without centralized information or computing (see section 3.3.2). Interestingly, this localizable property does not require the global safety and operational specifications S to be decomposable (*i.e.,* the design specifications S can depend on the value of all states). This is in stark contrast with the existing literature for deterministic and standard barrier functions: agent i can only evaluate the safety constraint S only depending on the information of Q^i.

Theorem 4. *Consider system* (3.8) *and* (3.9)*. We assume the initial condition $X_0 = x$ satisfies $\mathbb{P}(S_0|X_0 = x) \geq 1 - \epsilon$. If at each time k, each agent i generates a control policy that satisfies* (3.18)*, then the following condition holds:*

$$\mathbb{E}[\mathbb{P}(S_k|X_k)] \geq 1 - \epsilon,\ \forall k \geq 0. \tag{3.19}$$

Interestingly, although the conditions in (3.18) can be imposed by each agent i using its local information Q_k^i, the behavior can be guaranteed for global safety and operational specifications. The proof of theorem 4 is given in section 3.3.3.

3.3.2 Proposed Controller

To efficiently implement condition (3.18) in real time, we first show that (3.18) can be implemented as a linear function of U_k^i. We define $\Gamma_{\mathcal{D}}^i : \mathbb{R}^m \times \mathbb{R} \times \mathbb{R} \to \mathbb{R}^{\sum_{j\in\mathcal{A}^i} m^j}$ to be[1]

$$\begin{aligned}&\Gamma_{\mathcal{D}}^i(X_k, a, \delta)\\ =&\{X_k^j + \delta \mathbb{1}\{1 \le a - \sum_{l=1}^{j-1} m^l \le m^j\}\mathbf{1}_{m^j}^{[a-\sum_{l=1}^{j-1} m^l]} : j \in \mathcal{A}^i\}.\end{aligned} \tag{3.20}$$

Note that although $\Gamma_{\mathcal{D}}^i$ takes input of the state of the whole system, only the information available to agent i is required for evaluation. Let $\mathcal{D}^i(X_k)$ be defined as

$$\mathcal{D}^i(X_k) = [\mathcal{D}_{(1)}^i(X_k), \mathcal{D}_{(2)}^i(X_k), \cdots, \mathcal{D}_{(m)}^i(X_k)]^\intercal \in \mathbb{R}^m, \tag{3.21}$$

where

$$\mathcal{D}_{(a)}^i(X_k) = \frac{\Psi_k(\Gamma_{\mathcal{D}}^i(X_k, a, \Delta)) - \Psi_k(\Gamma_{\mathcal{D}}^i(X_k, a, -\Delta))}{2\Delta}. \tag{3.22}$$

Here, Δ is the step size to calculate the finite difference of Ψ_k. We additionally define $\Gamma_{\mathcal{H}}^i : \mathbb{R}^m \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \to \mathbb{R}^{\sum_{j\in\mathcal{A}^i} m^j}$ to be

$$\begin{aligned}&\Gamma_{\mathcal{H}}^i(X_k, a, b, \delta_a, \delta_b)\\ =&\{X_k^j + \delta_a \mathbb{1}\{1 \le a - \sum_{l=1}^{j-1} m^l \le m^j\}\mathbf{1}_{m^j}^{[a-\sum_{l=1}^{j-1} m^l]}\\ &+\delta_b \mathbb{1}\{1 \le b - \sum_{l=1}^{j-1} m^l \le m^j\}\mathbf{1}_{m^j}^{[b-\sum_{l=1}^{j-1} m^l]} : j \in \mathcal{A}^i\}.\end{aligned} \tag{3.23}$$

Note that although $\Gamma_{\mathcal{H}}^i$ takes input of the state of the whole system, only the information available to agent i is required for evaluation. Let

$$\begin{aligned}&\mathcal{H}^i(X_k)\\ =&\begin{bmatrix} \mathcal{H}_{(1,1)}^i(X_k) & \mathcal{H}_{(1,2)}^i(X_k) & \cdots & \mathcal{H}_{(1,m)}^i(X_k) \\ \mathcal{H}_{(2,1)}^i(X_k) & \mathcal{H}_{(2,2)}^i(X_k) & \cdots & \mathcal{H}_{(2,m)}^i(X_k) \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{H}_{(m,1)}^i(X_k) & \mathcal{H}_{(m,2)}^i(X_k) & \cdots & \mathcal{H}_{(m,m)}^i(X_k) \end{bmatrix},\end{aligned} \tag{3.24}$$

[1]Here, we use $\mathbb{R}^{\sum_{j\in\mathcal{A}^i} m^j}$ to denote the set that has $\sum_{j\in\mathcal{A}^i} m^j$ real elements.

where

$$\begin{aligned}\mathcal{H}^i_{(a,b)}(X_k) =& \frac{1}{\Delta^2}(\Psi_k(\Gamma^i_{\mathcal{H}}(X_k, a, b, \Delta, \Delta)) \\ &- \Psi_k(\Gamma^i_{\mathcal{H}}(X_k, a, b, -\Delta, \Delta)) \\ &- \Psi_k(\Gamma^i_{\mathcal{H}}(X_k, a, b, \Delta, -\Delta)) \\ &+ \Psi_k(\Gamma^i_{\mathcal{H}}(X_k, a, b, -\Delta, -\Delta))). \end{aligned} \tag{3.25}$$

Lemma 3. *If the limit of* $\lim_{\Delta t\to 0} A\Psi_k(Q^i_k)$ *exists, the following condition holds:*

$$\begin{aligned}\lim_{\Delta t\to 0} A\Psi_k(Q^i_k) = \lim_{\Delta\to 0}(&\mathcal{D}^i(X_k)\cdot(F(X_k)+G(X_k)U_k) \\ &+ \frac{1}{2}\operatorname{tr}(\Sigma^\intercal(X_k)\mathcal{H}^i(X_k)\Sigma(X_k))). \end{aligned} \tag{3.26}$$

Remark 4. The function $\Psi_k(x)$ can be smooth even when $\phi(x)$ is not differentiable. For example, consider the case with system (3.2) with $F = -\frac{1}{2}X$, $G = 0$ and $\Sigma = 2$. The system is discretized with $\Delta t = 0.1$. As an example, we define 3 barrier functions:

$$\phi_1(x) = -x^2 - 1 \tag{3.27}$$

$$\phi_2(x) = \frac{1}{2}x - 1 \tag{3.28}$$

$$\phi_3(x) = \sin(x), \tag{3.29}$$

and specify a composition of $\phi_1(x)$, $\phi_2(x)$, and $\phi_3(x)$, given by

$$\phi(x) = \min(\max(\phi_1(x), \phi_2(x)), \phi_3(x)). \tag{3.30}$$

Observe that $\phi(x)$ is not differentiable. However,

$$\Psi(x) = \mathbb{P}(\phi(X_\tau) \geq 0, \forall\tau \in \{1, 2, \cdots, 10\} | X_0 = x) \tag{3.31}$$

is smooth, as shown in fig. 3.1.

For each agent i, if the information of the a-th entry of X is not accessible, then the a-th entry of $\mathcal{D}^i$ will be 0. Similarly, if either information of the a-th or b-th entry of X is not accessible, then the (a, b)-th entry of $\mathcal{H}^i$ will be 0. Therefore, (3.26) can be evaluated using only the local information available to agent i and the current control action of other agents whose states are

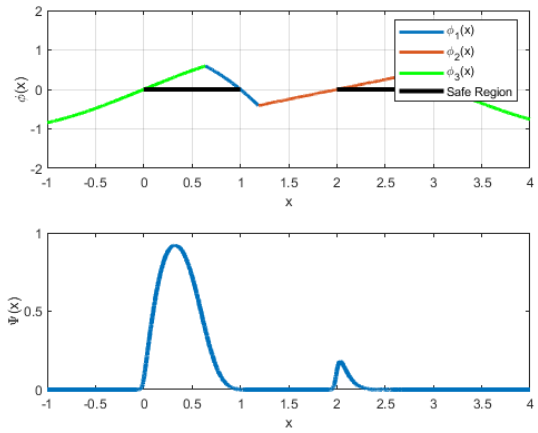


Figure 3.1: Min and max composition of 3 barrier functions. Note that although $\phi(x)$ (top plot) is not differentiable, the probabilistic formulation $\Psi(x)$ (bottom plot) is smooth.

available to agent i, *i.e.*, $\{U_k^j : j \in \mathcal{A}^i\}$. Since the control action of agent i is computed based on the control actions of other agents, the control actions of agents must be available in an order such that later agents can compute their control actions based on previously available control actions. To calculate (4.10) using the state information of the agents whose control actions are not available yet and ensure that there exist feasible control actions for these agent, we assume the existence of another controller:

$$U_k^i = R^i(Q_k^i). \tag{3.32}$$

This controller can be considered to be a controller that is conservative in terms of performance. With this controller, we propose a cascading architecture. We assume that there exists a way to rank all agents such that agent i computes its control action using its own state measurement, and the state measurements and control actions of a subset of agents j, $1 \leq j < i$. Based on theorem 4 and lemma 3, we propose the following constrained optimization

problem to find the control action. Each agent i uses Q_k^i to solve

$$\begin{aligned} U_k^i = \arg\min_{u^i} \; & J^i(N(Q_k^i), u^i) \\ \text{s.t. } & \mathcal{D}^i(X_k) \cdot (F(X_k) + G(X_k)u) \\ & + \frac{1}{2}\operatorname{tr}(\Sigma^\intercal(X_k)\mathcal{H}^i(X_k)\Sigma(X_k)) \\ & \geq -\gamma(\Psi_k(Q_k^i) - (1-\epsilon)) \\ & u^j = 0, \; \forall j \notin \mathcal{A}^i. \end{aligned} \tag{3.33}$$

Here, u contains the control actions of all agents and u^i is the control action of agent i. When computing (4.10), the agents with index $j < i$ are assumed to use the nominal control action N^j, while the agents with index $j > i$ are assumed to use R^j. The mapping $J^i : \mathbb{R}^{n^i} \times \mathbb{R}^{n^i} \to \mathbb{R}$ is an objective function that penalizes the derivation from the nominal controller policy for agent i. Additional constraints can be added to the optimization problem (3.33) to account other constraints, such as actuation limits. The proposed algorithm is shown in algorithm 2.

Remark 5. Although the input of $\mathcal{D}^i$ and $\mathcal{H}^i$ is the full state X_k, they can be evaluated using Q_k^i only, as defined in (3.20) to (3.25). Therefore, the constraint of (3.33) can be evaluated using local information Q_k^i only.

Algorithm 2 Proposed control algorithm

```
k ← 0
while k < K_max do
    for i = 1 : M do
        Obtain Q_k^i
        Receive U_k^l, l ∈ A^i\{i}
        Find U_k^i ← solve {u^i in (3.33)}
    end for
    Execute control actions U_k^i, 1 ≤ i ≤ M
    k ← k + 1
end while
```

Remark 6. In algorithm 2, agents with larger indexes make decisions based on the actions of agents with smaller indexes, so agents with smaller index gets more priority in decision making. Apart from this priority hierarchy, the

information sharing structure can also take forms of general tree structures, where the agents on the child nodes make decisions based on the actions of all the nodes on the path to the root node. There exists multiple ways to structure the information sharing structure and choose priorities for agents. One example is based on the physics of the system (*e.g.,* in a truck platooning system, the vehicles in behind make control decisions based on the vehicles before them). Another example is based on pre-defined priority (*e.g.,* in an intersection, emergency vehicles such as ambulance have higher priority in making control decisions compared to other vehicles).

3.3.3 Proof of Theorem 4

Lemma 4. *Let S be an event with marginal probability $\mathbb{P}(S)$ and conditional probability $\mathbb{P}(S|Y)$, where Y is a random variable with probability density function $f_Y(y)$. Then, we have the following condition.*

$$\mathbb{E}[\mathbb{P}(S|Y)] = \mathbb{P}(S). \tag{3.34}$$

Proof (lemma 4). We have

$$\begin{aligned}\mathbb{E}[\mathbb{P}(S|Y)] &= \int_{-\infty}^{\infty} \mathbb{P}(S|Y=y) f_Y(y) dy && (3.35)\\ &= \mathbb{P}(S) && (3.36)\end{aligned}$$

due to the law of total probability. ■

Proof (theorem 4). We first show that

$$\mathbb{E}[\Psi_k(X_k)] = \mathbb{E}[\Psi_k(Q_k^i)],\ \forall i \in \{1, 2, \cdots, M\}. \tag{3.37}$$

We have

$$\begin{aligned}&\mathbb{E}[\Psi_k(X_k)]\\ =&\mathbb{E}[\mathbb{P}(S_k|X_k)] && (3.38)\\ =&\mathbb{P}(S_k) && (3.39)\\ =&\mathbb{E}[\mathbb{P}(S_k|Q_k^i)],\ \forall i \in \{1, 2, \cdots, M\} && (3.40)\\ =&\mathbb{E}[\Psi_k(Q_k^i)],\ \forall i \in \{1, 2, \cdots, M\}. && (3.41)\end{aligned}$$

Here, (3.38) and (3.41) is due to definition (4.10), and (3.39) and (3.40) is due to lemma 4. Therefore, for all $i \in \{1, 2, \cdots, M\}$, we have

$$\begin{aligned}
&\mathbb{E}[-\gamma(\Psi_k(Q_k^i) - (1-\epsilon))] \\
=&-\gamma(\mathbb{E}[\Psi_k(Q_k^i)] - (1-\epsilon)) && (3.42)\\
=&-\gamma(\mathbb{E}[\Psi_k(X_k)] - (1-\epsilon)) && (3.43)\\
=&\mathbb{E}[-\gamma(\Psi_k(X_k) - (1-\epsilon))]. && (3.44)
\end{aligned}$$

Here, (3.42) and (3.44) is due to design requirement 1. In addition, for all $i \in \{1, 2, \cdots, M\}$, we have

$$\begin{aligned}
&\mathbb{E}[A\Psi_k(Q_k^i)] \\
=&\mathbb{E}[\frac{\mathbb{E}[\Psi_{k+1}(X_{k+1})|Q_k^i] - \mathbb{E}[\Psi_k(X_k)|Q_k^i]}{\Delta t}] && (3.45)\\
=&\frac{\mathbb{E}[\mathbb{E}[\Psi_{k+1}(X_k^i)|Q_k^i]]}{\Delta t} - \frac{\mathbb{E}[\mathbb{E}[\Psi_k(X_k^i)|Q_k^i]]}{\Delta t} && (3.46)\\
=&\frac{\mathbb{E}[\Psi_{k+1}(X_{k+1})]}{\Delta t} - \frac{\mathbb{E}[\Psi_k(X_k)]}{\Delta t} && (3.47)\\
=&\frac{\mathbb{E}[\mathbb{E}[\Psi_{k+1}(X_{k+1})|X_k]]}{\Delta t} - \frac{\mathbb{E}[\Psi_k(X_k)]}{\Delta t} && (3.48)\\
=&\mathbb{E}[\frac{\mathbb{E}[\Psi_{k+1}(X_{k+1})|X_k] - \Psi_k(X_k)}{\Delta t}] && (3.49)\\
=&\mathbb{E}[A\Psi_k(X_k)]. && (3.50)
\end{aligned}$$

Here, (3.45) and (3.50) is due to (4.11), and (3.47) and (3.48) is due to the law of total expectation. From (3.44) and (3.50), we know that

$$\mathbb{E}[A\Psi_k(Q_k^i)] \geq \mathbb{E}[-\gamma(\Psi_k(Q_k^i) - (1-\epsilon))] \tag{3.51}$$

implies

$$\mathbb{E}[A\Psi_k(X_k)] \geq \mathbb{E}[-\gamma(\Psi_k(X_k) - (1-\epsilon))]. \tag{3.52}$$

Here, (3.51) holds because of safety condition (3.18).

Next, we use mathematical induction to prove (4.13). Condition (4.13) holds for $k = 0$ due to the assumption on initial condition. We suppose (4.13) holds at time $k > 0$, and show (4.13) holds at time $k + 1$. Let

$$\mathbb{E}[\Psi_k(X_k)] = \mathbb{E}[\mathbb{P}(S_k|X_k)] = 1 - \epsilon + h \tag{3.53}$$

for some $h > 0$. We define the set of events V_i and variables $v_i, h_i,$ and δ_i, $i \in \{0, 1\}$, as follows:

$$V_0 = \{\Psi_k(X_k) < 1 - \epsilon\}, \tag{3.54}$$
$$V_1 = \{\Psi_k(X_k) \geq 1 - \epsilon\}, \tag{3.55}$$
$$v_0 = \mathbb{E}[\Psi_k(X_k) \mid V_0] = 1 - \epsilon - \delta_0, \tag{3.56}$$
$$v_1 = \mathbb{E}[\Psi_k(X_k) \mid V_1] = 1 - \epsilon + \delta_1, \tag{3.57}$$
$$h_0 = \mathbb{P}(V_0), \tag{3.58}$$
$$h_1 = \mathbb{P}(V_1). \tag{3.59}$$

The left hand side of (3.53) can then be written as

$$\begin{aligned} &\mathbb{E}[\Psi_k(X_k)] \\ =&\mathbb{E}[\Psi_k(X_k) \mid V_0]\,\mathbb{P}(V_0) + \mathbb{E}[\Psi_k(X_k) \mid V_1]\,\mathbb{P}(V_1) \\ =&v_0 h_0 + v_1 h_1. \end{aligned} \tag{3.60}$$

From

$$\begin{aligned} \mathbb{E}[\Psi_k(X_k) \mid V_0] < 1 - \epsilon, \\ \mathbb{E}[\Psi_k(X_k) \mid V_1] \geq 1 - \epsilon, \end{aligned} \tag{3.61}$$

we obtain

$$\delta_0 \geq 0 \tag{3.62}$$

and

$$\delta_1 \geq 0. \tag{3.63}$$

Moreover, $\{h_i\}_{i \in \{0,1\}}$ satisfies

$$\mathbb{P}(V_0) + \mathbb{P}(V_1) = h_0 + h_1 = 1. \tag{3.64}$$

Combining (3.53) and section 3.3.3 gives

$$1 - \epsilon + h = v_0 h_0 + v_1 h_1. \tag{3.65}$$

Applying (3.56) and (3.57) to (3.65) gives

$$1 - \epsilon + h = (1 - \epsilon - \delta_0)\, h_0 + (1 - \epsilon + \delta_1)\, h_1, \tag{3.66}$$

which, combined with (3.64), yields

$$h = \delta_1 h_1 - \delta_0 h_0. \tag{3.67}$$

On the other hand, we have

$$\begin{aligned}
&\mathbb{E}\left[\gamma\left(\Psi_k(X_k) - (1-\epsilon)\right)\right] \\
=&\mathbb{P}(V_0)\left(\mathbb{E}\left[\gamma\left(\Psi_k(X_k) - (1-\epsilon)\right) \mid V_0\right]\right) \\
&+ \mathbb{P}(V_1)\left(\mathbb{E}\left[\gamma\left(\Psi_k(X_k) - (1-\epsilon)\right) \mid V_1\right]\right) && (3.69)\\
=&h_0\left(\mathbb{E}\left[\gamma\left(\Psi_k(X_k) - (1-\epsilon)\right) \mid V_0\right]\right) \\
&+ h_1\left(\mathbb{E}\left[\gamma\left(\Psi_k(X_k) - (1-\epsilon)\right) \mid V_1\right]\right) && (3.70)\\
=&h_0\left(\gamma\left(\mathbb{E}\left[\Psi_k(X_k) - (1-\epsilon) \mid V_0\right]\right)\right) \\
&+ h_1\left(\gamma\left(\mathbb{E}\left[\Psi_k(X_k) - (1-\epsilon) \mid V_1\right]\right)\right) && (3.71)\\
=&h_0\left(\gamma\left(-\delta_0\right)\right) + h_1\left(\gamma\left(\delta_1\right)\right) && (3.72)\\
=&\gamma\left(-h_0\delta_0 + h_1\delta_1\right) && (3.73)\\
=&\gamma(h) && (3.74)\\
\leq& h. && (3.75)
\end{aligned}$$

Here, section 3.3.3 is due to (3.58) and (3.59); section 3.3.3 is obtained from design requirement 1; section 3.3.3 is based on (3.56) and (3.57); section 3.3.3 is due to design requirement 1 and (3.64); section 3.3.3 is due to (3.67); and (3.75) is due to design requirement 2. From section 3.3.3 to section 3.3.3, we have

$$\mathbb{E}\left[-\gamma\left(\Psi_k(X_k) - (1-\epsilon)\right)\right] \geq -h. \tag{3.76}$$

Recall that the control action is chosen to satisfy section 3.3.1. Now, we take the expectation over both side of section 3.3.1 to obtain

$$\mathbb{E}[A\Psi_k(X_k)] \geq \mathbb{E}[-\gamma(\Psi_k(X_k) - (1-\epsilon))]. \tag{3.77}$$

From (4.11), we have

$$A\Psi_k(X_k) = \frac{\mathbb{E}[\Psi_{k+1}(X_{k+1}) - \Psi_k(X_k)|X_k]}{\Delta t}. \tag{3.78}$$

Therefore, (3.77) can be written as

$$\begin{aligned}
&\frac{\mathbb{E}[\mathbb{E}[\Psi_{k+1}(X_{k+1}) - \Psi_k(X_k)|X_k]]}{\Delta t} \\
\geq&\mathbb{E}[-\gamma(\Psi_k(X_k) - (1-\epsilon))].
\end{aligned} \tag{3.79}$$

Using the law of total expectation, we have

$$\begin{aligned}&\frac{\mathbb{E}[\Psi_{k+1}(X_{k+1}) - \Psi_k(X_k)]}{\Delta t}\\ \geq&\mathbb{E}[-\gamma(\Psi_k(X_k) - (1-\epsilon))].\end{aligned} \tag{3.80}$$

Combining (3.53), (3.76), section 3.3.3 and design requirement 2 yields

$$\begin{aligned}&\mathbb{E}[\Psi_{k+1}(X_{k+1})]\\ \geq&\mathbb{E}[\Psi_k(X_k)] + \mathbb{E}[-\gamma(\Psi_k(X_k) - (1-\epsilon))]\Delta t &(3.81)\\ \geq&1 - \epsilon + h - h\Delta t &(3.82)\\ =&1 - \epsilon + h(1 - \Delta t). &(3.83)\end{aligned}$$

Since $\Delta t \ll 1$ and $h \geq 0$, we have

$$\mathbb{E}[\Psi_{k+1}(X_{k+1})] \geq 1 - \epsilon. \tag{3.84}$$

■

3.4 Deployment and Experiment

In this section, we test the empirical performance of the proposed method using numerical simulation of the deployment environment. We consider a multi-agent system whose setting resembles the group robot operations. Examples of such operations include warehouse robots operations and swarm vehicle operations. The simulation runs for a total time of t_{max}. The system consists a total of M autonomous agents. Let superscript i denote the i-th agent. All agents are governed by the following nonlinear dynamical system:

$$dp_t^{xi} = v_t^i \cos(\theta_t^i)dt \tag{3.85}$$
$$dp_t^{yi} = v_t^i \sin(\theta_t^i)dt \tag{3.86}$$
$$dv_t^i = a_t^i dt + \sigma^{vi} dW^{vi} \tag{3.87}$$
$$d\theta_t^i = \phi_t^i dt + \sigma^{\phi i} dW^{\phi i}, \tag{3.88}$$

where p^{xi} and p^{yi} are the position, v^i is the speed, θ^i is the heading angle, a^i is the acceleration, and ϕ^i is the steering rate. The amount of uncertainty

is characterized by W^{vi} and $W^{\phi i}$, which we assume are the independent Brownian motions with 0 initial value. For all $i \in \{1, 2, \cdots, M\}$, let

$$X_t^i := \begin{bmatrix} v_t^i \\ \theta_t^i \end{bmatrix}, U_t^i := \begin{bmatrix} a_t^i \\ \phi_t^i \end{bmatrix}, W^i := \begin{bmatrix} W^{vi} \\ W^{\phi i} \end{bmatrix}$$
$$G^i := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Sigma^i := \begin{bmatrix} \sigma^{vi} & 0 \\ 0 & \sigma^{\phi i} \end{bmatrix}. \tag{3.89}$$

Thus, (3.87) and (3.88) can be written as

$$dX_t^i = G^i U_t^i dt + \Sigma^i dW^i. \tag{3.90}$$

To implement the controller in digital system, we discretize the time into sampled points of equal interval Δt, *i.e.,* $t_k = k\Delta t, \forall k \in \mathbb{Z}_+$, such that (3.90) can be written in discrete time as

$$X_{k+1}^i = \mathcal{F}^i(U_k^i, W_k^i). \tag{3.91}$$

Let p_0^{xi} and p_0^{yi} be the starting point of agent i, and p_{goal}^{xi} and p_{goal}^{yi} be the goal of agent i. The set of agents whose information is available to agent i at time k is given by

$$\mathcal{A}_k^i = \{j : \sqrt{(p_k^{xi} - p_k^{xj})^2 + (p_k^{yi} - p_k^{yj})^2} \leq r\}, \tag{3.92}$$

where r is the maximum range that an agent can broadcast its state and control action information. The operational goal for each agent i is to follow a reference trajectory X^{ri} that enables them to reach the goal, *i.e.,*

$$X_k^{ri} = \begin{bmatrix} v_{max} \\ \text{atan2}(\frac{p_{goal}^{yi} - p_k^{yi}}{p_{goal}^{xi} - p_k^{xi}}) \end{bmatrix}, \tag{3.93}$$

where v_{max} is the maximum speed. The nominal controller aims to follow this reference using a proportional controller, *i.e.,*

$$N^i(Q_k^i) = K(X_k^i - X_k^{ri}), \ \forall i \in \{1, 2, \cdots, M\}, \tag{3.94}$$

where K is the controller gain. In addition to the nominal controller, which is considered to give the most aggressive control action, we also assume there

exists a controller that gives the most conservative control action. One example is a controller that makes the vehicle decelerate in the maximum rate, *i.e.,*

$$R^i(X_k^i) = \begin{bmatrix} -\text{sign}(v_k^i)a_{max} \\ 0 \end{bmatrix}, \ \forall i \in \{1, 2, \cdots, M\}, \tag{3.95}$$

where a_{max} is the maximum acceleration rate. In addition to the aforementioned agent, we also add an agent, labeled $M+1$, who does not execute safe control policies and whose state is completely unobservable to other agents. However, the other agents knows the initial location, the system dynamics, and the control policy of this agent. Specifically, the system dynamics of this agent is identical to other agents except for having larger uncertainties, and the control policy is identical to the nominal control policy for the other agents, given in (3.94). The safety specification for all agent is given by

$$\begin{aligned} &S_k = \{\sqrt{(p_\tau^{xi} - p_\tau^{xj})^2 + (p_\tau^{yi} - p_\tau^{yj})^2} \geq l, \\ &\forall \tau \in \{k, k+1, \cdots, k+T\}, i, j \in \{1, 2, \cdots, M\}, i \neq j\}, \end{aligned} \tag{3.96}$$

where l is the lowest safe distance, and T is the outlook time horizon. We implement the controller based on Algorithm 2. The objective function in (3.33) is given by

$$J^i(N(Q_k^i), u^i) = ||N(Q_k^i) - u^i||_2, \ \forall i \in \{1, 2, \cdots, M\}. \tag{3.97}$$

The key simulation parameters are shown in Table 3.1. In the simulation, we use

$$\gamma(h) = h - 10. \tag{3.98}$$

Using the same randomly generated starting points and goals, we run simulation with the nominal controller and the proposed control policy. The results are illustrated in Figure 3.2, and Figure 3.3. A video of the simulation showing the evolution of the trajectories is available at `https://github.com/haomingj/Probabilistic-Safety-Certificate-for-Multi-agent-Systems`.

Analysis. The proposed controller is able to ensure safety while preserving the performance of the system. This is shown in Figure 3.2, where all vehicles reach their goals in the simulation time. In addition, in Figure 3.3, the successful achievement of the safety objective at all times shows

Parameter	Value	Parameter	Value
Δt	0.01	T	100
K	1	l	0.5
r	10	v_{max}	10
a_{max}	20	ϵ	0.15
M	15	t_{max}	20
$\sigma^{vi},\ \forall i$	2	$\sigma^{\phi i},\ \forall i$	2

Table 3.1: Key parameters in the simulation.

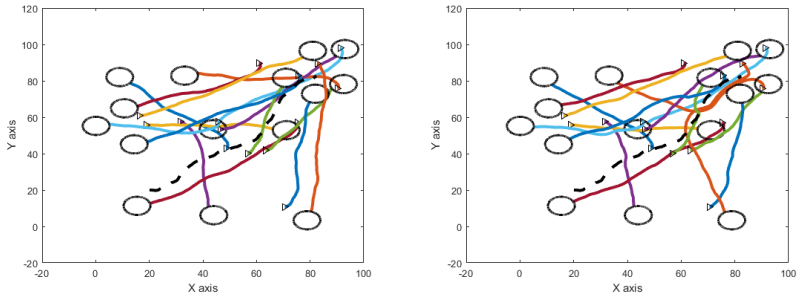


Figure 3.2: Agent trajectories with nominal controller (left) and proposed controller (right). The triangles show the starting point and direction for the agents and the circles show the goal regions. The dashed line shows the trajectory of the unobservable agent. All agents reach their goals within simulation time.

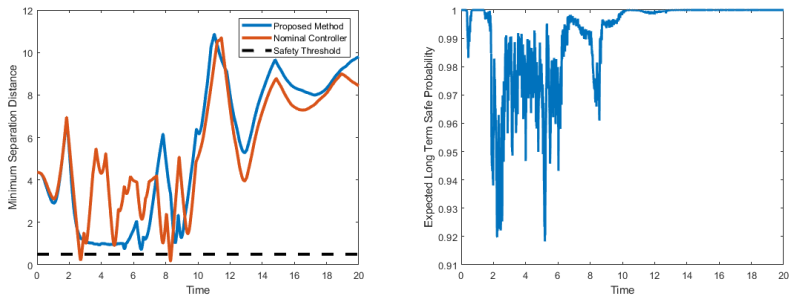


Figure 3.3: The minimum distance between any 2 agents (including the unobservable agent) for the nominal controller and the proposed controller (left) and the expected long term safe probability of the proposed method (right). For the nominal controller, the safety specification is violated several times. For the proposed controller, the safety specification is never violated, and the expected safe probability is maintained over $1 - \epsilon$.

the proposed controller's ability to maintain safety under a few challenging conditions. Firstly, the system (3.85) to (3.88) is nonlinear. Secondly, the agents only have partial system state information specified in $\mathcal{A}^i$ and cannot evaluate the full safety condition. The state information of one of the agent is completely inaccessible to other agents, which breaks of the assumptions of many existing method since the barrier function cannot be explicitly evaluated. Thirdly, the safety condition is composed of multiple barrier functions representing the distance between all agent pairs. This barrier function can be non-differentiable with respect to state since the closest agent to ego agent may change any time. Since most existing methods are not designed to ensure long term safety and performance under uncertainty as well as incorporating a binary composition of multiple barrier functions that can only be evaluated locally based on partial information or cannot be explicitly evaluated, comparison with existing methods is not included in the simulation.

3.5 Summary

In this chapter, we propose a safety certificate for multi-agent systems that ensures long term safety and performance using myopic controllers, achieves safety without overly compromising performance, and provides global guar-

antee on safety and performance conditions that can not be sufficiently evaluated with the information locally available to each agent. We verify the effectiveness of the proposed method in a simulation setting concerning group robot operation.

Chapter 4

Dealing with Vehicle Occlusions

4.1 Background

Visual occlusions impose huge challenges to autonomous driving because most sensors can not see through opaque objects, leading to large unobserved regions and potentially unsafe behaviors of the ego vehicle [69, 70]. Besides, the stochastic nature of all road users (other vehicles, pedestrians, *etc.*) introduces uncertainties into the system, which further increases the difficulty of dealing with occlusions [71]. Given such uncertainties caused by occlusions and complex interactions between road users, designing a safe controller for the ego vehicle is very difficult [72]. In this study, we focus on the problem of safe autonomous driving under scenarios with visual occlusions. The challenges of this problem include:

1. It is hard to control the level of safety of autonomous vehicles when there are visual occlusions and potential interactions with other road users, because the latent risks are difficult to measure [73];

2. Considering all aspects of the uncertainties in the system with long time horizons could be computationally intractable, which imposes difficulties for applications in real-world scenarios [74];

3. Approximately accounting for the latent risks will lead to over-conservative behaviors which compromise performance to certain extents [75].

4.1.1 Related Works

Previous studies for the safe control of vehicles in the presence of occlusions can be categorized into the following approaches.

1. External perception from infrastructures. With external perceptions from infrastructures, the autonomous vehicle directly gets information from other vehicles behind the occlusion, thus can execute safe control [76]. However, such pervasive perception requires expensive infrastructure systems, but autonomous vehicles may also need to operate in regions when such infrastructure is unavailable. The proposed method compasses this issue by leveraging the system model and data to acquire the latent risk of any given road situation with only onboard sensors.

2. Learning-based control. The learning-based method leverages the data from expert drivers and builds a mapping from the vehicle sensory input to the desired control of the vehicle [77, 78]. Even if the amount of data is enormous, generalization to the different scenarios is not guaranteed. The relationship between occlusion and vehicle motion is obscure due to the black-box nature of neural networks. In comparison, the proposed method characterizes the exact risk of different scenarios and can produce desired safety probability as specified.

3. Partially observed Markov decision process (POMDP). POMDP uses a belief state to represent the latent dynamics of occluded vehicles and solve the optimal control [79]. This framework considers the uncertainty of perception, but the computation is expensive for continuous control and often cannot be implemented in real-time [71]. On the other hand, the proposed method only requires solving a quadratic program to get the vehicle control, which has efficient online implementation.

4.1.2 Contributions of This Chapter

To resolve the aforementioned issues, we propose a model-based probabilistic safe control strategy to regulate the vehicle's speed and steering profiles under visual occlusions. Inspired by [80], the proposed method encodes future safety information into a probability value and imposes a linear constraint on the control input to guarantee the long-term safety of the system. The resulting

Table 4.1: Features of the existing methods and the proposed method.

Method	On-board sensing	Transparency in design	Real-time computation
Infrastructures		✓	✓
Learning-based	✓		✓
POMDP	✓	✓	
Proposed	✓	✓	✓

optimization-based controller can be solved efficiently via quadratic programs (QPs) while meeting other goals and constraints. The technical merits of the proposed method are

1. Guaranteed long-term safety accounting for latent risks that are invisible and occluded (see Theorem 4.3.1).

2. Balancing competing for safety and performance objectives, ensuring robustness to large uncertainty without being over-conservative (see Fig. 4.7 and Fig. 4.8).

3. Ease of design and transparency to the exposed risks (see the proposed optimization-based controller (4.17), remark 7 and remark 8).

4. Fast real-time response that ensures long-term safety using onboard resources (see section 4.4.2 for real-time hardware implementation).

The features of the proposed method compared to the existing methods is summarized in table 4.1.

The rest of the chapter is organized as follows. In section 4.2, we formulate the safe control problem of interest, in section 4.3, we introduce the proposed occlusion-aware control framework, and in section 4.4 we present the numerical and on-board simulations to validate the proposed method, and at the end, we present a summary of this chapter in section 4.5.

4.2 Problem Statement

In this section, we introduce the general problem statement, which includes the vehicle dynamics in section 4.2.1, interaction model in section 4.2.2, the occlusion model in 4.2.3, and the safety specifications in section 4.2.4.

4.2.1 System Model

We consider a general discrete-time control-affine dynamical model for the vehicle as follows:

$$x_{k+1} = f(x_k) + g(x_k)u_k \tag{4.1}$$

where $x \in \mathbb{R}^n$ is the vehicle's state, $u \in \mathbb{R}^m$ is the control input, and $f : \mathbb{R}^n \to \mathbb{R}^n$ and $g : \mathbb{R}^n \to \mathbb{R}^{n \times m}$ encompass the system dynamics, and k is the time step. We consider discrete-time dynamics throughout the chapter because all real-world vehicle controls are achieved with digital systems. One can discretize any continuous dynamics into the form of (4.1) as in [81]. The choice of model can range from simple double-integrators [82] to complete 6 DoF models [55]. The control action u is determined by a predetermined control law $N : \mathbb{R}^n \to \mathbb{R}^m$:

$$u = N(x) \tag{4.2}$$

This nominal controller will satisfy desired performance specifications, such as ensuring that the vehicle follows a planned trajectory and can be obtained via MPC, back-stepping, machine learning, or other techniques but may not guarantee safety. The closed-loop vehicle dynamics with the nominal controller will be:

$$x_{k+1} = f(x_k) + g(x_k)N(x_k) \tag{4.3}$$

The specific realizations of the vehicle model and the nominal controller for experiments are introduced in section 4.4.

4.2.2 Interaction Model

We model road users' behavior as a combination of decision-making and motion dynamics. The decision-making model characterizes the high-level decisions of the agent based on the surrounding situation and the context. Let $X \in \mathbb{R}^z$ be the joint state of all agents involved in the interaction, $\mathcal{Z}$ be the external factors that affect the decision-making, such as physical context, traffic characteristic and social contexts, as described in [83], and D be the decision-making function that outputs a distribution of the intentions of the agent (e.g., go/wait, lane-keep/lane-change) with respect to the joint state

X conditioned on the context $\mathcal{Z}$. The general decision-making process can be formulated as follows:

$$d_k \sim D(X_k|\mathcal{Z}_k) \tag{4.4}$$

where d is the road users' decision, and we assume that d can take on a finite number of decision values. In practice, this decision-making process can be modeled as a finite state machine [84], a POMDP [85], an interactive multiple model (IMM) filter [86], or a neural network [87].

The motion model characterizes the agents' behavior given the intention d. Specifically, the motion model is written as:

$$X_{k+1} \sim f_z(X_k \mid d_k) \tag{4.5}$$

where f_z is the distribution of the state update function of the agents. Previous studies have used social force model [88] and recurrent neural network [89] to represent the motion model f_z of the road users. For a given decision d, many models assume that f_z for each state X follows a Gaussian distribution, as different sources of noise and uncertainties will add up to a Gaussian due to the Central Limit Theorem [90]. The specific formulation of the interaction model used for the case study is described in section 4.4.

4.2.3 Occlusion Model

Occlusion is defined by the space where the ego vehicle is not visible. Visibility here broadly includes images and videos, radars, sonars and other sensing devices. Occlusion $\mathcal{H}_k$ is defined in map space $\mathcal{M}$, and $\mathcal{O}_t$ is the occupied space by objects and $\mathcal{V}(x(k), \mathcal{O}_k)$ is the visible space in the field of view (FOV) of the ego vehicle at time k. Then the occlusion $\mathcal{H}_k$ is defined as follow:

$$\mathcal{H}_k = (\bar{\mathcal{O}}_k \cap \bar{\mathcal{V}}(x(k), \mathcal{O}_k)) \in \mathcal{M} \tag{4.6}$$

where $\bar{\mathcal{O}}$ and $\bar{\mathcal{V}}$ are the exclusive space of $\mathcal{O}$ and $\mathcal{V}$ from the map space $\mathcal{M}$, and the occlusion $\mathcal{H}_k$ is the space excluding obstacle and visible spaces in the map. In Eq. (4.6), the method for identifying $\mathcal{O}_k$ and $\mathcal{V}(x(k), \mathcal{O}_k)$ is highly dependent on the configuration of the sensor. With the use of LiDAR, it is typical that $\mathcal{O}_k$ is detected using neural networks [91], and $\mathcal{V}(x(k), \mathcal{O}_k)$ is calculated virtually by ray casting algorithm [92]. Although it is expected

that the infrastructure-to-vehicle (I2V) or vehicle-to-vehicle(V2V) communication systems can compensate a part of the occlusion [76], not all occlusions can be covered in various driving scenes. Occlusion detection is out of scope in this chapter. However, the proposed method can incorporate the size and shape of the detected occlusion as parameters.

4.2.4 Safety Specification

Our goal is to ensure the long-term safety of all road users. We assume that there are B safety specifications for the overall interaction system, indexed by $j \in \{1, 2, \cdots, B\}$, and each specification is represented as follows: specification j is defined by the event

$$\mathcal{C}_j = \{X \in \mathbb{R}^z : \phi_j(X) \geq 0\}, \tag{4.7}$$

where $\phi_j(X) : \mathbb{R}^z \to \mathbb{R}$ is a continuous mapping. The definition can capture various safety requirements in autonomous driving, e.g., all road users do not collide with each other, and the vehicle's speed should be less than a certain value when it is close to other vehicles. Let

$$S = \{X_\tau \in \mathcal{C}_j, \forall \tau \in \{k, k+1, \cdots, k+T\}, \forall j\}, \tag{4.8}$$

where T is the outlook time horizon. The long-term safety we aim to ensure is defined as

$$\mathbb{P}(S) \geq 1 - \epsilon, \ \forall k \geq 0. \tag{4.9}$$

We will present the specific choice of safe event used in the experiments in section 4.4.

4.3 Proposed Method

In this section, we present the safe condition to ensure long-term safety in subsection 4.3.1 and its realization as the safe occlusion-aware control algorithm in subsection 4.3.2.

4.3.1 Condition for Assuring Safety

In this subsection, we present a sufficient condition for the long-term safety specifications (4.9). Let

$$\Psi(I) := \mathbb{P}(S|I) \in \mathbb{R} \tag{4.10}$$

be the sequence of probability of event S conditioned on the information I. We define a new notion of conditional discrete-time generator as below.

Definition 4. (Conditional discrete-time generator). The conditional discrete-time generator A of a discrete-time stochastic process $\{x_k\}_{k\in\mathbb{Z}_+}$ conditioned on another process $\{y_k\}_{k\in\mathbb{Z}_+}$ with sampling interval Δt evaluated at time k is given by

$$A\phi(x_k|y_k) = \frac{\mathbb{E}[\phi(x_{k+1})|y_k] - \mathbb{E}[\phi(x_k)|y_k]}{\Delta t} \tag{4.11}$$

whose domain is the set of all functions $\phi : \mathbb{R}^n \to \mathbb{R}$ of the stochastic process.

When $x_k = y_k$, this generator becomes the discrete-time counterpart of the continuous-time infinitesimal generator. We add the conditioning of y_k to capture the ego vehicle's limited information due to occlusions. Although the value of $A\phi(y_k)$ depends on both x_k and y_k, with a slight abuse of notation, for the rest of the chapter, we will use $A\phi(y_k)$ where the discrete-time stochastic process x_k in Definition 4 is the full state of the interaction system, *i.e.,* X_k in (4.5).

Let Q_k be the information that the ego vehicle can acquire at time k. This information Q_k will be $Q_k = [x_k, x_k^o]$ with x_k^o being the observed state of all other road users by the ego vehicle at time k. Note that $Q_k = x_k$ if no other road users appear from the occlusions.

We consider the following condition at all time k:

$$A\Psi(Q_k) \geq -\gamma(\Psi(Q_k) - (1-\epsilon)),\ \forall k \geq 0. \tag{4.12}$$

Here, $\gamma : \mathbb{R} \to \mathbb{R}$ is a function that satisfies the following 2 design requirements:

Requirement 1: $\gamma(h)$ is linear and increasing in h.

Requirement 2: $\gamma(h) \leq h$ for any $h \in \mathbb{R}$.

The probability measure of $\mathbb{P}(S|I)$ is taken over X, the global state, conditioned on Q, the information that can be accessed by the ego vehicle. Therefore, the values on both sides of (4.12) can be computed using Q.

Theorem 4.3.1. *Consider systems* (4.1) *and* (4.5)*. We assume the initial condition* $x_0 = x$ *satisfies* $\mathbb{P}(S|x_0 = x) \geq 1 - \epsilon$*. If at each time* k*, the ego vehicle generates a control policy that satisfies* (4.12)*, then the following condition holds:*

$$\mathbb{P}(S) = \mathbb{E}[\mathbb{P}(S|x_k)] \geq 1 - \epsilon, \ \forall k \geq 0. \tag{4.13}$$

See [93, 94] for the proof. Theorem 4.3.1 says the long-term safety of the system is guaranteed by the proposed safe condition (4.12) for all time with desired probability.

4.3.2 Proposed Safe Occlusion-Aware Control

In this section, we propose a control strategy that imposes (4.12) to ensure long-term safety of the system. We start by approximating $A\boldsymbol{\Psi}(Q)$, the infinitesimal generator of long-term safety. Since only the ego's vehicle's state can be controlled, with a slight abuse of notation, we use $\boldsymbol{\Psi}(x)$ to represent $\boldsymbol{\Psi}(Q)$ in the control design phase for the rest of the chapter. This $\boldsymbol{\Psi}(x)$ will refer to different $\boldsymbol{\Psi}(Q)$ under specific situations (*e.g.,* there are no other road users in sight, or pedestrians are currently crossing the street). Let $\mathcal{D}(x) \in \mathbb{R}^n$ denote the finite-difference approximation of the gradient $\nabla_x \boldsymbol{\Psi}(x)$, *i.e.,*

$$\mathcal{D}_j(x) = \frac{\boldsymbol{\Psi}(x + \Delta e_j) - \boldsymbol{\Psi}(x - \Delta e_j)}{2\Delta} \tag{4.14}$$

where $\mathcal{D}_j$ is the j^{th} element of $\mathcal{D}$, Δ is the step-size, and e_j denotes a vector that takes a scalar value of 1 in the j^{th} entry and 0 otherwise.

Lemma 5. *If* $A\boldsymbol{\Psi}(x)$ *exists, then:*

$$A\boldsymbol{\Psi}(x) = \lim_{\Delta \to 0} \mathcal{D}_j^T(x) \left(f(x) + g(x)u\right). \tag{4.15}$$

Lemma 5 is a result of the chain rule, with the left-hand side of (4.15) being the time derivative of $\boldsymbol{\Psi}(x)$, and the right-hand side being the state

derivative of $\mathbf{\Psi}(x)$ multiplies dx/dt which is the dynamics (4.1). With this, we obtain the inequality constraint on the control-action u:

$$-\mathcal{D}_j^T(x)g(x)u \leq \mathcal{D}_j^T(x)f(x) + \gamma\left(\mathbf{\Psi}(x) - (1-\epsilon)\right) \tag{4.16}$$

Utilizing the safety condition (4.16) and the nominal controller N from section 4.2.1, we can formulate the safe controller $K : \mathbb{R}^n \to \mathbb{R}^m$ as a constrained quadratic optimization problem:

$$\begin{aligned} K(x) := \underset{u\in\mathbb{R}^m}{\arg\min} \left\|u - N(x)\right\|_2 \\ \text{s.t. } (4.16) \end{aligned} \tag{4.17}$$

The optimization problem penalizes deviation from the nominal control action (minimally invasive) while ensuring the specified constraints are satisfied, complying with requisite safety specifications.

Remark 7. The proposed optimization-based safe control (4.17) is easy to design and implement because it only contains function γ and the desired risk tolerance ϵ as tunable parameters and only imposes linear constraints on control, which forms an efficient quadratic program (QP).

Remark 8. The variable $\mathbf{\Psi}(x)$ has the physical meaning of the safety probability of the system in the long term. Its value at x indicates how risky the system will be in the future, evolving from state x. This property of $\mathbf{\Psi}(x)$ can also guide the control design when necessary (*e.g.,* one can directly specify the expected future state and control based on $\mathbf{\Psi}(x)$ when the control constraint (4.16) is numerically infeasible).

4.3.3 Algorithm Description

We present the overall safe control strategy in Algorithm 3. The safety probability, in procedure $\mathbf{\Psi}(x)$, is numerically estimated using Monte-Carlo simulations; we loop over the number of specified MC-episodes (N_E), and at the k^{th} iteration, we do the following. In line 3, we initialize the safety check p_k that switches to 0 when a violation is detected. In line 4, we initialize the state of vehicle dynamics initial value problem (IVP) with the current state estimate of the actual vehicle. Next, in line 5, we jointly solve the time-invariant closed-loop vehicle dynamics IVP (4.3) with the initial condition from line 4 and the interaction motion model (4.5) over the specified time interval $\mathcal{T} = \{k, k+1, \cdots k+T\}$, giving us a forward rollout. Since both

Algorithm 3 Occlusion and interaction-aware safe controller

Input: x ▷ Vehicle State
Output: u ▷ Safe Control Action
Parameters: T, N_E ▷ Preview Horizon, # Episodes

1: **procedure** $\boldsymbol{\Psi}(x)$
2: **for** $k \in \{1, 2, \ldots, N_E\}$ **do** ▷ MC Episodes
3: $p_k \leftarrow 1$ ▷ Initialize safety check
4: $x_0 \leftarrow x$ ▷ Initialize state
5: Solve (4.3) and (4.5) in $\mathcal{T}$ ▷ Forward Rollout
6: **if** not S **then**
7: $p_k \leftarrow 0$ ▷ Safety Violation
8: **end if**
9: **end for**
10: **return** $\frac{1}{N_E} \sum_{k=1}^{N_E} p_k$ ▷ Safe probability
11: **end procedure**
12:
13: **procedure** $K(x)$
14: $u_N \leftarrow N(x)$ ▷ Compute nominal control action
15: Obtain $\mathcal{D}(x)$ using (4.14) ▷ Gradient of $\boldsymbol{\Psi}$
16: Obtain u by solving QP (4.17) with constraint (4.16)
17: **return** u
18: **end procedure**

the vehicle and the interaction models are time-invariant, the start and end times of the interval $\mathcal{T}$ are irrelevant. In line 7, we check for a safety violation in the forward rollout. Finally, at the end of the procedure, we compute and return the mean of p_k over all the episodes. Since $\boldsymbol{\Psi}(x)$ gives the safety probability of the system over the time horizon $\mathcal{T}$, it encodes information of prediction on the future as well as the levels of uncertainty.

Procedure $K(x)$ encompasses the constrained optimization controller outlined in (4.17), which involves evaluating the nominal control action u_N in line 14, computing the finite difference approximation of the gradient of safe probability $\mathcal{D}(x)$, and finally obtaining the safe control action by solving the QP (4.17). This control action ensures that condition (4.9) is met.

Therefore, Algorithm 3 can account for long-term safety and guarantees to steer system trajectories toward the direction of non-decreasing long-term safe probability in the presence of latent risks, eliminating potential myopic

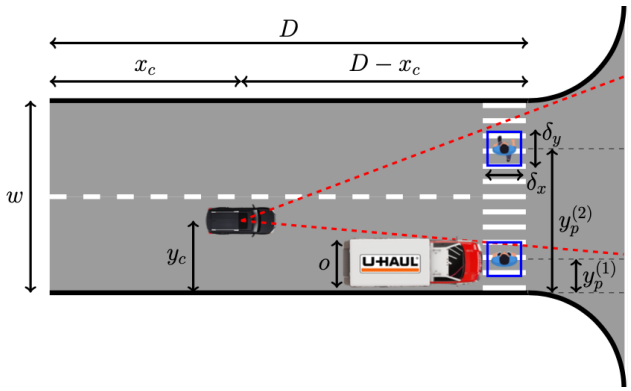


Figure 4.1: Occluded crosswalk scenario of interest.

decision-making, typically seen in traditional safe control techniques [1], that may result in unsafe behaviors in the future.

4.4 Deployment and Experiment

For the remainder of this chapter, we focus on a case study of the safe control strategy on a pedestrian-vehicle interaction scenario at occluded crossing intersections. We introduce the design of the simulation in section 4.4.1, the experiments on a 1/10th scale autonomous vehicle in section 4.4.2, and present the results in section 4.4.3. We point out that even though we have chosen to examine the safety of pedestrian-vehicle interactions at crossing intersections as the case study, the proposed control strategy can be applied to different road scenarios without redesign.

4.4.1 Case Study Scenario

We consider a case of an intersection with an unsignalized marked crosswalk (zebra crossing) as seen in Fig. 4.1. We use local coordinates whose origin is D away from the edge of the crosswalk.

Here, the vehicle's position is (x_c, y_c) , the distance from the car to the crosswalk is $D - x_c$, and the i^{th} pedestrian's position along the crosswalk is denoted by $y_{\text{p}}^{(i)}$. We assign a bounding box to each pedestrian with dimensions (δ_x, δ_y), centered around the pedestrian's position, as seen in Fig. 4.1. The obstruction, which is a parked truck, has size o and occludes pedestrians' presence from the field of view of the vehicle until they have moved past it.

1) Vehicle Model: For the simulation, we start by setting up the dynamics of the vehicle based upon [82]. Assuming the vehicle is a point-mass moving along a straight line, we get the following dynamics

$$m\frac{dv}{dt} = F_t - F_r, \tag{4.18}$$

where m is the mass of the vehicle, v is the longitudinal velocity of the vehicle, F_t is the tire force generated by the engine/motor, and F_r is the net drag force due to the tire's rolling resistance and aerodynamic drag. Here, we assume F_t to be our control input. With this, we can write down the governing equations of motion as an ODE. Let $x = \begin{bmatrix} x_1 & x_2 \end{bmatrix}^T$, where x_1 is the vehicle's position, and $\dot{x}_1 = x_2 = v$ the longitudinal velocity. With this, assuming a time-step of Δt, we get the following discrete-time system dynamics using the forward-Euler method

$$x_{k+1} = \underbrace{x_k + \Delta t \begin{bmatrix} x_{2k} \\ -\frac{1}{m}F_r \end{bmatrix}}_{f(x_k)} + \underbrace{\Delta t \begin{bmatrix} 0 \\ \frac{1}{m} \end{bmatrix}}_{g(x_k)} u_k. \tag{4.19}$$

2) Nominal Cruise Controller: The cruise controller maintains a set cruising speed while ensuring comfortable acceleration/deceleration. When a pedestrian is visible in the vehicle's field of view, the cruise controller attempts to reduce the vehicle's speed based on the calculated time-to-collision T_{TTC} to that pedestrian

$$T_{\text{TTC}} = \frac{r}{\max\left(-\dot{r}, 0^+\right)}, \tag{4.20}$$

where 0^+ is a small positive constant and r is the estimated range to the pedestrian, note that the vehicle's auxiliary automatic emergency braking system will take precedence over the nominal cruise controller in a catastrophic situation.

3) Pedestrian Model: In our study, we model the behaviors of pedestrians as the combination of decision-making and motion dynamics described in section 4.2.2. Specifically, in the scenario shown in Fig. 4.1, we model that the pedestrians keep crossing without detecting the ego vehicles with a certain probability. This pedestrian model allows us to account for the worst-case scenarios when evaluating safety (*e.g.,* distracted pedestrian keeps crossing even as a car approaches them).

The decision process for pedestrian i, assumes that after the pedestrian has crossed the occlusion, they will recognize the oncoming vehicle and stop with a probability α:

$$d(k) \sim D(y_p^{(i)} \mid \mathcal{Z}_k) = \begin{cases} \text{Bernoulli}(\alpha) & \text{if} \quad y_p^i \geq o \\ 0 & \text{if} \quad y_p^i < o \end{cases} \tag{4.21}$$

where $\mathcal{Z}_k$ is the event of a vehicle currently approaching the crosswalk at time step k and $d(k) \in \{0, 1\}$ is a Bernoulli stochastic process, indicating whether or not the pedestrian recognizes the vehicle and stops.

For the pedestrian motion model, we have that when pedestrian i begins crossing, they travel at a fixed speed sampled from a normal distribution $v_{\text{ped}}^{(i)} \sim \mathcal{N}(\_v_{\text{ped}}, \sigma_{\text{ped}}^2)$ [95] till they've reached the end of the crosswalk or stop after recognizing the oncoming car:

$$\begin{aligned} & y_{p_{(k+1)}}^{(i)} \sim f_z(y_{p_{(k)}}^{(i)} \mid d(k)) \\ = & \begin{cases} 0 & \text{if} \quad d(k) = 1 \\ v_{\text{ped}}^{(i)} \Delta t + y_{p_{(k)}}^{(i)} & \text{if} \quad d(k) = 0 \end{cases} \end{aligned} \tag{4.22}$$

Further, we assume that pedestrians arrive at the crossing independently of each other and at random with a mean interarrival time T_a [96, 97]. That is to say, within an infinitesimally small time interval dt, the probability of a pedestrian arriving at the crossing is dt/T_a. As a consequence, the time interval ΔT between two successive pedestrians arriving at the crosswalk will follow an exponential distribution, and the number of pedestrians N_p that arrive within a time interval Δt will follow a Poisson distribution:

$$\Delta T \sim \text{Exponential}\,(1/T_a) \tag{4.23}$$

$$N_{\text{ped}} \sim \text{Poisson}\,(\Delta t/T_a) \tag{4.24}$$

5) Safety Specification: For this case study, we define the safety criteria in terms of the set $\mathcal{B}^i \subset \mathbb{R}^2$, which is set of the i^{th} pedestrian's bounding box as seen in Fig. 4.1:

$$\mathcal{B}^i = \left[x_p^{(i)} - \delta_x, x_p^{(i)} + \delta_x\right] \times \left[y_p^{(i)} - \delta_y, y_p^{(i)} + \delta_y\right] \tag{4.25}$$

with this, we specify the safe event $\mathcal{C}_t^i$ at time t as the set of outcomes wherein the vehicle is not present in $\mathcal{B}^i$, i.e., $(x_c, y_c) \notin \mathcal{B}^i$.

4.4.2 Hardware Experimental Setup

We evaluate the feasibility and efficacy of the proposed safe control algorithm in a real-world scaled setting of our case-study environment. In particular, we implement the proposed method on a 1/10th scale autonomous vehicle (AV) (see [98] for specific details on the hardware platform). We used an NVIDIA Jetson Xavier NX with a CPU SPEC2006 score of 18.9 GFLOPS as our mobile-embedded computing platform and ROS-2 in C++ for software. The computing capability of our platform is relatively limited. One major challenge of the hardware experiments includes added stochasticity due to imperfect state estimation, which in our case, comes from a particle filter. Another challenge is that most autonomous driving stacks rely on kinematic control inputs, i.e., velocity and not acceleration. To account for this, we use an online double integrator model of the vehicle dynamics (4.19) to translate our proposed controller's acceleration outputs into velocity commands, allowing seamless integration into existing state-of-the-art platforms.

1) Hardware Nominal Controller: For path tracking, we use a kinematic model-based linear time-varying MPC [99]. We use the cruise controller outlined in section 4.4.1 for speed control.

2) Proposed Controller Implementation: The limited compute capability of the embedded platform poses a challenge to real-time implementation. To address this issue, we propose modifying procedure $\mathbf{\Psi}(x)$ in Algorithm 3 as follows. First, we offline precompute the values of $\mathbf{\Psi}(x)$ with a mesh grid of x to form a lookup table as shown in Fig. 4.2. We then store this lookup table and use it to build a sinc interpolator. With the interpolator, it is possible to achieve real-time performance.

3) Experiment Setup: Fig. 4.3 shows the experimental setup for the hardware evaluation. The goal of the nominal controller, in this case, would be to drive the vehicle along the corridor and through the occluded intersection (blue bin) as seen in Fig. 4.3.

4.4.3 Results and Analyses

In this section, we present empirical results of proposed method's performance with numerical simulations and hardware experiments. These serve to quantify and corroborate the technical merits of the proposed method, specifically the guaranteed long-term safety, balancing opposing safety and performance objectives and robustness to large uncertainties. For all experi-

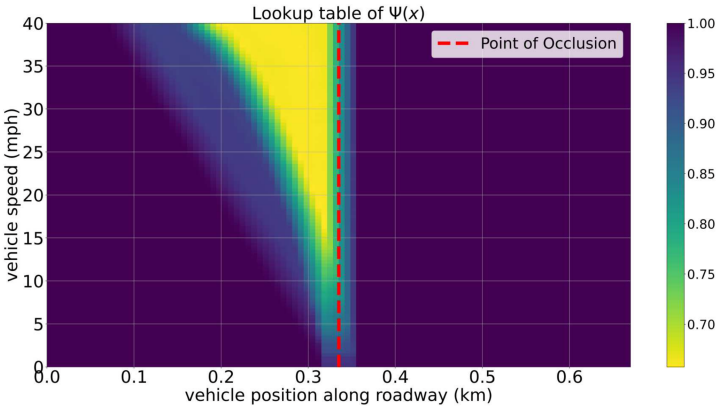


Figure 4.2: Precomputed lookup table of $\boldsymbol{\Psi}(x)$.

Figure 4.3: Case-study environment for hardware experiments.

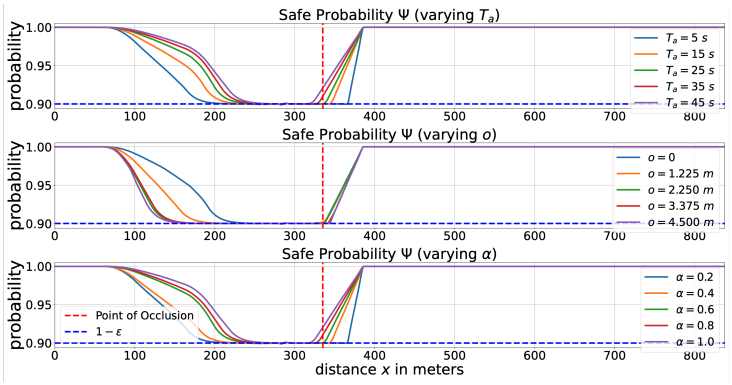


Figure 4.4: Long-term safe probability of proposed method for three parameter cases. The top subplot shows the effect of varying the mean interarrival time T_a, the middle varies in occlusion size o, and the bottom-most varies in pedestrian awareness probability α.

ments, we pick an outlook horizon of $T = 10$ s and a baseline cruising velocity of $v_{\text{cruise}} = 35$ mph.

1) Long-term safety guarantee: We choose a risk tolerance of $\epsilon = 0.10$. We run the proposed controller with different pedestrian interarrival time T_a, occlusion size o, and pedestrian awareness α. We choose $T_a = 25$ s, $o = 2.25$ m, and $\alpha = 0.4$ as the baseline parameter values and vary one of the parameter values for ablation experiments.

Fig. 4.4 shows the proposed controller's ability to guarantee long-term safety under all tested circumstances. In the first subplot of Fig. 4.4, the safety probability drops earlier in response to shorter interarrival times, larger occlusion sizes, or lower pedestrian awareness, thereby demonstrating the algorithm's predictive capabilities.

Fig. 4.5 shows the vehicle velocities generated with the proposed safe controller on different parameter settings. We see that the proposed method modulates the vehicle's velocity tantamount to perceived latent risks. For cases with higher perceived latent risk, we see that the speed reduces well ahead of the occlusion's position and maintains that speed until past it, showcasing the proposed controller's ability to look into the future and impose a more effective safe control on the system once the safety probability tends to drop. Further, when perceived risks are lower, the controller does not slow down more than necessary, not compromising the desired performance. This phenomenon is made more evident in Fig. 4.6, where we compare the

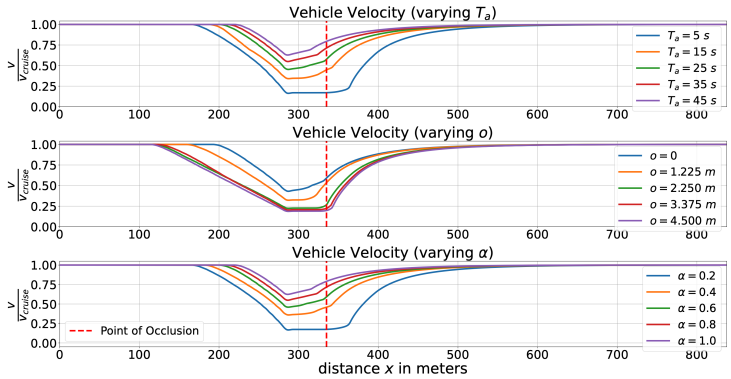


Figure 4.5: Safe vehicle velocity generated for three parameter cases. The top subplot shows the effect of varying the mean interarrival time T_a, the middle varies in occlusion size o, and the bottom-most varies in pedestrian awareness probability α.

minimum safe speeds of the vehicle with varying risk tolerance values ϵ.

2) Safety v/s Performance Trade-off: We begin by quantifying safety, performance, and uncertainty in the context of our case study. We use the distance traveled by the vehicle over 2 minutes as the performance metric; for safety, we use the minimum safe probability achieved over the run, and for uncertainty in the pedestrian arrival process, we evaluate the Shannon Entropy of (4.24). To obtain the trade-off, in the case of the nominal controller, we vary the desired cruising speed, and for the proposed controller, we range over the risk tolerance ϵ with baseline parameters. In this case, we have chosen [6.433, 8.467, 10.411, 12.223, 14.258] mph as the desired speeds for the nominal controller to match the risk levels achieved by the proposed method closely. For the proposed controller, we choose [0.1, 0.125, 0.150, 0.175, 0.200] as values for the risk tolerance parameter ϵ. And finally, we also consider $\mathcal{H}_\infty$ control to demonstrate the effects of using a deterministic worst-case safe controller. Fig. 4.7 exhibits our proposed method's ability to fulfill the desired safety requirements while not being excessively conservative, and Fig. 4.8 shows that the proposed method's performance degrades gracefully with increasing uncertainty. Furthermore, we see that accounting for all possible worst-cases without considering causality, as in the case of the $\mathcal{H}_\infty$, produces overly conservative behaviors that compromises performance or in some cases induces infeasibility.

3) Hardware Experiment Results

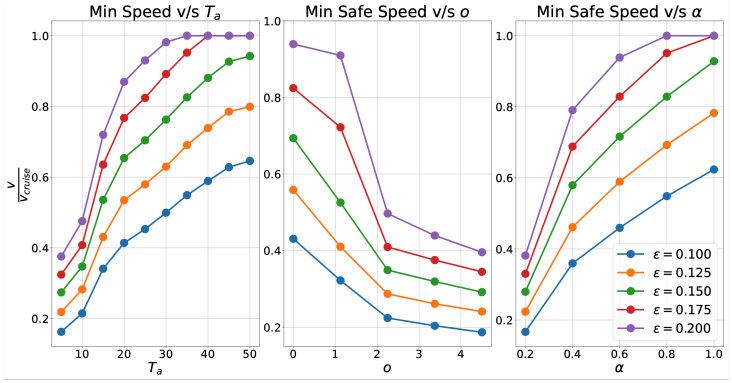


Figure 4.6: Minimum safe speeds achieved with the proposed controller over all three parameters and for different risk tolerances ϵ.

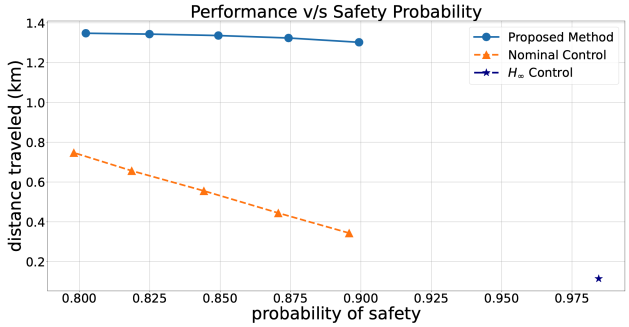


Figure 4.7: Performance v/s safety tradeoff.

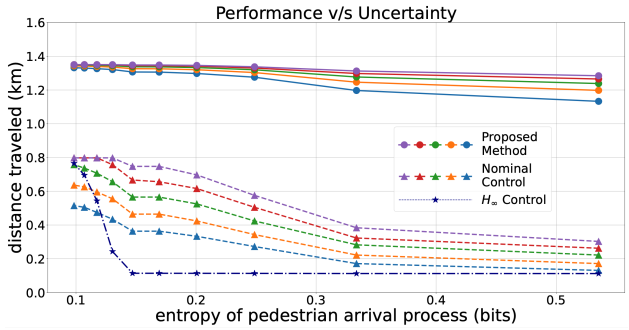


Figure 4.8: Performance v/s uncertainty in pedestrian arrival process. Matching colors for plots of the nominal and proposed controller correspond to equivalent safety probabilities.

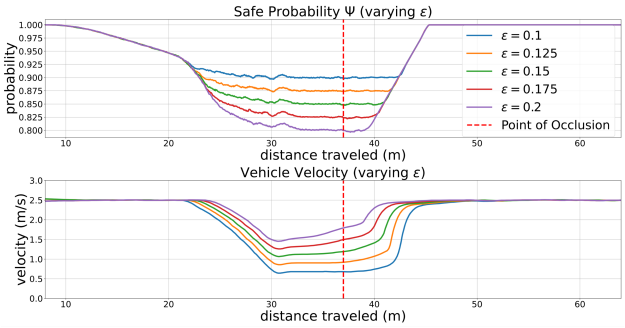


Figure 4.9: Experimental results of long-term safe probability (top) and safe vehicle velocities (bottom) for five cases of ϵ.

A video of the experiments can be found at Video Link. We run repeated identical experiments on the 1/10th scale AV over five values of the risk tolerance parameter ϵ and record estimated state and sensor data. Fig. 4.9 demonstrates that the performance of the proposed controller on hardware is consistent with our simulation results. Further, benchmarking the proposed algorithm on the embedded platform yields the following statistics for computational throughput: average rate of 67.924 Hz, maximum rate of 166.67 Hz, minimum rate of 52.631 Hz, with a standard deviation of 0.02661 Hz, over 61130 samples.

4.5 Summary

This chapter proposes an occlusion- and interaction-aware safe control strategy that ensures long-term safety in the presence of latent risks without overly compromising performance. We demonstrate its reliability and computational efficiency via numerical simulations and hardware experiments. Finally, we show that the proposed controller is modular and can seamlessly integrate into existing control frameworks, vastly improving its applicability. Future work includes conducting real-world experiments with the proposed method, and comparing the results with human driving behaviors.

Bibliography

[1] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *European control conference*. IEEE, 2019, pp. 3420–3431.

[2] O. Khatib, "Real-time obstacle avoidance for manipulators and mobile robots," in *Autonomous robot vehicles*. Springer, 1986, pp. 396–404.

[3] 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*, vol. 52, no. 8, pp. 1415–1428, 2007.

[4] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, nov 1999. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0005109899001132

[5] 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.

[6] M. Farina, L. Giulioni, and R. Scattolini, "Stochastic linear Model Predictive Control with chance constraints – A review," *Journal of Process Control*, vol. 44, pp. 53–67, aug 2016. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0959152416300130

[7] L. Hewing, K. P. Wabersich, M. Menner, and M. N. Zeilinger, "Learning-Based Model Predictive Control: Toward Safe Learning in Control," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 3, no. 1, pp. 269–296, may 2020. [Online]. Available: https://www.annualreviews.org/doi/10.1146/annurev-control-090419-075625

[8] M. Chen and C. J. Tomlin, "Hamilton–Jacobi Reachability: Some Recent Theoretical Advances and Applications in Unmanned Airspace Management," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, no. 1, pp. 333–358, may 2018. [Online]. Available: https://www.annualreviews.org/doi/10.1146/annurev-control-060117-104941

[9] M. Ahmadi, X. Xiong, and A. D. Ames, "Risk-sensitive path planning via cvar barrier functions: Application to bipedal locomotion," *arXiv preprint arXiv:2011.01578*, 2020.

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

[11] W. Luo, W. Sun, and A. Kapoor, "Multi-robot collision avoidance under uncertainty with probabilistic safety barrier certificates," *arXiv preprint arXiv:1912.09957*, 2019.

[12] Y. Lyu, W. Luo, and J. M. Dolan, "Probabilistic safety-assured adaptive merging control for autonomous vehicles," in *2021 IEEE International Conference on Robotics and Automation (ICRA)*, 2021, pp. 10 764–10 770.

[13] S. Yaghoubi, K. Majd, G. Fainekos, T. Yamaguchi, D. Prokhorov, and B. Hoxha, "Risk-bounded control using stochastic barrier functions," *IEEE Control Systems Letters*, 2020.

[14] C. Santoyo, M. Dutreix, and S. Coogan, "A barrier function approach to finite-time stochastic system verification and control," *Automatica*, p. 109439, 2021.

[15] G. P. Moustris, S. C. Hiridis, K. M. Deliparaschos, and K. M. Konstantinidis, "Evolution of autonomous and semi-autonomous robotic surgical systems: a review of the literature," *The international journal of medical robotics and computer assisted surgery*, vol. 7, no. 4, pp. 375–392, 2011.

[16] B. Øksendal, *Stochastic Differential Equations: An Introduction with Applications*, 6th ed., ser. Universitext. Berlin Heidelberg: Springer-Verlag, 2003.

[17] A. N. Borodin, *Stochastic processes*. Springer, 2017.

[18] A. Chern, X. Wang, A. Iyer, and Y. Nakahira, "Safe control in the presence of stochastic uncertainties," *Accepted to 2021 60th Conference on Decision and Control*, 2021.

[19] J. L. W. V. Jensen, "Sur les fonctions convexes et les inégalités entre les valeurs moyennes," *Acta Mathematica*, vol. 30, pp. 175–193, 1906. [Online]. Available: http://projecteuclid.org/euclid.acta/1485887155

[20] A. Chern, X. Wang, A. Iyer, and Y. Nakahira, "Safe control in the presence of stochastic uncertainties," *arXiv preprint arXiv:2104.01259*, 2021.

[21] L. C. Evans, "Partial differential equations and monge-kantorovich mass transfer," *Current developments in mathematics*, vol. 1997, no. 1, pp. 65–126, 1997.

[22] R. J. LeVeque *et al.*, *Finite volume methods for hyperbolic problems*. Cambridge university press, 2002, vol. 31.

[23] Q. Lu, A. Sorniotti, P. Gruber, J. Theunissen, and J. De Smet, "H loop shaping for the torque-vectoring control of electric vehicles: Theoretical design and experimental assessment," *Mechatronics*, vol. 35, pp. 32–43, 2016.

[24] H.-S. TAN and Y.-K. CHIN, "Vehicle antilock braking and traction control: a theoretical study," *International journal of systems science*, vol. 23, no. 3, pp. 351–365, 1992.

[25] L. Zhang, H. Ding, J. Shi, Y. Huang, H. Chen, K. Guo, and Q. Li, "An adaptive backstepping sliding mode controller to improve vehicle maneuverability and stability via torque vectoring control," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 2598–2612, 2020.

[26] M. Bauer and M. Tomizuka, "Fuzzy logic traction controllers and their effect on longitudinal vehicle platoon systems," *Vehicle system dynamics*, vol. 25, no. 4, pp. 277–303, 1996.

[27] A. Parra, A. Zubizarreta, J. Pérez, and M. Dendaluce, "Intelligent torque vectoring approach for electric vehicles with per-wheel motors," *Complexity*, vol. 2018, 2018.

[28] X. Wu, C. Ma, M. Xu, Q. Zhao, and Z. Cai, "Single-parameter skidding detection and control specified for electric vehicles," *Journal of the Franklin Institute*, vol. 352, no. 2, pp. 724–743, 2015.

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

[30] 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, 2018.

[31] M. Wielitzka, M. Dagen, and T. Ortmaier, "Sensitivity-based road friction estimation in vehicle dynamics using the unscented kalman filter," in *2018 Annual American Control Conference (ACC)*. IEEE, 2018, pp. 2593–2598.

[32] S. Jung and T. C. Hsia, "Explicit lateral force control of an autonomous mobile robot with slip," in *2005 IEEE/RSJ International Conference on Intelligent Robots and Systems*. IEEE, 2005, pp. 388–393.

[33] S. De Pinto, C. Chatzikomis, A. Sorniotti, and G. Mantriota, "Comparison of traction controllers for electric vehicles with on-board drivetrains," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 6715–6727, 2017.

[34] L. De Novellis, A. Sorniotti, P. Gruber, J. Orus, J.-M. R. Fortun, J. Theunissen, and J. De Smet, "Direct yaw moment control actuated through electric drivetrains and friction brakes: Theoretical design and experimental assessment," *Mechatronics*, vol. 26, pp. 1–15, 2015.

[35] Y. Wang, L. Yuan, H. Chen, P. Du, and X. Lian, "An anti-slip control strategy with modifying target and torque reallocation for heavy in-wheel motor vehicle," *Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering*, p. 09544070211063086, 2021.

[36] J. Zhou, H. Yue, J. Zhang, and H. Wang, "Iterative learning double closed-loop structure for modeling and controller design of output stochastic distribution control systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 6, pp. 2261–2276, 2014.

[37] C. Yin, J.-X. Xu, and Z. Hou, "A high-order internal model based iterative learning control scheme for nonlinear systems with time-iteration-varying parameters," *IEEE Transactions on Automatic Control*, vol. 55, no. 11, pp. 2665–2670, 2010.

[38] K.-H. Park, "An average operator-based pd-type iterative learning control for variable initial state error," *IEEE Transactions on Automatic Control*, vol. 50, no. 6, pp. 865–869, 2005.

[39] I. D. Landau, R. Lozano, M. M'Saad, and A. Karimi, *Adaptive control: algorithms, analysis and applications*. Springer Science & Business Media, 2011.

[40] G. Bai, Y. Meng, L. Liu, W. Luo, and Q. Gu, "Review and comparison of path tracking based on model predictive control," *Electronics*, vol. 8, no. 10, p. 1077, 2019.

[41] F. Borrelli, A. Bemporad, M. Fodor, and D. Hrovat, "An mpc/hybrid system approach to traction control," *IEEE Transactions on Control Systems Technology*, vol. 14, no. 3, pp. 541–552, 2006.

[42] P. Falcone, F. Borrelli, J. Asgari, H. E. Tseng, and D. Hrovat, "Predictive active steering control for autonomous vehicle systems," *IEEE Transactions on control systems technology*, vol. 15, no. 3, pp. 566–580, 2007.

[43] O. Barbarisi, G. Palmieri, S. Scala, and L. Glielmo, "Ltv-mpc for yaw rate control and side slip control with dynamically constrained differential braking," *European Journal of Control*, vol. 15, no. 3-4, pp. 468–479, 2009.

[44] B. Leng, L. Xiong, Z. Yu, K. Sun, and M. Liu, "Robust variable structure anti-slip control method of a distributed drive electric vehicle," *IEEE Access*, vol. 8, pp. 162 196–162 208, 2020.

[45] T. Brüdigam, M. Olbrich, D. Wollherr, and M. Leibold, "Stochastic model predictive control with a safety guarantee for automated driving," *IEEE Transactions on Intelligent Vehicles*, pp. 1–1, 2021.

[46] A. Carvalho, Y. Gao, S. Lefevre, and F. Borrelli, "Stochastic predictive control of autonomous vehicles in uncertain environments," in *12th International Symposium on Advanced Vehicle Control*, 2014, pp. 712–719.

[47] G. Siddharth, Z. Wang, H. Jing, and Y. Nakahira, "Adaptive safe control for driving in uncertain environments," *arXiv preprint*, 2022.

[48] W. Luo, W. Sun, and A. Kapoor, "Multi-robot collision avoidance under uncertainty with probabilistic safety barrier certificates," *Advances in Neural Information Processing Systems*, vol. 33, pp. 372–383, 2020.

[49] P. Falcone, H. Eric Tseng, F. Borrelli, J. Asgari, and D. Hrovat, "Mpc-based yaw and lateral stabilisation via active front steering and braking," *Vehicle System Dynamics*, vol. 46, no. S1, pp. 611–628, 2008.

[50] H. Zhao, B. Ren, H. Chen, and W. Deng, "Model predictive control allocation for stability improvement of four-wheel drive electric vehicles in critical driving condition," *IET Control Theory & Applications*, vol. 9, no. 18, pp. 2688–2696, 2015.

[51] E. Siampis, E. Velenis, S. Gariuolo, and S. Longo, "A real-time nonlinear model predictive control strategy for stabilization of an electric vehicle at the limits of handling," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 6, pp. 1982–1994, 2017.

[52] J. Yoon, W. Cho, J. Kang, B. Koo, and K. Yi, "Design and evaluation of a unified chassis control system for rollover prevention and vehicle stability improvement on a virtual test track," *Control Engineering Practice*, vol. 18, no. 6, pp. 585–597, 2010.

[53] M. Ataei, A. Khajepour, and S. Jeon, "Model predictive control for integrated lateral stability, traction/braking control, and rollover prevention of electric vehicles," *Vehicle system dynamics*, vol. 58, no. 1, pp. 49–73, 2020.

[54] M. Isaksson Palmqvist, "Model predictive control for autonomous driving of a truck," https://www.diva-portal.org/smash/get/diva2:930995/FULLTEXT01.pdf, 2016.

[55] U. Kiencke and L. Nielsen, "Automotive control systems: for engine, driveline, and vehicle," 2000.

[56] P. Falcone, M. Tufo, F. Borrelli, J. Asgari, and H. E. Tseng, "A linear time varying model predictive control approach to the integrated vehicle dynamics control problem in autonomous systems," in *2007 46th IEEE Conference on Decision and Control*. IEEE, 2007, pp. 2980–2985.

[57] J. A. Andersson, J. V. Frasch, M. Vukov, and M. Diehl, "A condensing algorithm for nonlinear mpc with a quadratic runtime in horizon length," *Automatica*, pp. 97–100, 2013.

[58] L. T. Biegler, "Efficient solution of dynamic optimization and nmpc problems," in *Nonlinear model predictive control*. Springer, 2000, pp. 219–243.

[59] H. Zhu, B. Brito, and J. Alonso-Mora, "Decentralized probabilistic multi-robot collision avoidance using buffered uncertainty-aware voronoi cells," *Autonomous Robots*, pp. 1–20, 2022.

[60] D. Claes, D. Hennes, K. Tuyls, and W. Meeussen, "Collision avoidance under bounded localization uncertainty," in *2012 IEEE/RSJ International Conference on Intelligent Robots and Systems*. IEEE, 2012, pp. 1192–1198.

[61] L. Lindemann and D. V. Dimarogonas, "Control barrier functions for signal temporal logic tasks," *IEEE control systems letters*, vol. 3, no. 1, pp. 96–101, 2018.

[62] 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.

[63] M. Farina, L. Giulioni, and R. Scattolini, "Stochastic linear model predictive control with chance constraints–a review," *Journal of Process Control*, vol. 44, pp. 53–67, 2016.

[64] L. Hewing, K. P. Wabersich, M. Menner, and M. N. Zeilinger, "Learning-based model predictive control: Toward safe learning in control," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 3, pp. 269–296, 2020.

[65] M. Chen and C. J. Tomlin, "Hamilton–jacobi reachability: Some recent theoretical advances and applications in unmanned airspace management," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, pp. 333–358, 2018.

[66] V. Dhiman, M. J. Khojasteh, M. Franceschetti, and N. Atanasov, "Control barriers in bayesian learning of system dynamics," *IEEE Transactions on Automatic Control*, 2021.

[67] K. P. Wabersich, L. Hewing, A. Carron, and M. N. Zeilinger, "Probabilistic model predictive safety certification for learning-based control," *IEEE Transactions on Automatic Control*, vol. 67, no. 1, pp. 176–188, 2021.

[68] Z. Wang, H. Jing, C. Kurniawan, A. Chern, and Y. Nakahira, "Myopically verifiable probabilistic certificate for long-term safety," in *2022 American Control Conference (ACC)*. IEEE, 2022, pp. 4894–4900.

[69] M.-Y. Yu, R. Vasudevan, and M. Johnson-Roberson, "Occlusion-aware risk assessment for autonomous driving in urban environments," *Robotics and Automation Letters*, vol. 4, no. 2, pp. 2235–2241, 2019.

[70] R. Poncelet, A. Verroust-Blondet, and F. Nashashibi, "Safe geometric speed planning approach for autonomous driving through occluded intersections," in *International Conference on Control, Automation, Robotics and Vision*. IEEE, 2020, pp. 393–399.

[71] Z. Zhang and J. Fisac, F, "Safe occlusion-aware autonomous driving via game-theoretic active perception," in *Robotics: Science and Systems*. RSS, 2021.

[72] M. Koç, E. Yurtsever, K. Redmill, and Ü. Özgüner, "Pedestrian emergence estimation and occlusion-aware risk assessment for urban autonomous driving," in *International Intelligent Transportation Systems Conference*. IEEE, 2021, pp. 292–297.

[73] M. Kahn, A. Sarkar, and K. Czarnecki, "I know you can't see me: Dynamic occlusion-aware safety validation of strategic planners for autonomous vehicles using hypergames," in *International Conference on Robotics and Automation*. IEEE, 2022, pp. 11 202–11 208.

[74] Y. Lyu, W. Luo, and J. M. Dolan, "Probabilistic safety-assured adaptive merging control for autonomous vehicles," in *International Conference on Robotics and Automation*. IEEE, 2021, pp. 10 764–10 770.

[75] T. Brüdigam, M. Olbrich, D. Wollherr, and M. Leibold, "Stochastic model predictive control with a safety guarantee for automated driving," *Transactions on Intelligent Vehicles*, 2021.

[76] J. Müller, J. Strohbeck, M. Herrmann, and M. Buchholz, "Motion planning for connected automated vehicles at occluded intersections with infrastructure sensors," *Transactions on Intelligent Transportation Systems*, 2022.

[77] D. Isele, R. Rahimi, A. Cosgun, K. Subramanian, and K. Fujimura, "Navigating occluded intersections with autonomous vehicles using deep reinforcement learning," in *International Conference on Robotics and Automation*. IEEE, 2018, pp. 2034–2039.

[78] K. Sama, Y. Morales, H. Liu, N. Akai, A. Carballo, E. Takeuchi, and K. Takeda, "Extracting human-like driving behaviors from expert driver data using deep learning," *Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9315–9329, 2020.

[79] C. Hubmann, N. Quetschlich, J. Schulz, J. Bernhard, D. Althoff, and C. Stiller, "A pomdp maneuver planner for occlusions in urban scenarios," in *Intelligent Vehicles Symposium*. IEEE, 2019, pp. 2172–2179.

[80] S. Gangadhar, Z. Wang, H. Jing, and Y. Nakahira, "Adaptive safe control for driving in uncertain environments," in *Intelligent Vehicles Symposium*. IEEE, 2022, pp. 1662–1668.

[81] K. Ogata, *Discrete-time control systems*. Prentice-Hall, Inc., 1995.

[82] C.-Y. Liang and H. Peng, "String stability analysis of adaptive cruise controlled vehicles," *International Journal Series C Mechanical Systems, Machine Elements and Manufacturing*, vol. 43, no. 3, pp. 671–677, 2000.

[83] A. Rasouli and J. K. Tsotsos, "Autonomous vehicles that interact with pedestrians: A survey of theory and practice," *Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 900–918, 2019.

[84] P. Kielar, M, O. Handel, D. Biedermann, H, and A. Borrmann, "Concurrent hierarchical finite state machines for modeling pedestrian behavioral tendencies," *Transportation Research Procedia*, vol. 2, pp. 576–584, 2014.

[85] C. Hubmann, J. Schulz, G. Xu, D. Althoff, and C. Stiller, "A belief state planner for interactive merge maneuvers in congested traffic," in *International Conference on Intelligent Transportation Systems*. IEEE, 2018, pp. 1617–1624.

[86] C. Burger, T. Schneider, and M. Lauer, "Interaction aware cooperative trajectory planning for lane change maneuvers in dense traffic," in *International Conference on Intelligent Transportation Systems*. IEEE, 2020, pp. 1–8.

[87] A. Rasouli, I. Kotserub, and J. Tsotsos, K, "Are they going to cross? a benchmark dataset and baseline for pedestrian crosswalk behavior," in *International Conference on Computer Vision Workshops*. IEEE, 2017.

[88] D. Helbing and P. Molnár, "Social force model for pedestrian dynamics," *Physical Review E*, vol. 51, no. 5, pp. 4282–4286, 1995.

[89] F. Camara, N. Bellotto, S. Cosar, F. Weber, D. Nathanael, M. Althoff, J. Wu, J. Ruenz, A. Dietrich, G. Markkula *et al.*, "Pedestrian models for autonomous driving part ii: high-level models of human behavior," *Transactions on Intelligent Transportation Systems*, vol. 22, no. 9, pp. 5453–5472, 2020.

[90] O. Johnson, *Information theory and the central limit theorem*. World Scientific, 2004.

[91] A. H. Lang, S. Vora, H. Caesar, L. Zhou, J. Yang, and O. Beijbom, "Pointpillars: Fast encoders for object detection from point clouds," in *Conference on Computer Vision and Pattern Recognition*, 2019, pp. 12 697–12 705.

[92] X. Zhang, H. Fu, and B. Dai, "Lidar-based object classification with explicit occlusion modeling," in *International Conference on Intelligent Human-Machine Systems and Cybernetics*. IEEE, 2019.

[93] H. Jing and Y. Nakahira, "Probabilistic safety certificate for multi-agent systems," in *2022 IEEE 61st Conference on Decision and Control (CDC)*. IEEE, 2022, pp. 5343–5350.

[94] Z. Wang, H. Jing, C. Kurniawan, A. Chern, and Y. Nakahira, "Myopically verifiable probabilistic certificate for long-term safety," *arXiv preprint arXiv:2110.13380*, 2021.

[95] P. Onelcin and Y. Alver, "The crossing speed and safety margin of pedestrians at signalized intersections," *Transportation Research Procedia*, vol. 22, pp. 3–12, 2017.

[96] D. R. Cox, *Queues*. Chapman and Hall/CRC, 2020.

[97] J. D. Lartey *et al.*, "Predicting traffic congestion: A queuing perspective," *Open Journal of Modelling and Simulation*, vol. 2, no. 02, p. 57, 2014.

[98] M. O'Kelly, H. Zheng, A. Jain, J. Auckley, K. Luong, and R. Mangharam, "Tunercar: A superoptimization toolchain for autonomous racing," in *International Conference on Robotics and Automation*, 2020, pp. 5356–5362.

[99] J. Kong, M. Pfeiffer, G. Schildbach, and F. Borrelli, "Kinematic and dynamic vehicle models for autonomous driving control design," in *Intelligent Vehicles Symposium*, 2015, pp. 1094–1099.

[100] Z. Wang, H. Jing, A. Chern, and Y. Nakahira, "Myopically verifiable probabilistic certificate for long-term safety," *Under Review*, 2023.

[101] S. Gangadhar, Z. Wang, K. Poku, N. Yamada, K. Honda, Y. Nakahira, H. Okuda, and T. Suzuki, "An occlusion- and interaction-aware safe control strategy for autonomous vehicles," in *2023 22nd IFAC World Congress*, 2023.

Appendix A

Research Products for This Project

A.1 Journal Publications

Z. Wang, H. Jing, A. Chern, and Y. Nakahira, "Myopically verifiable probabilistic certificate for long-term safety," *Under Review*, 2023

A.2 Conference Publications

Z. Wang, H. Jing, C. Kurniawan, A. Chern, and Y. Nakahira, "Myopically verifiable probabilistic certificate for long-term safety," in *2022 American Control Conference (ACC)*. IEEE, 2022, pp. 4894–4900

H. Jing and Y. Nakahira, "Probabilistic safety certificate for multi-agent systems," in *2022 IEEE 61st Conference on Decision and Control (CDC)*. IEEE, 2022, pp. 5343–5350

S. Gangadhar, Z. Wang, H. Jing, and Y. Nakahira, "Adaptive safe control for driving in uncertain environments," in *Intelligent Vehicles Symposium*. IEEE, 2022, pp. 1662–1668

S. Gangadhar, Z. Wang, K. Poku, N. Yamada, K. Honda, Y. Nakahira, H. Okuda, and T. Suzuki, "An occlusion- and interaction-aware safe control strategy for autonomous vehicles," in *2023 22nd IFAC World Congress*, 2023

A.3 Code

Open source code for myopic long-term safe control [68]:
https://github.com/jacobwang925/MCLS.